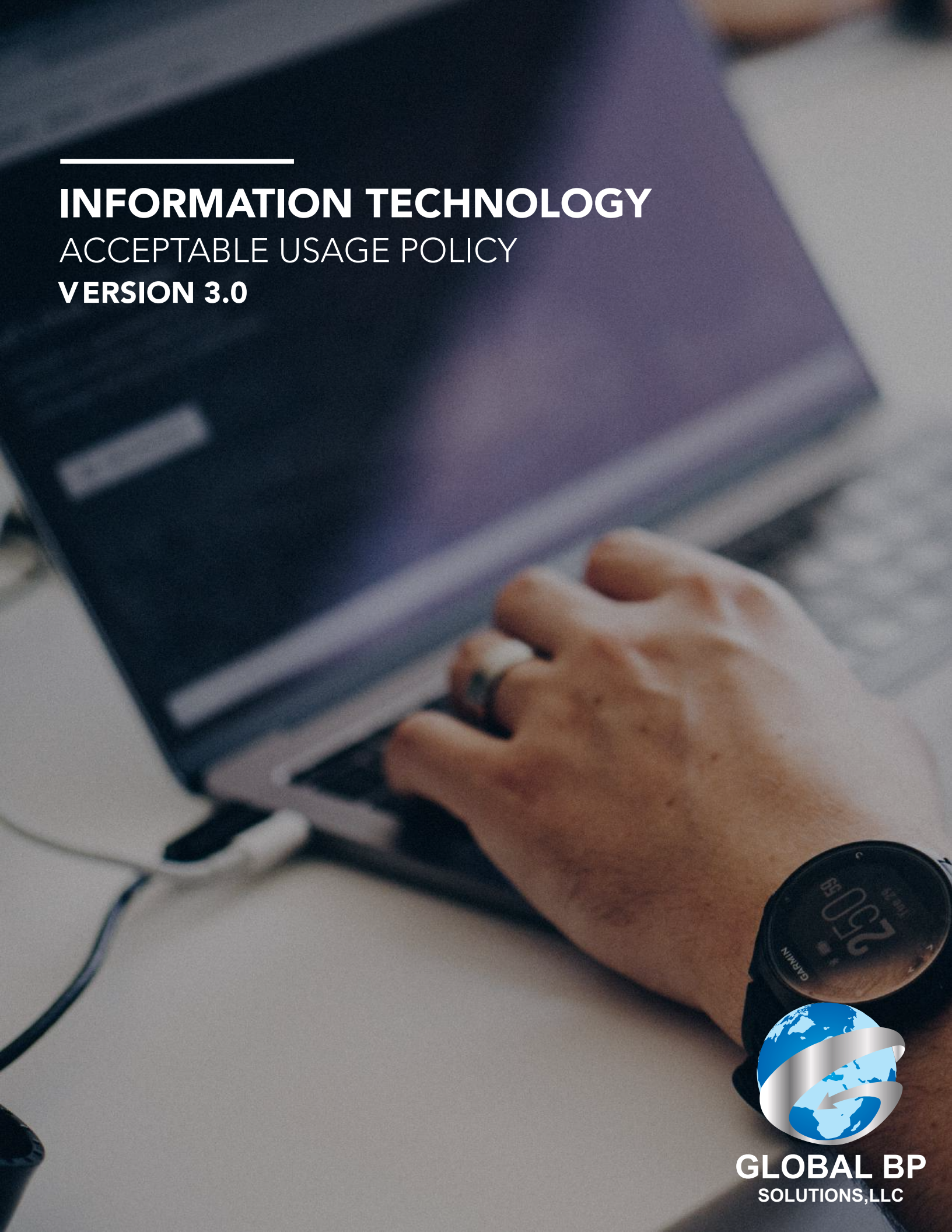


INFORMATION TECHNOLOGY

ACCEPTABLE USAGE POLICY

VERSION 3.0

GLOBAL BP
SOLUTIONS,LLC

Reader Information

Title:	GBPS Information Technology Acceptable Use Policy.
Purpose:	To provide clear guidance on the appropriate, safe and legal way in which to use the GBPS's Information Technology resources protecting our clients.
Author:	GBPS IT Department.
Target Audience:	All users (including GBPS staff, students, contractors, sub- contractors, agency staff and authorized third party commercial service providers) of the GBPS's I.T. resources.
Superseded Documents:	All local Information Technology Acceptable Use Policies and Procedures.
Related Documents:	GBPS Information Security Policy. GBPS Electronic Communications Policy. GBPS Password Standards Policy. GBPS Encryption Policy. GBPS Mobile Phone Device Policy. GBPS Access Control Policy. GBPS Service Provider Confidentiality Agreement. GBPS Information Classification & Handling Policy.

Document History

Version	Owner	Author	Publish Date
1.0	GBPS	GBPS Information Security Project Board (IST)	January 2018
2.0	GBPS	Information Security Team (IST)	August 2018
3.0	GBPS	Information Security Team (IST)	June 2019

1.0 Purpose

The Global BP Solutions (GBPS) is committed to the correct and proper use of its Information Technology (I.T.) resources in support of its administrative and service functions.

The inappropriate use of information technology (I.T.) resources could expose GBPS to risks including virus and malicious software attacks, theft and unauthorized disclosure of information, disruption of network systems and services or litigation. The purpose of this policy is to provide GBPS staff and other users of its I.T. resources with clear guidance on the appropriate, safe and legal way in which they can make use of the organizations I.T. resources.

This policy is mandatory and by accessing any I.T. resources which are owned or leased by the GBPS management team, users are agreeing to abide by the terms of this policy.

2.0 Scope

This policy represents the GBPS's national position and takes precedence over all other relevant policies which are developed at a local level. The policy applies to:

All Information Technology (I.T.) resources provided by the GBPS;

All users (including GBPS staff, students, contractors, sub-contractors, agency staff and authorized third party commercial service providers) of the GBPS's I.T resources;

All use (both personal & GBPS business related) of the GBPS's Information Technology (I.T.) resources;

All connections to (locally or remotely) the GBPS network Domains (LAN/WAN/Wi-Fi);

All connections made to external networks through the GBPS network.

3.0 Definitions

A list of terms used throughout this policy are defined in *Appendix A*.

4.0 Policy

4.1 Principles of Acceptable Use

The acceptable use of the GBPS's Information Technology (I.T.) resources is based on the following principles:

All the GBPS's I.T. resources and any information stored on them remain the property of the GBPS or in case were-by employer has shipped their equipment remains their property trusted to us.

Users must ensure that they use Information Technology (I.T.) resources at all times in a manner which is lawful, ethical and efficient.

Users must respect the rights and property of others, including privacy, confidentiality and intellectual property.

Users must respect the integrity and security of the GBPS's Information Technology (I.T.) resources.

4.2 Monitoring

The GBPS reserves the right to routinely monitor, log and record any and all use of its Information Technology (I.T.) resources for the purpose of:

1) Helping to trace and resolve technical faults.
2) Protecting and maintaining network and system security.
3) Maintaining system performance and availability.
4) Ensure the privacy and integrity of information stored on the GBPS network.
5) Investigating actual and suspected security incidents.
6) Preventing, detecting and minimizing inappropriate use.
7) Protecting the rights and property of the GBPS, its staff, patients and clients.
8) Ensuring compliance with GBPS policies, current legislation and applicable regulations.

Routine monitoring reports inclusive of Web Sites accessed history, harmful content and apps monitoring, downloads, machine new apps installed, will be kept by the GBPS IT in storage for at least 30 days after which they can be overwritten with fresh data.

While the GBPS does not routinely monitor an individual user's use of its Information Technology (I.T.) resources it reserves the right to do so when a breach of its policies or illegal activity is suspected.

The extensive monitoring of an individual user will only be undertaken at the request of the individual's line manager in agreement with HR Directorate. The monitoring may include, but will not be limited to individual login sessions, details of information systems and records accessed, contents of hard disks, internet sites visited, time spent on the internet, telephone usage and the content of electronic communications.

GBPS will at all times seek to act in a fair manner and respect the individual

user's right for the privacy of their personal information.

Information collected through monitoring will not be used for purposes other than those for which the monitoring was introduced, unless it is clearly stated in the users interest to do so or it reveals activity that the GBPS could not be reasonably expected to ignore, for example a user found to be viewing, downloading or forwarding child pornography must be reported to HR immediately.

Individual monitoring reports will only be accessible to the appropriate authorized GBPS personnel and will be deleted when they are no longer required.

In the process of dealing with computer support calls GBPS ICT staff may need to access a user's computer to resolve the support call. In such circumstance's ICT staff must respect the privacy of the individual user and not access information, documents or emails of a personal nature without the user's permission or unless they need to in order to resolve the support call. In some cases, the ICT department may use remote control software to connect and take control of a user's computer remotely. In such circumstances the ICT staff will not use this software to connect to the user's computer without first attempting to contact the user of the computer first.

4.3 Personal Use

The GBPS's Information Technology (I.T.) resources are to be used primarily for the employer's work only business-related purposes. However, at the discretion of their line manager occasional personal use may be permitted by a user provided it:

1) Is not excessive;
2) Only taken at specific hours and time such as lunch hour breaks;
3) Does not take priority over their employer work responsibilities;
4) It does not interfere with the performance and work of the user, other staff or the GBPS;
5) Does not incur unwarranted expense or liability for the employer;
6) Does not have a negative impact on the employer in any way;
7) Does not involve commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit;
8) Is lawful and complies with this policy and all other relevant GBPS policies

4.4 Confidentiality and Privacy

GBPS is legally required to ensure the security and confidentiality of all personal information it processes on behalf of its staff, clients and patients in accordance to HIPAA standards.

In accordance with the ***GBPS information classification and handling policy*** (all GBPS information (irrespective of its format) must be classified, controlled and handled according to the sensitivity of its contents. Classification controls should take account of the organizational needs for sharing or restricting data and the associated impacts and risks (e.g. consequences if information is mishandled).

In the course of a user's work for GBPS, he/she may have access to, or hear information concerning the medical or personal affairs of GBPS staff, patients or clients. Such information irrespective of the format (i.e. paper, electronic or otherwise) is strictly confidential and must always be safeguarded.

Users must respect the privacy and confidentiality of information at all times. They must not access information or information systems unless they have a valid GBPS business related reason to do so or they have been granted permission by the information owner.

Users must not remove any confidential or restricted information (irrespective of format) from the GBPS facility they are employed at without the authorization of their line manager. Such authorization must be issued in advance of the first instance and may apply thereafter if necessary. Where a user has been authorized to remove confidential or restricted information from a GBPS facility they will be responsible for the safe transport and storage of the information and be held liable and accountable for it by signing non-disclosure agreements.

Confidential and restricted information must only be discussed or shared with others on a strict "need to know" basis.

Confidential and restricted information must only be discussed or shared with other GBPS staff or staff of a GBPS who have a valid GBPS business related reason and are authorized to have access to the information.

Confidential and restricted information must not be released and disclosed to third party commercial service providers. Their service provision is limited to what they can do and access if need be;

1) A signed contract in place with the GBPS for the provision of goods or services to the GBPS, and;

2) A valid legal and business reason for needing access our network (for example: they require access to the information in order to provide the goods or services to the GBPS), and;

3) Agreement that all activity will be monitored and scrutinized as they provide a service;

4) Signed a copy of the *GBPS Service Providers Confidentiality*

Agreement.

5) At no point and time any patient information is released, nor publicized, nor given to GBPS service providers in any way.

Confidential or restricted information (irrespective of the format) must not be copied, renamed, deleted or modified without the authorization of the information owner. This includes information on storage devices and information in transit.

Users must not remove from their GBPS employment location any confidential or restricted information, (irrespective of the format - paper, electronic or otherwise) belonging to the GBPS without the prior authorization of their line manager.

Personal information which is shared with others for purposes other than medical care, such as medical research or service planning must be first anonymized or pseudonymized otherwise the explicit consent of the patient or client is required.

Personal information belonging to GBPS staff, patients or clients must not be used for presentations, training or testing purposes unless it has first been anonymized or pseudonymized unless by the explicit consent of the employer, patients or clients is required.

4.5 User Access Accounts & Passwords

Where appropriate individual users will be granted access to GBPS's Information Technology (I.T.) resources which are necessary for them to perform their specific function for the GBPS.

Each authorized user will be assigned an individual user access account name and password set which they can use to access a particular GBPS Information

Technology (I.T.) resource. In some circumstances the use of generic / group access accounts is permitted (see section 4.3.3 of the *GBPS Access Control Policy*).

Each user is responsible for all activities performed on any GBPS I.T. device, information system or application while logged in under their individual access account and password.

Users must ensure all passwords assigned to them are kept secure in accordance with section 4.4 of the *GBPS Password Standards Policy*.

Users who suspect their password is known by others must change their password immediately.

Users and ICT department must ensure all default passwords which are supplied by a vendor for new GBPS I.T. devices and information systems are changed at installation time. Never at any time do we use default passwords and information from manufacturer.

All access to GBPS Information Technology (I.T.) resources must be controlled and managed in accordance with the *GBPS Access Control Policy.*

All passwords used to access GBPS Information Technology (I.T.) resources must be created and managed in accordance with the *GBPS Password Standards Policy*).

Computer passwords expire every 60 days. Email Passwords to be changed every 90 days. All passwords are complex minimum 8 words containing lowercase, uppercase, numbers and special characters/symbols.

4.6 Software and Electronic Media

Only software which has the correct and proper license may be installed and used within the GBPS organization.

Mobile and smart device application software (i.e. apps) must only be downloaded and installed on GBPS smart devices where there is a valid GBPS business reason and the software can add value to the users work.

All software and electronic media developed and purchased on behalf the GBPS remains the property of the GBPS and must not be used, copied, distributed or borrowed without authorization.

The ICT Directorate on behalf of the GBPS reserves the right to remove software at any time, for reasons including but not limited to (1) non-compliance with GBPS

policies, (2) non-compliance with HIPAA standards and protocols, (3) the software is not properly licensed, or (3) the software is found to have a negative impact on the performance of the GBPS network, systems or equipment.

4.7 GBPS I.T. Devices & Equipment

All GBPS I.T. devices and equipment must be purchased through agreed and approved channels, GBPS contract agreements, ICT framework agreements or directly through the ICT Directorate.

GBPS I.T. devices and equipment which has not been purchased through agreed channels must be approved by the ICT Directorate before being allowed to connect to the GBPS network.

All I.T. devices and equipment provided by the GBPS remain the property of the GBPS. Users must not remove or borrow GBPS I.T. devices or equipment without the authorization of their line manager. The security of any GBPS I.T. device and equipment borrowed is the responsibility of the borrower and the I.T. device and equipment must be returned by the borrower before they leave the employment or, at the request of the borrower's line manager or the ICT Directorate.

Users must not alter the hardware or software configuration of any GBPS I.T. device or equipment without the prior authorization of the ICT Directorate.

Users must take due care when using GBPS I.T. devices and equipment and take reasonable steps to ensure that no damage is caused to the I.T. device or equipment. They must not use I.T. devices and equipment (either in a GBPS facility, while traveling or at home) if they have reason to believe it is dangerous to themselves or others.

Users must report all damaged, lost or stolen GBPS I.T. devices and equipment to their line manager and the ICT Directorate.

Old and obsolete GBPS I.T. devices and equipment must be recycled in liason with ICT Directorate.

The ICT Directorate on behalf of the GBPS reserves the right to remove any I.T. devices and equipment from the network at any time, for reasons including but not limited to (1) non-compliance with GBPS policies, (2) the I.T. device or equipment does not meet approved specification and standard, or (3) the I.T. device or equipment is deemed to be interfering with the operation of the network.

4.8 Laptops, Mobile Computer Devices & Smart Devices

Users must ensure that GBPS laptops, mobile computer devices and smart devices provided to them are protected at all times. They must take all reasonable steps to ensure that no damage is caused to the device and the device is protected against loss or theft.

GBPS smart devices must only be issued to users who have signed a copy of the *GBPS Smart Device User Agreement.*

All GBPS smart devices must be registered with the ICT Directorate so that they can be routed through the GBPS network infrastructure and managed securely.

GBPS Laptops, mobile computer devices and smart devices must be hardware encrypted and password protected in accordance with the *GBPS Password Standards Policy.*

Passwords used to access GBPS laptops, mobile computer devices and smart devices must not be written down on the device or stored with or near the device.

In accordance with the *GBPS Encryption Policy* all GBPS laptops, mobile computer devices and smart devices must have GBPS approved encryption software installed or device encryption enabled prior to their use within the GBPS.

Confidential and restricted information must only be stored on a GBPS laptop, mobile computer device or smart device with the authorization of the user's line manager and awareness of IT Directorate. Such authorization must be issued in advance of the information being stored on the device. Where authorization has been granted only the minimum amount of confidential or restricted information must be stored on the device as is absolutely necessary for a given function to be carried out.

When working in the office GBPS laptops, mobile computer devices and smart devices must be physically secured and positioned in such a way as to minimize the risk of theft. When they have to be left unattended for any period of time and at the end of each working day the devices should be secured to a desk or some other stationary object using an appropriate locking mechanism (i.e. Laptop cable lock) or locked in the employee's drawer or the IT secure safe.

GBPS laptops, mobile computer devices and smart devices must not be left unattended at all times without locking them.

When traveling by car, GBPS laptops, mobile computer devices and smart devices should be stored securely out of sight when not in use. Avoid leaving the devices unattended in the boot of a car overnight.

When traveling by taxi, train or plane GBPS laptops, mobile computer devices and smart devices should be kept close to hand at all times. Avoid placing the devices in locations where they could easily be forgotten or left behind (i.e. in overhead racks or boots of taxis).

When using a GBPS laptop, mobile computer devices or smart device in a public place user need to take precautions to ensure the information on the device screen cannot be viewed by others.

Users should check before using their GBPS smart device to make and accept phone calls within GBPS premises and other secure facilities so as to ensure there is no interference with sensitive electronic medical equipment.

Users must ensure that all GBPS laptops, mobile computer devices and smart devices provided to them are not accessed (including internet access) by persons who are not GBPS Staff (i.e. friends, family members and others etc)

Remote access connections to the GBPS network from a GBPS laptop, mobile computer devices or smart device must be made in accordance with the *GBPS Remote Access Policy*

4.9 GBPS Network

Access to GBPS network domains and network resources is controlled and managed in accordance with the *GBPS Access Control Policy*

Access rights and privileges to the GBPS network domains and network resources will be allocated based on the specific requirement of a user's GBPS role / function, rather than on their status

Access to GBPS network domains will generally be controlled by the use of individual user access account's, however in certain circumstances the use of generic or group accounts maybe permitted (see section 4.3.3 of the *GBPS Access Control Policy*).

Remote access connections to GBPS network domains and network resources will be granted and approved in accordance the *GBPS Remote Access Policy*.

Where there is a business need and with the approval of a GBPS information owner or his/her nominee, third party commercial service providers may request and be granted local access (on-site) and/or remote access to the GBPS network domains and information systems. Such access request should be managed in accordance with the *GBPS Access Control Policy*.

Third party commercial service providers who are granted local access (on-site) and/or remote access to the GBPS network domains and information systems must sign a copy of the *GBPS Third Party Network Access Agreement*.

Users must not:

1) Disconnect any GBPS I.T. devices, equipment or removable storage devices to or from a GBPS network domain without the prior authorization of the ICT Directorate.

2) Connect any GBPS I.T. devices and equipment, laptop or smart device to an external network without the prior authorization of the ICT Directorate.

3) Connect any I.T. devices and equipment, laptop, smart device, mobile phone device or removable storage device which is their personal property and is not owned or leased by the GBPS to a GBPS network domain without the prior authorization of the ICT Directorate

All activity on GBPS network domains is routinely monitored, logged and recorded for the purposes of helping to trace and resolve technical faults and investigating actual and suspected security breaches (See section 4.2).

4.10 Email

All email use within the GBPS is governed by requirements of the *GBPS Electronic Communications Policy*.

4.11 Internet

All internet use within the GBPS is governed by requirements of the *GBPS Electronic Communications Policy*.

Internet access is only by obtaining a username and password from ICT department. User will not be able to access any resource without it.

MAC Address of the actual device is also required to grant the user internet access. User Internet Protocol (IP) is always reserved for increased security.

User machine is controlled by port access on the switch for advanced security.

4.12 Telephone System

Access to the GBPS telephone system is primarily intended for GBPS work related purposes. The making and taking of personal calls is not allowed and prohibited at any level.

Users must respect the privacy of others at all times and not attempt to access calls where the user is not the intended recipient or log into voice mail accounts that the user is not expressly authorized to access.

The use of GBPS mobile phone devices is governed by the requirements of the *GBPS Mobile Phone Device Policy.*

The use of GBPS fax via Ring Central is governed by the requirements of the *GBPS Electronic Communications Policy*.

4.13 Information Backup

Where an agreement exists between the ICT Directorate and the information owner, GBPS network servers will be automatically backed up on a daily basis with 7-day retention period to prevent corrupt backup copies.

GBPS backups are highly and heavily encrypted from the user's machine to the server. The server then adds another layer of encryption in preparation to a cloud off site backup.

Information backups especially those containing confidential and restricted information must be stored securely in a locked drawer, filing cabinet or safe.

Information backups should be regularly tested to ensure that a recovery can take place following an incident or hardware/software failure.

4.14 Virus & Malicious Software Protection

To protect the GBPS from computer viruses and other malicious software, no electronic document or file from any source outside of the GBPS should be opened unless it has first been scanned for known viruses and malicious software. This requirement covers electronic files in any format, including floppy disks, CD's, DVD's and email attachments.

The ICT Directorate will ensure virus scanning software is available on every GBPS desktop and laptop computer device that is connected to the GBPS network and undertake the regular updating of such virus scanning software. Due to their nature standalone desktop computers and laptops which are not regularly connected to the GBPS network are unlikely to have fully up to date virus protection. Users of these computer devices must contact the ICT Directorate at least once a month and have their virus scanning software updated manually.

The ICT Directorate is not responsible for supplying or updating virus scanning software on computer devices which are not owned or leased by the GBPS.

Users who receive a virus warning message should send it to the ICT Directorate to determine the authenticity of the warning. Under no circumstances should they forward it on to other users, neither respond to the sender with any information without consultation.

4.15 Information Storage

4.15.1 GBPS On-Site Server Storage

For security and legal reason, the GBPS's preferred position is that:

1) All GBPS confidential or restricted information is stored on a GBPS network server.

2) All GBPS network servers hosting critical or national information systems, applications, databases, financial systems and management systems should be located within the GBPS's central hosting facility.

3) All other GBPS network servers which host GBPS information systems that process confidential or restricted information are located on-site within GBPS managed facilities.

4) All Users' folders are stored on the NAS with security and password access. Information from the NAS is directed to the server encrypted as a second backup copy. A 3rd backup copy is then sent to the GBPS secure cloud offsite with multiple encryptions.

GBPS network servers are reserved for the hosting/storage of GBPS business-related systems and information only. Any non-work-related data is not required to be stored on our servers.

4.15.2 GBPS On-Site Local Storage

When technical or business requirements necessitate a GBPS line manager may sanction the temporary storage/hosting of confidential information, restricted information or a GBPS information system on a GBPS computer device other than a GBPS network server.

Where confidential information, restricted information or a GBPS information system is stored/hosted on a local computer or removable storage device the user of the device and their line manager must ensure the following controls are implemented.

1) Where possible the computer or removable storage device is password protected in accordance with the *GBPS Password Standards Policy*.

2) The confidential and restricted information and/or the computer or removable storage device are encrypted in accordance with the *GBPS Encryption Policy*.

3) Only the minimum amount of confidential or restricted information's is as necessary for a specified task is stored on the computer or removable storage device;

4) The confidential and restricted information is regularly backed up and the backup copies are stored in a secure place and not with the computer or removable device;

5) The confidential and restricted information is deleted from computer or removable storage device when it no longer required.

GBPS approved encrypted USB memory sticks are available from the ICT Directorate to GBPS staff that have a requirement to temporarily store or transfer confidential or restricted information. The USB memory sticks will be issued to GBPS staff who have returned a signed copy of the *GBPS USB Memory Stick Usage Agreement* to their local ICT department.

Under no circumstance should unapproved USB memory sticks (encrypted or otherwise) be used to transfer or store GBPS information systems, confidential information or restricted information.

Removable storage devices and GBPS approved encrypted USB memory sticks except those used for backup purposes must not be used for the long-term storage of confidential or personal information.

Photographic, video and audio recordings which are taken as part of a patient's or client's treatment and care must be transferred from the recording device (i.e. digital camera, video camera, mobile phone, tape recorder etc.) onto a GBPS network server as soon as is practical. When the transfer is complete the photographic, video or audio recording on the recording device should be deleted. In the event that this cannot be carried out immediately the recording device should be locked away securely when not in use.

4.15.3 Third Party Storage Facilities

In special circumstances such as when business, technical (i.e. specialized system support etc), security (i.e. disaster recovery backup etc) or legal (i.e. archiving,) requirements necessitate GBPS confidential or restricted information and/or information systems maybe physically stored off-site at a third party storage facility or hosted off-site on third party servers and equipment.

Where GBPS confidential information, restricted information or information systems are physically stored off-site at a third party storage facility or hosted off-site on third party servers and equipment the GBPS's preferred position is that third party storage facility, servers and equipment are (1) located within the U.S.A or failing that, (2) they are located within a country which is a member of the European Economic Area (EEA).

In exceptional circumstances the GBPS may consider requests to store / host GBPS confidential information, restricted information or information systems on third party servers and equipment which are located in a country outside the European Economic Area (EEA). Each request will be evaluated on a case by case basis and will take into account the sensitivity of the information involved, data protection law and any other legal issues, available alternatives, support issues, logistics and the security controls in place.

The storage / hosting of GBPS confidential and restricted information and information systems off-site at third party storage facilities or on third party servers and equipment must be approved by the relevant information owner.

GBPS confidential information, restricted information and information systems may only be stored /hosted off-site at third party storage facilities or on third party servers and equipment, when:

1) The GBPS has satisfied its self that the third party storing / hosting the GBPS information and information systems has the appropriate human, organizational and technological controls in place to protect the GBPS information and information systems against unauthorized access and disclosure, accidental loss, destruction, deterioration, damage and alteration, and;

2) A signed legal contract exists between GBPS and the third party governing the processing or storage of the GBPS information and/or information systems, and;

3) The third party has signed a copy of the *GBPS Service Provider Confidentiality Agreement*.

4.15.4 Storage on Personal I.T. Devices & Equipment

Users are strictly prohibited from hosting/storing GBPS confidential information, restricted information or information systems on any computer device, mobile computer device, smart device, mobile phone device, removable storage device, photographic, video or audio recording device or any other equipment which is their personal property and is not owned or leased by the GBPS.

4.16 Physical Security

GBPS I.T. devices and equipment must be physically secured and positioned in such a way as to minimize the risk of unauthorized individuals accessing the device or viewing information displayed on the device screen.

4.16.1 GBPS Network Servers & data communications Equipment

In circumstances where for technical or business reasons GBPS network servers hosting critical clinical information systems, applications, databases, financial systems or management systems are hosted locally, the servers should be located within an accessed controlled area on-site (i.e. a server / comms room or a locked room) which is only accessible to authorised GBPS staff.
GBPS local file and print servers should be located within an accessed controlled area on-site (i.e. a server / comms room or a locked room) which is only accessible to authorised GBPS staff.

Critical GBPS network and data communication equipment (for example, switches, routers, hubs, patch panels etc.) should be placed in communications racks or cabinets and located within accessed controlled areas (i.e., a server / comms room or a locked room) which are only accessible to authorised GBPS staff.

Power and communications cabling carrying data or supporting key information systems should be protected from interception and damage.

Local server / comms rooms or other areas housing GBPS network servers and/or network and data communication equipment situated on the ground floor should have all windows kept shut or where possible have shutters installed on the windows.

All non GBPS staff given access to local server / comms rooms or other areas housing GBPS network servers and/or network and data communication equipment must be accompanied by an authorized GBPS staff member throughout their visit.

Hazardous and combustible materials must not be stored within or near GBPS local server / comms rooms or other areas housing GBPS network servers and/or network and data communication equipment.

4.16.2 GBPS Computers & Peripheral Devices

Users should operate a clear screen policy and log off or ‘lock’ their GBPS computer (using *Ctrl+Alt+Delete* keys) when they have to leave it unattended for any period of time and within breaks.

Where practical users should operate a clear desk policy and clear their desks of all confidential and restricted information (irrespective of the format) at the end of each working day or when leaving their workplace for a major part of the day,

Removable storage devices, GBPS approved USB memory sticks, mobile phone devices, laptops, smart devices and photographic, video and audio recording devices should be stored away in a locked cabinet or drawer when not in use.

Where possible, fax machines, printers, scanners and photocopiers which are used to regularly fax, print, scan or copy confidential or restricted information should be located within areas which are not accessible by the general public.

Confidential and restricted information, when faxed, printed, scanned or copied should where practical be collected from the fax machine, printer, scanner or photocopier immediately.

4.17 Information Transfer

Transfer(s) of confidential or restricted information to third parties must be authorised by a GBPS line manager (()). Such authorization must be issued in advance of the first instance and may apply thereafter if necessary.

Where it is necessary to transfer confidential or restricted information to third parties, only the minimum amount of information should be transferred as is necessary for a given task to be carried out.

Where possible all transfer(s) of confidential and restricted information should take place electronically via secure channels (i.e. Secure FTP, TLS, VPN etc.) or encrypted email.

In circumstances where electronic transfer is not possible, confidential or restricted information may be transferred manually using a removable storage device provided the removable storage device or the information is encrypted in accordance with the requirements of the *GBPS Encryption Policy*. Where possible the removable storage device should be hand delivered by a GBPS staff member to the intended recipient. If this is not possible the removable storage device should be posted to the intended recipient and the intended recipient contacted within a couple of days to confirm they have received the information on the removable storage device. When sending bulk confidential or personal data by post to the same address the use of registered post or some other secure and certifiable delivery method must be used.

4.18 Information Disposal

Confidential and restricted information must be securely deleted when it is no longer required.

All traces of confidential and restricted information must be purged from old GBPS computers, smart devices, mobile computer devices, mobile phone devices and removable storage devices before they are reused within the GBPS, sold to staff, donated to charity or recycled.

The simple deletion or formatting of information stored on a device is not sufficient to remove all traces of the information. The information must be purged by either (1) using special sanitation software to overwrite the information a number of times, or (2) the hard disk must be degaussed (i.e. information is permanently purged using a powerful magnet) or (3) the physical destruction of the media (i.e. hard disk, magnetic tape, video & audio tapes, CD/DVD's, etc) the information is stored on.

Photocopiers and scanners which are fitted with hard disks must be purged of all confidential and personal data before they are disposed of or returned to the vendor.

Computers and other I.T. equipment which are leased from third parties must be purged of all confidential and personal data before being returned to the third-party leasing company.

Where the disposal of old GBPS computer equipment and removable storage devices is outsourced to a commercial service provider the commercial service provider must:

1) Ensure the operation of purging the computer equipment of all confidential and restricted information and the destruction of the media (i.e. hard disk, magnetic tape, video & audio tapes, CD/DVD's, etc) is carried out on-site at a GBPS facility before the equipment is taken off-site to a licensed recycling facility within U.S.A.

2) Provide the GBPS with a certificate of disposal / destruction for all the equipment that was disposed of / destroyed by them.

3) Signed a copy of the *GBPS Service Providers Confidentiality Agreement.*

4.19 Working from Home (Home Working)

Users who are authorised by the GBPS to work from home (home workers) must take all reasonable measures to ensure all the GBPS computer devices provided to them are kept secure and are protected against unauthorized access, damage, loss, theft and computer viruses.

Users who work from home must ensure:

1) All work carried out by them on behalf of the GBPS while working at home is processed and stored on a GBPS computer device and not any other device which is their personal property or the personal property of another household member;

2) All GBPS computer devices used by them to work from home are password in accordance with the *GBPS Password Standards Policy*.

3) All GBPS computer devices used by them to work from home have GBPS approved encryption software installed;

4) All GBPS computer devices used by them to work from home have GBPS approved anti-virus software installed and this is kept up to date;

5) All confidential and restricted information which is accessed by them or stored on a GBPS computer device provided to them is kept secure and confidential at all times;

6) All GBPS computer devices and information provided to them are not accessed (including internet access) by members of their family, other household members or visitors;

7) All GBPS computer devices and information (irrespective of the format) are securely locked away when not in use;

8) All remote access connections made from the home workers computer devices to the GBPS network are made in accordance with the *GBPS Remote Access Policy;*

9) All old printouts, faxes and other paper-based records that contain confidential or restricted information are shredded or disposed of securely and are not disposed along with their ordinary household rubbish;

All computer devices provided by the GBPS remain the property of the GBPS and must be returned to the GBPS by the home worker before they leave the employment of the GBPS or at the request of their GBPS line manager or the ICT Directorate.

4.20 Periods of Absence

During planned periods of absence such as career breaks, holidays, on training courses or working off-site for an extended period of time, users should ensure wherever possible that their line manager or work colleagues have access to important GBPS business related documents and email messages stored on their computer so that there is no disruption to service delivery.

During unplanned periods of absence such as ill health, or where a user has forgotten to provide access to their line manager or work colleagues, the user's line manager may be permitted to access their computer to retrieve GBPS business related documents or emails messages so as to minimize any disruption to service delivery. In such circumstances line managers must respect the privacy of the user and not access documents or emails of a personal nature unless there are compelling conditions that warrant doing so.

4.21 Users leaving the GBPS & User Transfers

Users must return all GBPS mobile phone devices and accessories (e.g. mobile phone car kit and battery charger etc.), computer equipment (e.g. laptop, smart devices, printers, 3G cards, removable storage devices, USB memory sticks etc), information (i.e. documents, files, important email messages etc.) and other important items (e.g. swipe cards, keys, parking permit and I.D. badge etc) to their GBPS line manager before they leave the employment of the GBPS.

Line managers must contact the ICT department to ensure that the information system and network access accounts belonging to users leaving the employment of the GBPS are revoked immediately once they leave the organization. (see the *GBPS Access Control Policy*)

Users leaving the employment of the GBPS should also ensure they remove or delete all non-GBPS personal information & email messages (i.e. information / email messages which are of a personal nature and belong to the user and not the GBPS) from their GBPS mobile phone device and computer equipment before they

leave as it may not be possible to get a copy of this data once they have left the GBPS.

Users who are transferring internally within the GBPS must ensure they return all accessories, laptops, and swipe cards etc to their current GBPS line manager before they transfer. They must also ensure that their current line manager or work colleagues have access to important GBPS business related documents and email messages so that there is no disruption to service delivery after they transfer.

Line managers must contact the ICT department to ensure that access account privileges that are no longer required by a user as a result of them transferring internally within the GBPS are removed. (see the *GBPS Access Control Policy*)

4.22 Information Security Breach

Information security breaches include but are not limited to the following (1) the loss or theft of a computer device containing confidential or restricted information, (2) the loss or theft of a photographic, video or audio recording device containing confidential or restricted information, (3) the loss or theft of a USB memory stick or some other form of removable storage device containing confidential or restricted information, (4) the transmitting of confidential or restricted information by fax or email to an incorrect fax number or email address, (5) incidents where confidential or restricted information was mistakenly or otherwise disclosed to unauthorized persons.

Users must report all actual or suspected information security breaches immediately to their line manager, the ICT Directorate and/or the Consumer Affairs section.

Information security breaches must be managed in accordance with the *GBPS Data Protection Breach Management Policy*.

4.23 Unacceptable Use

The GBPS's Information Technology (I.T.) resources must not be used:

1) For personal use;
2) For commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit;
3) For political activities, such as promoting a political party / movement, or a candidate for political office, or campaigning for or against government decisions;
4) To knowingly misrepresent GBPS and the client;
5) To transmit confidential or restricted information outside the GBPS unless the information has been encrypted and transmission has been authorised by their GBPS line manager;
6) To store or transfer confidential or restricted information (encrypted or otherwise) onto an **unapproved** USB memory stick;
7) To enter into contractual agreements inappropriately (i.e. without authorization or where another form of agreement is required);
8) To create, view, download, host or transmit material (other than users who are authorised by GBPS to access such material for research etc.) of a pornographic or sexual nature or which may generally be considered offensive or obscene and could cause offence to others on the grounds of race, creed, gender, sexual orientation, disability, age or political beliefs. material is defined as information (irrespective of format), images, video clips, audio recordings etc;
9) To retrieve, create, host or transmit material which is designed to cause annoyance, inconvenience or needless anxiety to others;
10) To retrieve, create, host or transmit material which is defamatory;
11) For any activity that would infringe intellectual property rights (e.g. unlicensed installation, distribution or copying of copyrighted material);
12) For any activity that would compromise the privacy of others;
13) For any activity that would intentionally cause disruption to the computer systems, telephone systems or networks belonging to GBPS or others;
14) For any activity that would deliberately cause the corruption or destruction of data belonging to GBPS or others;
15) For any activity that would intentionally waste the GBPS's resources (e.g. staff time and Information Technology (I.T.) resources);
16) For any activity that would intentionally compromise the security of the GBPS's Information Technology (I.T.) resources, including the confidentiality and integrity of information and availability of IT resources (e.g. by deliberately or carelessly causing computer virus and malicious software infection);
17) For the installation and use of software or hardware tools which could be used to probe or break GBPS I.T. security controls;

18) For the installation and use of software or hardware tools which could be used for the unauthorized monitoring of electronic communications within GBPS or elsewhere;

19) To gain access to information systems or information belonging to GBPS or others which you are not authorized to use;

20) For creating or transmitting “junk” or “spam” emails. This includes but is not limited to unsolicited commercial emails, jokes, chain-letters or advertisements;

21) For any activity that would constitute a criminal offence, give rise to a civil liability or otherwise violate any law.

The above list should not be seen as exhaustive, as other examples of unacceptable use of the GBPS’s I.T. resources may exist.

GBPS has the final decision on deciding what constitutes personal use.

5.0 Roles & Responsibilities

5.1 ICT Directorate

The ICT Directorate is responsible for:

The provision of reliable computer systems which deploy appropriate technical safeguards against threats to their availability, operation, stability, and performance;

The management and security of GBPS network (LAN/WAN);

The provision of facilities for information backups on GBPS network file servers and other centralized information stores but excluding backups of the hard disks on individual computers;

The provision and management of anti-virus/spyware software throughout GBPS.

The provision, deployment and management of encryption facilities throughout GBPS.

The provision of additional security measures to enable use of computer systems outside the normal working environment when this is appropriate and necessary;

The procurement of all IT networking equipment, software and services;

The installation of all software;

The installation of all IT equipment, including connection to GBPS network;

The provision of training, advice and guidance to computer systems users.

5.2 Information Owners

Information owners are responsible for:

The implementation of this policy and all other relevant policies within GBPS directorate or service they manage;

The ownership, management, control and security of the information processed by their directorate or service on behalf of GBPS;

The ownership, management, control and security of GBPS information systems used by their directorate or service to process information on behalf of GBPS;

Maintaining a list of GBPS information systems and applications which are managed and controlled by their directorate or service.

Making sure adequate procedures are implemented within their directorate or service, so as to ensure all GBPS staff, students, contractors, sub-contractors, agency staff and third-party commercial service providers that report to them are made aware of and are instructed to comply with this policy and all other relevant policies;

Making sure staff that report to them are provided with adequate training so as to ensure on-going compliance of this policy and all other relevant policies;

5.3 Line Managers & Human Resources Directorate

Line managers & H.R are responsible for:

The implementation of this policy and all other relevant GBPS policies within the business areas for which they are responsible;

Ensuring that all GBPS staff, students, contractors, sub-contractors and agency staff who report to them are made aware of and have access to this policy and all other relevant GBPS policies;

Ensuring that all GBPS staff, students, contractors, sub-contractors and agency staff who report to them are provided with adequate training and are instructed to comply with this policy and all other relevant GBPS policies;

Ensuring staff, students, contractors, sub-contractors and agency staff who report to them return all GBPS computer devices (e.g. laptop, smart devices, printer, mobile phone devices, removable storage devices etc), information, important email messages and other important items (e.g. swipe cards, keys and I.D. badge

etc) before they leave the employment of the GBPS or transfer to another GBPS directorate or service area;

Reporting all actual or suspected information security breaches immediately to the ICT Directorate and/or the Consumer Affairs section;

Consulting with the HR Directorate in relation to the appropriate procedures to follow when a breach of this policy has occurred.

5.4 Users

Each user of GBPS's I.T. resources is responsible for:

Complying with the terms of this policy and all other relevant GBPS policies, procedures, regulations and applicable legislation;

Respecting and protecting the privacy and confidentiality of the information systems and network they access, and the information processed by those systems or networks;

Ensuring they only use user access accounts and passwords which have been assigned to them;

Ensuring all passwords assigned to them are kept confidential at all times and not shared with others;

Complying with instructions issued by designated information owners, system administrators, network administrators and/or the ICT Directorate on behalf of the GBPS;

Reporting all lost, stolen or damaged I.T. devices to their line manager and the ICT Directorate;

Reporting all actual or suspected information security breaches immediately to their line manager, the ICT Directorate and/or the Consumer Affairs section;

Reporting all misuse and breaches of this policy to their line manager;

Ensuring they return to their line manager, all GBPS computer devices (e.g. laptop, smart devices, printer, mobile phone devices, removable storage devices etc), information, important email messages and other important items (e.g. swipe cards, keys and I.D. badge etc) before they leave the employment of the GBPS or transfer to another GBPS directorate or service area.

Ensuring they remove or delete all non-GBPS personal information and email messages (i.e. information which is of a personal nature and belongs to the user and not the GBPS) from their GBPS computer before they leave the employment of the GBPS, as it may not be possible to get a copy of this data from the GBPS once the user has left the GBPS.

5.5 Network Administrators

Each GBPS network administrator is responsible for:

Complying with the terms of this policy and all other relevant GBPS policies, procedures, regulations and applicable legislation.

5.6 System Administrators

Each GBPS system administrator is responsible for:

Complying with the terms of this policy and all other relevant GBPS policies, procedures, regulations and applicable legislation;

Complying with instructions issued by the ICT Directorate on behalf of the GBPS.

6.0 Enforcement

The GBPS reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. GBPS staff, students, contractors, sub-contractors or agency staff who breach this policy maybe subject to disciplinary action, including suspension and dismissal as provided for in the GBPS disciplinary procedure.

Breaches of this policy by a third-party commercial service provider, may lead to the withdrawal of GBPS information technology resources to that third-party commercial service provider and/or the cancellation of any contract(s) between the GBPS and the third-party commercial service provider.

7.0 Review & Update

This policy will be reviewed and updated annually or more frequently if necessary to ensure any changes to the GBPS's organization structure and business practices are properly reflected in the policy.

Appendix A

Anonymized / Anonymization: The process of rendering data into an irrevocable form which does not identify any individual and can no longer be linked to an individual.

Authorization / Authorised: Official GBPS approval and permission to perform a particular task.

Backup: The process of taking copies of important files and other information stored on a computer to ensure they will be preserved in case of equipment failure, loss or theft etc.

Breach of Information Security: The situation where GBPS confidential or restricted information has been put at risk of unauthorized disclosure as a result of the loss or theft of the information or, through the accidental or deliberate release of the information.

Confidential information: (As defined by the *GBPS Information Classification & Handling Policy*) Information which is protected by Irish and/or E.U. legislation or regulations, GBPS policies or legal contracts. The unauthorized or accidental disclosure of this information could adversely impact the GBPS, its patients, its staff and its business partners. Some examples of confidential information include:

Patient / client / staff personal data (Except that which is restricted)
Patient /client / staff medical records (Except that which is restricted)
Unpublished medical research
Staff personal records
Financial data / budgetary Reports
Service plans / service performance monitoring reports
Draft reports
Audit reports
Purchasing information
Vendor contracts / Commercially sensitive data
Data covered by Non-Disclosure Agreements
Passwords / cryptographic private keys
Data collected as part of criminal/HR investigations
Incident Reports

Defamatory: False statement or series of statements which affect the reputation of a person or an organization.

Electronic Media: Any Information that has been created and is stored in an electronic format, including but not limited to software, electronic documents, photographs, video and audio recordings.

Encryption / Encrypt: The process of converting (encoding) information from a readable form (plain text) that can be read by everyone into an unreadable form (cipher text) that can only be read by the information owner and other authorised persons.

Encryption Key: A piece of data (parameter usually a password) used to encrypt/decrypt information.

Generic / Group Access Account: An access account that is intended for use by a number of different people and not an individual user and as such is not derived from a single user's name.

Home Working: The situation where GBPS staff carry out their contractual obligations (either on an occasional or regular basis) on behalf of the GBPS while working from their home instead of a GBPS facility.

Home Worker(s): GBPS Staff are authorised to work from their home (on an occasional or regular basis) instead of a GBPS facility.

GBPS Network: The data communication system that interconnects different GBPS Local Area Networks (LAN), Wide Area Networks (WAN) and Wi-Fi Wireless Networks.

GBPS Server: A computer on the GBPS network used to provide network services and/or manage network resources.

Information: Any data in an electronic format that is capable of being processed or has already been processed.

Information Owner: The individual responsible for the management of a GBPS directorate or service (GBPS RDO or National Director (or equivalent)).

Information System: A computerized system or software application used to access, record, store, gather and process information.

Information Technology (I.T.) resources: Includes all I.T. devices and equipment, computer facilities, networks, data & telecommunications systems, equipment and infrastructure, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords, and information and data that are owned or leased by the GBPS.

Intellectual Property: Any material which is protected by copyright law and gives the copyright holder the exclusive right to control reproduction or use of the material. For example - books, movies, sound recordings, music, photographs software etc.

Line manager: The individual a user reports directly to.

Mobile Computer Device: Any handheld computer device including but not limited to laptops, tablets, notebooks, PDA's etc.

Mobile Phone Device: Any wireless telephone device not physically connected to a landline telephone system. Including but not limited to mobile phones, smart phone devices (for example, Apple iPhones, Windows Mobile enabled devices, Google Android enabled devices, Nokia Symbian enabled devices, Blackberry RIM enabled devices etc). This does not include cordless telephones which are an extension of a telephone physically connected to a landline telephone system.

Network Administrators: These are the individuals responsible for the day to day management of a GBPS network domain. Also includes GBPS personnel who have been authorised to create and manage user accounts and passwords on a GBPS network domain

Network Domain: A set of connected network resources (Servers, Computers, Printers, Applications) that can be accessed and administered as group with a common set of rules

Personal Information: Information relating to a living individual (i.e. GBPS Staff, or patient or client) who is or can be identified either from the information or from the information in conjunction with other information. For example: - an individual's name, address, email address, photograph, date of birth, fingerprint, racial or ethnic origin, physical or mental health, sexual life, religious or philosophical beliefs, trade union membership, political views, criminal convictions etc.

Personal Use: The use of the GBPS's Information Technology (IT) resources for any activity(s) which is not GBPS work-related.

Pornography / Pornographic: The description or depiction of sexual acts or naked people that are designed to be sexually exciting.

Privacy: The right of individual or group to exclude themselves or information about themselves from being made public.

Process / Processed / Processing: Performing any manual or automated operation or set of operations on information including:

Obtaining, recording or keeping the information;
Collecting, organizing, storing, altering or adapting the information;
Retrieving, consulting or using the information;
Disclosing the information or data by transmitting, disseminating or otherwise making it available;
Aligning, combining, blocking, erasing or destroying the information.

Pseudonymized / Pseudonymization: Is a process which involves the replacement of all personal identifiers (i.e. an individual's name address etc) contained within information with artificial identifiers (for example replacing an individual's name and address with

their initials or some other code etc). The purpose of pseudonymization is to make it difficult for any unauthorized third parties to identify any individual(s) from the information, but to allow the organization who pseudonymized the information in the first place to trace back the information to its origins.

Removable Storage Device: Any optical or magnetic storage device or media, including but not limited to floppy disks, CD, DVD, magnetic tapes, ZIP disk, USB flash drive (i.e. memory stick/pen/keys), external/portable hard drives.

Restricted Information: (As defined by the *GBPS Information Classification & Handling Policy*) Highly sensitive confidential information**.** The unauthorized or accidental disclosure of this information would seriously and adversely impact the GBPS, its patients, its staff and its business partners. Some examples of restricted information include:

Patient / client / staff sensitive restricted information (i.e. mental health status, HIV status, STD/STI status etc)
Childcare / Adoption information
Social Work information
Addiction Services information
Disability Services information
Unpublished financial reports
Strategic corporate plans
Sensitive medical research

Smart Device: A handheld mobile computer device which is capable of wireless connection (via Wi-Fi, 3G, 4G etc.), voice and video communication and, internet browsing. (for example: Apple IOS enabled devices (i.e. iPhone & iPad), Google Android enabled devices (i.e. Samsung Galaxy tablet), Windows Mobile enabled devices and, Blackberry RIM enabled devices etc)

Social Media: The name given to various online technology tools that enable people to communicate easily via the internet to share information and resources. It includes the following types of web sites:

1) **Internet Chat Rooms:** Websites that allow interactive messaging, where users can exchange views and opinions in real time on a variety of subject matters.

2) **Internet Discussion Forums/Message Boards:** Websites that allow users to participate in on-line discussions on a particular subject matter.

3) **Internet Social Networking Websites:** Websites that allow users to build on-line profiles, share information, pictures, blog entries and music clips etc. Including but not limited to Bebo, Facebook, Twitter, Myspace, Friendster, Whispurr, LinkedIn and Viadeo.

4) **Internet Video Hosting/ Sharing Websites:** Websites that allows users to upload video clips, which can then be viewed by other users. Including but not limited to Youtube, Yahoo Video, Google Video and MyVideo.

5) **Blogging Websites:** Websites that allow a user to write an on-line diary (known as a blog) sharing their thoughts and opinions on various subjects

Software: A computer program or procedure that enables a computer to perform a particular task.

System Administrators: The individual(s) charged by the designated system owner with the day to day management of GBPS information systems. Also includes the GBPS personnel and third parties who have been authorised to create and manage user accounts and passwords on these applications and systems.

Third Party Commercial Service Provider: Any individual or commercial company that have been contracted by the GBPS to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, data management services, patient / client care and management services etc.) to the GBPS.

Third Party Servers and Equipment: Any servers or computer equipment used to store or host GBPS information and/or information systems which are not owned by the GBPS.

Third Party Storage Facilities: Any location or facility used to store GBPS information, information systems and/or computer equipment which is not owned or managed by the GBPS.

Users: Any authorized individual who uses the GBPS's I.T. resources.

Ring Central: Software for VOIP phone system and fax.

ENCRYPTION POLICY

VERSION **2.0** REVISED JUNE 2019

This policy maybe updated at any time(without notice) to ensure changes to the GBPS organizationstructure and/or business practices are properly reflected in the policy.

GLOBAL BP
SOLUTIONS,LLC

Reader Information

Title:	GBPS (Global BP Solutions) Encryption Policy.
Purpose:	To define the acceptable of use and management of encryption throughout the GBPS.
Author:	Information Security Team (IST).
Target Audience:	All users (including GBPS staff, interns, contractors, sub-contractors, agency staff and authorized third party commercial service providers) of the GBPS's I.T resources.
Superseded Documents:	All local encryption policies and procedures.
Related Documents:	GBPS Information Security Policy. GBPS Information Technology Acceptable Use Policy. GBPS Electronic Communications Policy. GBPS Password Standards Policy.

Document History

Version	Owner	Author	Publish Date
1.0	GBPS	GBPS Information Security Team (IST)	April 2019
2.0	GBPS	GBPS Information Security Team (IST)	June 2019

1.0 Purpose

The purpose of this policy is to define the acceptable use and management of encryption software and hardware throughout the Global BP Solutions (GBPS).

This policy is mandatory and by accessing any Information Technology (I.T.) resources which are owned or leased by the GBPS, users are agreeing to abide by the terms of this policy.

2.0 Scope

This policy represents the GBPS's national position and takes precedence over all other relevant policies which are developed at a local level. The policy applies to:

All Information Technology (I.T.) resources provided by the GBPS;

All users (including GBPS staff, students, contractors, sub-contractors, agency staff and authorized third party commercial service providers) of the GBPS's I.T resources;

All connections to (locally or remotely) the GBPS network Domains (LAN/WAN/Wi-Fi);

All connections made to external networks through the GBPS network.

3.0 Definitions

A list of terms used throughout this policy are defined in *appendix A*.

4.0 Policy

4.1 Principles of Encryption

Where possible all confidential and restricted information must be stored on a secure GBPS network server with restricted access. Where it has been deemed necessary by a GBPS line manager (or equivalent) or above) and IT Directorate to store confidential or restricted information on any device other than a GBPS network server the information must be encrypted.

All confidential and restricted information transmitted via email to an email address or domain must be encrypted.

All passwords used as part of the process to encrypt/decrypt information must meet the requirements of the *GBPS Password Standards Policy*.

4.2 Servers

Confidential and restricted information stored on shared GBPS network servers which are situated in physically insecure locations (For example remote file/print servers) must be protected by the use of strict access controls and encryption. software.

4.3 Desktop Computers

All desktop computers will need to have encryption software installed:

1) Desktop computers which for business, geographic or technical reasons need to permanently store confidential or restricted information locally on the computer's hard drive (as opposed to a secure GBPS network server).

2) Desktop computers which for business, geographic or technical reasons need to permanently host client information systems (for example, MS Access, Excel etc.) that process confidential or restricted information locally on the computer's hard drive (as opposed to a secure GBPS network server).

3) Desktop computers used by GBPS staff to work from home (home working).

The preferred method of encryption for GBPS desktop computer devices is whole disk encryption.

4.4 Laptop, Mobile Computer & Smart Devices

All GBPS laptop computer devices must have GBPS approved encryption software installed prior to their use within the GBPS. In addition to encryption software the

laptop must be password protected and have up to date anti-virus software installed.

GBPS mobile computer devices & smart devices must have device encryption enabled or GBPS approved encryption software installed prior to their use within the GBPS.

The preferred method of encryption for laptop computers, mobile computer devices and smart devices is whole disk encryption. Mobile computer devices and smart devices which are not capable of whole disk encryption must use file/folder level encryption to encrypt all confidential and restricted information stored on the device.

Laptop, mobile computer devices and smart devices must not be used for the long-term storage of confidential and restricted information.

4.5 Removable Storage Devices

All confidential and restricted information stored on removable storage devices must be encrypted. In addition to being encrypted, removable storage devices must be stored in a locked cabinet or drawer when not in use preferably the I.T safe.

Removable storage devices except those used for backup purposes must not be used for the long-term storage of confidential and restricted information.

The preferred method of encryption for removable storage devices is whole disk/device encryption. Where whole disk encryption is not possible, then file/folder level encryption must be used to encrypt all confidential and restricted information stored on the removal storage device.

4.6 USB Memory Sticks

Confidential and restricted information may only be stored on **GBPS approved encrypted USB memory sticks** which are available from the ICT Directorate. The storage of confidential or restricted information on any other USB memory sticks (encrypted or otherwise) will be considered a breach of this policy.

GBPS approved USB memory sticks must only be used on an **exceptional** basis where it is essential to store or temporarily transfer confidential or restricted information. They must **not be used for the long-term storage of confidential or restricted information,** which must where possible be stored on a secure GBPS network server.

Confidential and restricted information stored on the GBPS approved USB memory stick must not be **transferred** to any internal machine (except a secure GBPS network server) or external system in an **unencrypted form**.

4.7 Transmission Security

All confidential or restricted information transmitted through email to an email address in-within/outside of the GBPS and client's domain must be encrypted. The transfer of such information outside of the GBPS domain must be authorized by a line manager with written confirmation archived by I.T Directorate. The authorization must be issued in advance of the first instance and will apply thereafter if necessary.

Where confidential and restricted information is transmitted through a public network (for example the internet) to an external third party the information must be encrypted first or sent via a secure channel (for example: Secure FTP, TLS, VPN etc). The transfer must be authorized by a line manager. The authorization must be issued in advance of the first instance and will apply thereafter if necessary.

All confidential and restricted information transmitted around existing wireless networks must be encrypted using WPA (Wi-Fi Protected Access) or better. All new wireless networks installations must be encrypted using WPA2 (Wi-Fi Protected Access) or better.

5.0 Roles & Responsibilities

5.1 ICT Directorate

The ICT Directorate is responsible for:

The selection and procurement of all encryption facilities used within the GBPS also applications with high ratings and recommended.

The provision, deployment and management of encryption facilities within the network.

The provision of training, advice and guidance on the use of encryption facilities within the GBPS on behalf of their clients;

5.2 Information Owners

Information owners are responsible for:

The implementation of this policy and all other relevant policies within the GBPS directorate or service they manage;

The ownership, management, control and security of the information processed by their directorate or service on behalf of the client;

The ownership, management, control and security of GBPS information systems used by their directorate or service to process information on behalf of the client;

Maintaining a list of information systems and applications which are managed and controlled by the directorate.

Making sure adequate procedures are implemented within their directorate or service, so as to ensure all GBPS employees, third parties and others that report to them are made aware of, and are instructed to comply with this policy and all other relevant policies;

Continuous implementation of procedures within their directorate or service to ensure compliance of this policy and all other relevant policies and governing bodies like HIPAA;

5.3 Users

Each user of the GBPS's IT resources is responsible for:

Complying with the terms of this policy and all other relevant GBPS policies, procedures, regulations and applicable legislation.

Respecting and protecting the privacy and confidentiality of the information they process at all times.

Complying with instructions issued by the ICT Directorate on behalf of the employer.

Ensuring all encryption passwords assigned to them are kept confidential at all times and not shared with others;

Ensuring encryption passwords used to access encrypted devices are not written down on the encrypted device or stored with or near the encrypted device;

Reporting all misuse and breaches of this policy to their line manager or ARM.

5.4 Line Managers with I.T Directorate

In addition to each user's responsibilities, line managers are directly responsible for:

The implementation of this policy and all other related GBPS policies within the business areas for which they are responsible.

Ensuring that all employees who report to them are made aware of and are instructed to comply with this policy and all other relevant GBPS policies.

Consulting with the HR Directorate in relation to the appropriate procedures to follow when a breach of this policy has occurred.

6.0 Approved Encryption Algorithms and Protocols at GBPS

6.1 Symmetric Key Encryption Algorithms

Triple Data Encryption Standard (3DES)
(Minimum encryption key length of 168 bits)

Advanced Encryption Standard (AES)
(Minimum encryption key length of 256 bits)

6.2 Asymmetric Key Encryption Algorithms

Digital Signature Standard (DSS)
Rivest, Shamir & Adelman (RSA)
Elliptic Curve Digital Signature Algorithm (ECDSA)

6.3 Encryption Protocols

IPSec (IP Security)
SSL (Secure Socket Layer)
SSH (Secure Shell) *(Only used and activated when there is a need and deactivated afterwards).*
TLS (Transport Layer Security)
S/MIME (Secure Multipurpose Internet Extension)

6.4 Encryption Key Management

Key management must be fully automated
Private keys must be kept confidential
Keys in transit and storage must be encrypted

7.0 Enforcement

We will take action as it deems appropriate against individuals who breach the conditions of this policy. GBPS staff, intern students, client facing employees, contractors, sub-contractors or agency staff who breach this policy maybe subject

to disciplinary action, including suspension and dismissal as provided for in the GBPS/HR disciplinary procedures.

Breaches of this policy by a third-party commercial service provider, may lead to the withdrawal of GBPS information technology resources to that third-party commercial service provider and/or the cancellation of any contract(s) between the GBPS and the third-party commercial service provider.

8.0 Review & Update

This policy will be reviewed and updated annually or more frequently if necessary, to ensure that any changes to the GBPS's organization structure and business practices are properly reflected in the policy. Latest technology as it comes out can lead to the review of this document accordingly.

Appendix A

Asymmetric Key Encryption Algorithms: A class of encryption algorithm in which two different keys are used: one for encrypting the information, and one for decrypting the information (Public-key encryption).

Authorization / Authorized: Official GBPS approval and permission to perform a particular task.

Confidential information: (As defined by the *GBPS information Classification & Handling Policy*) Information which is protected by Irish and/or E.U. legislation or regulations, GBPS policies or legal contracts. The unauthorized or accidental disclosure of this information could adversely impact the GBPS, its patients, its staff and its business partners. Some examples of confidential information include:

Patient / client / staff personal data (Except that which is restricted)
Patient /client / staff medical records (Except that which is restricted)
Unpublished medical research
Staff personal records
Financial data / budgetary Reports
Service plans / service performance monitoring reports
Draft reports
Audit reports
Purchasing information
Vendor contracts / Commercially sensitive data
Data covered by Non-Disclosure Agreements
Passwords / cryptographic private keys
Data collected as part of criminal/HR investigations
Incident Reports

Decryption / Decrypt: The process of decoding information which has been converted into an unreadable form (cipher text) back into a readable form (plain text).

GBPS Network: The data communication system that interconnects different GBPS Local Area Networks (LAN) and Wide Area Networks (WAN)

GBPS Network Server: A computer on the GBPS network used to manage network resources.

Home Worker(s): GBPS employee(s) who is authorised to work from their home (on an occasional or regular basis) instead of a GBPS facility.

Home Working: The situation where GBPS employees carry out their contractual obligations (either on an occasional or regular basis) on behalf of the GBPS while working from their home instead of a GBPS facility.

Information: Any data in an electronic format that is capable of being processed or has already been processed.

Information Owner: The individual responsible for the management of a GBPS directorate or service or equivalent.

Information Technology (I.T.) resources: Includes all computer facilities and devices, networks and data communications infrastructure, telecommunications systems and equipment, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords, and information and data that are owned or leased by the GBPS.

Mobile Phone Device: Any wireless telephone device not physically connected to a landline telephone system. Including but not limited to mobile phones, smart phone devices (for example, Apple iPhones, Windows Mobile enabled devices, Google Android enabled devices, Nokia Symbian enabled devices, Blackberry RIM enabled devices etc). This does not include cordless telephones which are an extension of a telephone physically connected to a landline telephone.

Personal information: Information relating to a living individual (GBPS employee, client and patient) who is or can be identified either from the information or from the information in conjunction with other information. For example: - an individual's name, address, email address, photograph, date of birth, fingerprint, racial or ethnic origin, physical or mental health, sexual life, religious or philosophical beliefs, trade union membership, political views, criminal convictions etc.

Process / Processed / Processing: Performing any manual or automated operation or set of operations on information including:

Obtaining, recording or keeping the information;
Collecting, organizing, storing, altering or adapting the information;
Retrieving, consulting or using the information;
Disclosing the information or data by transmitting, disseminating or otherwise making it available;
Aligning, combining, blocking, erasing or destroying the information.

Removable storage Device: Any optical or magnetic storage device or media including but not limited to floppy disks, CD, DVD, magnetic tapes, ZIP disk, USB flash drive (i.e. memory stick/pen/keys), external hard drives.

Restricted Information: (As defined by the *GBPS information Classification & Handling Policy*) Highly sensitive confidential information**.** The unauthorized or accidental

disclosure of this information would seriously and adversely impact the GBPS, its patients, its staff and its business partners. Some examples of restricted information include:

Patient / client / staff sensitive personal information (i.e. mental health status, HIV status, STD/STI status etc.)
Childcare / Adoption information
Social Work information
Addiction Services information
Disability Services information
Unpublished financial reports
Strategic corporate plans
Sensitive medical research

Smart Device: A handheld mobile computer device which is capable of wireless connection (via Wi-Fi, 3G, 4G etc.), voice and video communication and, internet browsing etc. (for example: Apple IOS enabled devices (i.e. iPhone & iPad), Google Android enabled devices (i.e. Samsung Galaxy tablet), Windows Mobile enabled devices and, Blackberry RIM enabled devices etc).

Symmetric Key Encryption Algorithms: A class of encryption algorithm in which the same key is used for both encryption and decryption of the information.

Third Party Commercial Service Provider: Any individual or commercial company that have been contracted by the GBPS to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, data management services, patient / client care and management services etc.) to the GBPS.

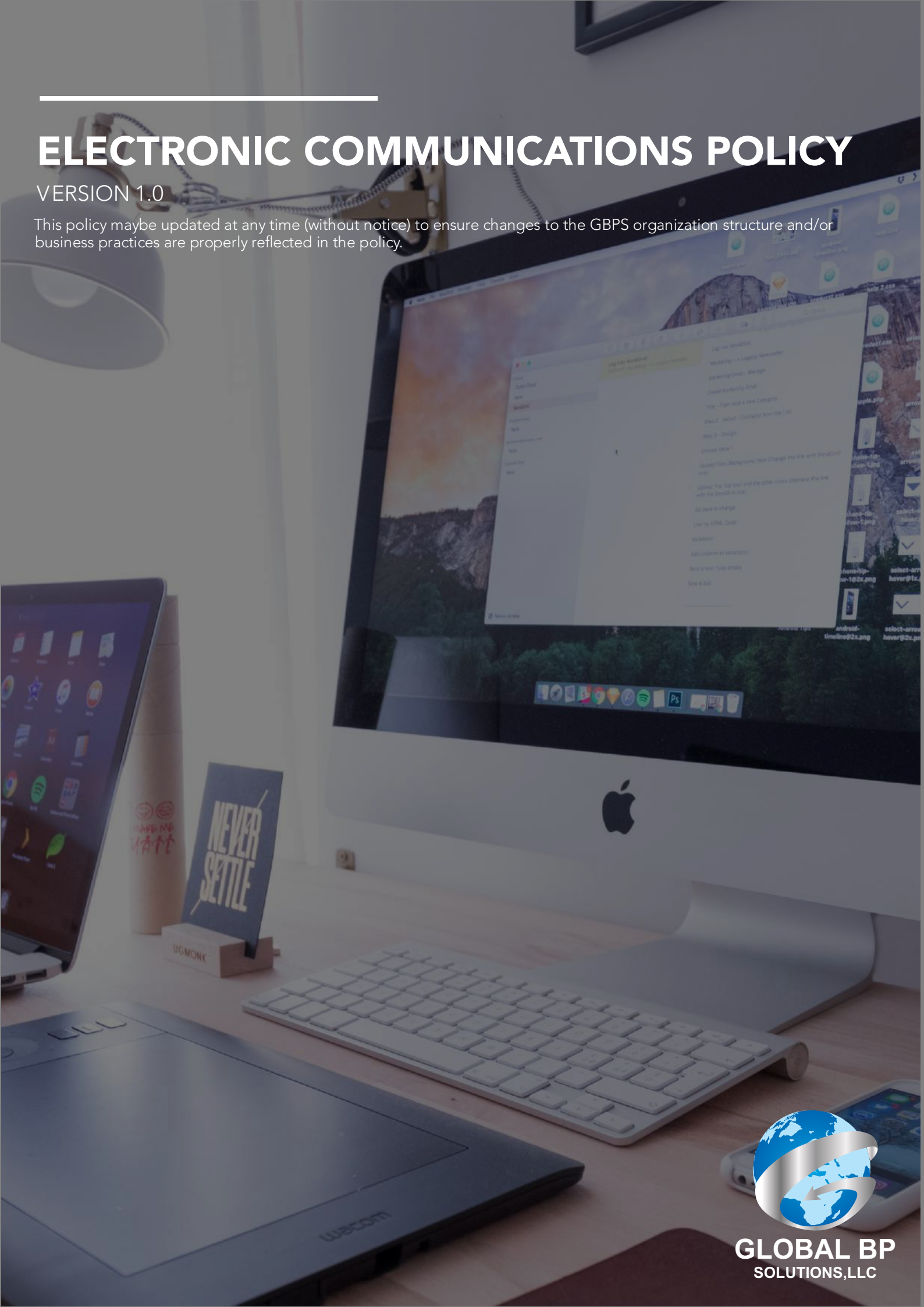
Transmission / Transmitted: The process of sending something (information or otherwise) from one location to another location.

Whole Disk Encryption: A method encryption where the entire contents (bits & bytes) of a magnetic or optical disk are encrypted.

ELECTRONIC COMMUNICATIONS POLICY

VERSION 1.0

This policy maybe updated at any time (without notice) to ensure changes to the GBPS organization structure and/or business practices are properly reflected in the policy.



GLOBAL BP
SOLUTIONS,LLC

Reader Information

Title:	GBPS Electronic Communications Policy.
Purpose:	To provide clear guidance on the appropriate, safe and legal way in which to use the GBPS's electronic communications, email, internet and facsimile (fax) services.
Author:	Information Security Team (IST) on behalf of the GBPS.
Target Audience:	All users (including GBPS staff, students, contractors, sub-contractors, agency staff and authorized third party commercial service providers) of the GBPS's electronic communications, email, internet and facsimile (fax) services.
Superseded Documents:	All local email, internet/intranet and fax policies and procedures.
Related Documents:	GBPS Information Security Policy. GBPS Information Technology Acceptable Use Policy. GBPS Password Standards Policy. GBPS Encryption Policy. GBPS Internet Content Filter Standard. GBPS Service Provider Confidentiality Agreement. GBPS Information Classification & Handling Policy
Review Date:	June 2019

Document History

Version	Owner	Author	Publish Date
1.0	GBPS	GBPS Information Security Team (IST)	January 2018
2.0	GBPS	GBPS Information Security Team (IST)	August 2018
3.0	GBPS	GBPS Information Security Team (IST)	June 2019

1.0 Purpose

Global BP Solutions (GBPS) is committed to the correct and proper use of its electronic communications, email, internet and facsimile (fax) services in support of its administrative and service functions.

The inappropriate use of GBPS' electronic communications, email, internet or fax services could expose the organization to risks ranging from virus attacks, theft and disclosure of information, disruption of network systems and services and litigation. The purpose of this policy is to define acceptable use of GBPS's electronic communications, email, internet, intranet and fax services.

This policy is mandatory and by using any of the GBPS's electronic communications, email, internet, intranet and fax services, users are agreeing to abide by the terms of this policy.

2.0 Scope

This policy represents the GBPS's national position and takes precedence over all other relevant policies which may be developed at a local level. The policy applies to:

All electronic communications, email, internet, intranet and fax services provided by the GBPS;

All Information Technology (I.T.) resources provided by the GBPS;

All users (including GBPS staff, students, contractors, sub-contractors, agency staff and authorized third party commercial service providers) of the GBPS's electronic communications, email, internet and facsimile (fax) facilities;

All use (both personal & GBPS business related) of the GBPS's electronic communications, email, internet and facsimile (fax) facilities;

All connections to (locally or remotely) the GBPS's email, internet, intranet and fax facilities;

All connections made to external networks through the GBPS network.

3.0 Definitions

A list of terms used throughout this policy are defined in *appendix A*.

4.0 Policy

4.1 Principles of Acceptable Use

The acceptable use of the GBPS's electronic communications, email, internet and facsimile (fax) services is based on the following principles:

Access to the GBPS's email and internet facilities should be regarded as a business requirement and not an automatic entitlement.

Users have a responsibility to ensure that they use GBPS's email, internet, intranet and fax facilities at all times in a manner which is lawful, ethical and efficient.

Users are expected to respect the rights and property of others, including privacy, confidentiality and intellectual property.

Users are expected to respect the integrity and security of the GBPS's email, internet, intranet and fax facilities.

4.2 Monitoring

The GBPS reserves the right to routinely monitor, log and record any and all use of its electronic communications, email and internet facilities for the purpose of:

1) Helping to trace and resolve technical faults.
2) Protecting and maintaining network and system security.
3) Maintaining system performance and availability.
4) Ensure the privacy and integrity of information stored on the GBPS network.
5) Investigating actual and suspected security incidents.
6) Preventing, detecting and minimizing inappropriate use.
7) Protecting the rights and property of the GBPS, its staff, patients and clients.
8) Ensuring compliance with GBPS policies, current legislation and applicable regulations.

Routine monitoring reports will be kept by the GBPS for at least 30 days after which time they may be purged or deleted.

While the GBPS does not routinely monitor an individual user's use of its electronic communications, email and internet activity it reserves the right to do so when a breach of its policies or illegal activity is suspected.

The monitoring of an individual user will only be undertaken at the request of the individual's line manager and the HR Directorate. The monitoring may include but is not limited to details of internet sites visited, time spent on sites, pages viewed,

information downloaded and the contents of email messages.

GBPS will at all times seek to act in a fair manner and respect the individual user's right for the privacy of their personal data under the *U.S Data Protection Law.* Personal information collected through monitoring will not be used for purposes other than those for which the monitoring was introduced, unless it is clearly in the users interest to do so or it reveals activity that GBPS could not be reasonably expected to ignore, for example a user found to be viewing, downloading or forwarding child pornography, hacking activities etc.

Individual monitoring reports will only be accessible to the appropriate authorised GBPS personnel and will be deleted when they are no longer required.

In the process of dealing with computer support calls GBPS ICT staff may need to access a user's computer to resolve the support call. In such circumstance's ICT staff must respect the privacy of the individual user and not access information, documents or emails of a personal nature without the user's permission or unless they need to in order to resolve the support call. In some cases, the ICT department may use remote control software to connect and take control of a user's computer remotely. In such circumstances the ICT staff will not use this software to connect to the user's computer without first attempting to contact the user of the computer first.

4.3 Personal Use

The GBPS's electronic communications, email, internet, intranet and fax services are to be used primarily for GBPS business-related purposes.

GBPS has the final decision on deciding what constitutes personal use.

4.4 File Transfer

Where possible all external transfers of confidential or restricted information must take place electronically via secure channels (i.e. Secure FTP, TLS, VPN etc) or encrypted email.

4.5 Email

The primary purpose of the GBPS email system is to promote effective communication on GBPS business matters. Authorised users may be granted access to email services subject to the requirements of their role within the GBPS.

Users must respect the privacy of others at all times and only use email accounts that have been issued to them.

Users should be careful when using their GBPS email account to send personal messages that their words or actions do not have a negative impact on the GBPS in any way.

Only email facilities provided by the GBPS may be used in connection with an individual user work for the GBPS. The use of third-party web-based email services for the transmission of GBPS confidential or restricted information is strictly prohibited.

Access to third party web-based email servers is not allowed using the GBPS network. However, email messages can be sent from the GBPS network to third party web-based email servers, but it should be noted that this is not a secure method of sending information.

Where necessary individual users may apply for and be granted access to individual governmental or health sector web mail servers (i.e. Department of Health & Children, Royal College of Surgeons, voluntary hospitals etc.). In addition, users who are on secondment to the GBPS or are employed jointly by the GBPS and another organization (i.e. joint appointments) may apply for and be granted access to the web mail server of the organization they are on secondment from or the organization which they are a jointly employed by.

Users who are secondment to the GBPS from an academic institute or are jointly employed by the GBPS and an academic institute will only be granted access to the academic institute's faculty web mail server. Access to the academic institute's student web mail servers is not permitted.

For security reasons users who regularly receive GBPS confidential or restricted information via email must not forward their GBPS email messages to their own personal third-party web-based email account.

Users should ensure they keep their personal email messages separate from their GBPS business related email messages.

In circumstances where it is necessary to transmit confidential or restricted information via email the sender must ensure the following checks are carried out before sending the information:

1) The name and email address of all the intended recipient(s) are correct;

2) The email message is clearly marked as "Private & Confidential";

3) Only the minimum amount of confidential or restricted information as is necessary for a given function(s) to be carried out is to be sent;

Where it is necessary to transmit confidential or restricted information to an email address outside of the GBPS domain, the sender must ensure the following additional checks are carried out before and after sending the information:

1) The transfer is authorised by a GBPS line manager. The authorization

must be issued in advance of the first instance and will apply thereafter if necessary.

2) All confidential or personal information sent with the email message is encrypted in-line with the requirements of the *GBPS Encryption Policy*.

3) The password used to decrypt (read) the confidential or restricted information must not be sent along with the original email message.

4) Where practical check that the email message and information have been received by the intended recipient(s) (i.e. ask for a delivery receipt or phone the intended recipients to confirm receipt).

Where there is a business need, GBPS line managers may apply to the ICT department to have a generic or group GBPS email address created which will be shared by multiple users (see section 4.3.3 of the *GBPS Access Control Policy*).

Users who require their secretaries or other colleagues to have access to their mailbox or calendars should setup shared mailboxes and calendars as necessary, rather than sharing their usernames and passwords.

Email distribution lists must only be used for the authorised distribution of GBPS work-related information which is relevant to everyone on the list.

Email carries the same legal status as other written documents and should be used with the same care.

Email is capable of forming or varying a contract in the same way as a written letter. Users must be careful when wording an email, so it cannot be construed as forming or varying a contract when this is not the intention.

A disclaimer must be automatically attached to all GBPS out-going email messages. This disclaimer does not excuse the user from undertaking fundamental checks before sending the email (.i.e. checking the email content for accuracy, correct address etc.).

The amount of email in a user's personal inbox and sent items folder must be kept to a minimum. Personal emails and attachments that are not GBPS business related must be deleted as soon as possible after receipt. Confidential and restricted information which has been received via email should not be stored permanently in a user's mailbox once it has been read. Old GBPS work-related email and attachments that are no longer required should should be archived or moved to a personal folder on the users computer.

During planned periods of absence such as career breaks, holidays or on training courses users should ensure where practical, their mailbox is put on divert to one of their colleagues so that there is no disruption to service delivery.

Users leaving the employment of the GBPS will have all emails forwarded to the replacement personnel or line manager. They should also ensure they remove or delete all personal email messages (i.e. email messages which are of a personal nature and are not GBPS business related) from their GBPS mailbox before they leave as it may not be possible to get a copy of these once they have left the GBPS.

All email accounts maintained on the GBPS's email system are the property of the GBPS.

4.6 Internet & Intranet

The primary purpose of the GBPS internet and intranet service is to provide access to a valuable business tool to facilitate communication, information sharing, education and learning and authorized research.

Authorised users may be granted access to internet services over the GBPS network subject to the requirements of their role within the GBPS.

In accordance with the GBPS *Internet Content Filter Standard* each user who has been granted access to the internet over the GBPS network will be assigned to one or more GBPS internet user access groups depending on their role or function within the GBPS.

The GBPS automatically filters internet access over its network and blocks access to individual websites or categories of internet content that it considers inappropriate.

Users who have a legitimate GBPS business reason may with the approval of their line manager apply to their local ICT department for access to blocked internet content. Access requests should be made using the *GBPS Internet Content Filter Exemption Request Form.*

GBPS line managers approving internet access requests of behalf of users have a responsibility to ensure they only approve and sign access requests for the user once they are satisfied that all categories and subcategories of internet content requested by the user are appropriate, necessary and relevant to the user's current role within the GBPS.

Internet access from GBPS smart devices will be exempt from the standard GBPS internet content filtering protocols. However, the users of GBPS smart devices will be held responsible for all internet connections made from their GBPS smart device. They must ensure that all internet access from their device is in accordance with requirements of this policy, the *GBPS I.T. Acceptable Use Policy and the GBPS Internet Filter Standard.*

Confidential or restricted information regarding GBPS and client business practices and procedures or personal information about any patients, clients or employees should not be published at all.

Users must not install or use any third party internet facilities on GBPS computer devices without the prior authorization of their line manager and the ICT Directorate.

Users must only use internet accounts that have been issued to them.

Users need to remember that when visiting an internet site, the unique address for their GBPS computer device (i.e. I.P. address) can be logged by the internet sites that they visit so the GBPS could be identified. Therefore, any internet activity that is carried out by them may affect GBPS.

Users should be aware that information hosted on the internet offers no guarantee of accuracy, reliability or authenticity.

4.7 Social Media

Access to social media websites is blocked automatically by the GBPS and that includes harmful material, hacking and adult sites. However, users who have a legitimate client business reason may with the approval of their line manager/ARM apply to the ICT department for access to these sites. Access requests should be made using the *GBPS Internet Content Filter Exemption Request Form.*

Users should be aware that all use of social media, either in a personal capacity or when communicating on behalf of the GBPS must be in accordance with the *GBPS Social Media Policy & Guidelines.*

Confidential or restricted information regarding GBPS business practices and procedures or personal information about any GBPS patients, clients or employees must not be posted or discussed on any social media websites.

4.8 Fax

Users must respect the privacy of others at all times and only access fax messages where they are the intended recipient or they have a valid GBPS work-related reason.

User ill only be able to fax after entering a username and password on the Fax/Scan/Printer all-in-one device.

Users who receive fax messages where they are not the intended recipient must contact the sender and notify them of their error and destroy or return the fax message as directed by the sender.

Users will use fax only if client has asked for it and will abide to the following:

1) Only the minimum amount of confidential or restricted information as is necessary for a given function(s) to be carried out is included in the fax message;

2) When the fax message has been sent, keep a copy of the transmission slip and where practical contact the intended recipient to confirm receipt of the fax message.

3) Remove all documents from the fax machine immediately after faxing.

Where possible, only fax machines which are owned or leased by the GBPS should be used to send or receive confidential and restricted information thus Ring Central and physical fax machine if need be.

Users who frequently send confidential or restricted information via fax to third parties should periodically remind the third parties that they need to notify the GBPS immediately if their fax number(s) changes.

Fax messages are capable of forming or varying a contract in the same way as a written letter. Users must be careful when wording a fax message, so it cannot be construed as forming or varying a contract when this is not the intention.

Fax messages carry the same legal status as other written documents and should be used with the same care.

4.9 Security

Users who breach information security by inadvertently transmitting confidential, restricted or personal information by fax, email or the internet to an incorrect address or destination, must follow the procedure below:

1) The breach must be managed and reported in accordance with the *GBPS Data Protection Breach Management Policy*;

2) The user must contact the recipient of the fax, email or internet message immediately and request that the information is returned to the GBPS immediately or destroyed.

Viruses and other forms of malicious software are usually spread via email and the internet. Users who receive a virus warning message must notify the ICT Directorate and under no circumstances should they forward it on to other users.

4.10 Unacceptable Use

The GBPS's email, internet and fax facilities may not be used:

1) For personal use;
2) For commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit;
3) For political purposes, such as promoting a political party / movement, or a candidate for political office, or campa igning for or against government decisions;
4) To knowingly misrepresent the GBPS or the client;
5) To enter into contractual agreements inappropriately (i.e. without authorization or where another form of agreement is required);
6) For any activity that would infringe intellectual property rights (e.g. unlicensed installation, distribution or copying of copyrighted material);
7) To send messages that contain libelous, defamatory or harassing remarks, images or other material;
8) To bully others;
9) For creating or transmitting "junk" or "spam" emails. This includes but is not limited to unsolicited commercial emails, jokes, chain-letters or advertisements;

10) For any activity that would constitute a criminal offence, give rise to a civil liability or otherwise violate any law;
11) For any activity that would deliberately compromise the privacy of others;
12) For any activity that would intentionally waste the GBPS's resources (e.g. employee time and IT resources);
13) For any activity that would intentionally compromise the security and availability of the GBPS's IT services (e.g. by deliberately or carelessly causing computer virus and malicious software infection);
14) To transmit confidential or personal information outside the GBPS unless the information has been encrypted (email and internet) and the transmission has been authorised by a GBPS line manager;
15) To create, view, download, host or transmit material (other than users who are authorised by the GBPS to access such material for research etc.) of a pornographic or sexual nature or which may generally be considered offensive or obscene and could cause offence to others on the grounds of race, creed, gender, sexual orientation, disability, age or political beliefs. material is defined as information (irrespective of format), images, video clips, audio recordings etc;
16) To forge or attempt to forge an email message or, send an email message using another person's account without their permission;
17) To upload or download access-restricted GBPS information contrary to this policy or in violation of any other GBPS policy.

The above list should not be seen as exhaustive, as other examples of unacceptable use of the GBPS's electronic communications, email, internet and facsimile (fax) services may exist.

The GBPS has the final decision on deciding what constitutes personal use.

The GBPS will refer any use of its electronic communications, email, internet and facsimile (fax) services for illegal activities to the Gardai

5.0 Roles & Responsibilities

5.1 ICT Directorate

The ICT Directorate is responsible for:

The provision of reliable and secure email and internet facilities;

The deployment and management of internet content monitoring and filtering facilities;

The deployment and management of appropriate technical and security safeguards to ensure availability, integrity and security of the email and internet facilities;

The provision, deployment and management of encryption facilities;

The provision of training, advice and guidance to computer systems users;

Monitoring of all electronic communications, email and internet traffic with no negative intents to ensure maximum security.

5.2 Information Owners

Information owners are responsible for:

The implementation of this policy and all other relevant policies within the GBPS directorate or service they manage;

The ownership, management, control and security of the information processed by their directorate or service on behalf of the GBPS;

The ownership, management, control and security of GBPS information systems used by their directorate or service to process information on behalf of the GBPS;

Maintaining a list of GBPS information systems and applications which are managed and controlled by their directorate or service.

Making sure adequate procedures are implemented within their directorate or service, so as to ensure all GBPS staff, students, client facing employees, contractors, sub-contractors, agency staff and commercial service providers that report to them are made aware of and are instructed to comply with this policy and all other relevant policies;

Making sure staff that report to them are provided with adequate training so as to ensure on-going compliance of this policy and all other relevant policies;

5.3 Line Managers

Line managers are responsible for:

The implementation of this policy and all other related GBPS policies within the business areas for which they are responsible;

Ensuring that all GBPS staff, students, contractors, sub-contractors and agency staff who report to them are made aware of and have access to this policy and all other relevant GBPS policies;

Ensuring that all GBPS staff, students, contractors, sub-contractors and agency staff who report to them are provided with adequate training and are instructed to comply with this policy and all other relevant GBPS policies;

Ensuring they only approve and sign internet access requests for employees, once they are satisfied that all categories and subcategories of internet content requested by the employee are appropriate, necessary and relevant to the employee's current role within the GBPS.

Reporting all actual or suspected breaches of information security immediately to the ICT Directorate and/or the Consumer Affairs section;

Consulting with the HR Directorate in relation to the appropriate procedures to follow when a breach of this policy has occurred.

5.4 Users

Each user of the GBPS's electronic communications, email, internet and facsimile(fax) services is responsible for:

Complying with the terms of this policy and all other relevant GBPS policies, procedures, regulations and applicable legislation;

Respecting and protecting the privacy and confidentiality of the information they process at all times;

Complying with instructions issued by the ICT Directorate on behalf of the GBPS;

Reporting all misuse and breaches of this policy to their line manager.

6.0 Enforcement

The GBPS reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. GBPS staff, students, contractors, sub-contractors or agency staff who breach this policy maybe subject to disciplinary action, including suspension and dismissal as provided for in the GBPS disciplinary procedure.

Breaches of this policy by a third-party commercial service provider, may lead to the withdrawal of GBPS information technology resources to that third party

commercial service provider and/or the cancellation of any contract(s) between the GBPS and the third-party commercial service provider.

The GBPS will refer any use of its electronic communications, email, internet and facsimile (fax) services for illegal activities to the Gardai

7.0 Review & Update

This policy will be reviewed and updated annually or more frequently if necessary, to ensure that any changes to the GBPS's organization structure and business practices are properly reflected in the policy.

Appendix A

Authorization / Authorised: Official GBPS approval and permission to perform a particular task.

Breach of Information Security: The situation where GBPS confidential or personal information has been put at risk of unauthorized disclosure as a result of the loss or theft of the information or, through the accidental or deliberate release of the information.

Confidential information: (As defined by the *GBPS Information Classification & Handling Policy*) Information which is protected by Irish and/or E.U. legislation or regulations, GBPS policies or legal contracts. The unauthorised or accidental disclosure of this information could adversely impact the GBPS, its patients, its staff and its business partners. Some examples of confidential information include:

Patient / client / staff personal data (Except that which is restricted)
Patient /client / staff medical records (Except that which is restricted)
Unpublished medical research
Staff personal records
Financial data / budgetary Reports
Service plans / service performance monitoring reports
Draft reports
Audit reports
Purchasing information
Vendor contracts / Commercially sensitive data
Data covered by Non-Disclosure Agreements
Passwords / cryptographic private keys
Data collected as part of criminal/HR investigations
Incident Reports

Decryption / Decrypt: The process of decoding information which has been converted into an unreadable form (cipher text) back into a readable form (plain text).

Defamatory: False statement or series of statements which affect the reputation of a person or an organization

Email: System for sending messages electronically from one individual to another via telecommunications links between computers.

Email Disclaimer: Legal statement appended to an email message.

Encryption / Encrypt: The process of converting (encoding) information from a readable form (plain text) that can be read by everyone into an unreadable form (cipher text) that can only be read by the information owner and other authorised persons.

Encryption Key: A piece of data (parameter usually a password) used to encrypt/decrypt information.

Information: Any data in an electronic format that is capable of being processed or has already been processed.

Information Owner: The individual responsible for the management of a GBPS directorate or service **(**or equivalent).

Information System: A computerized system or software application used to access, record, store, gather and process information.

Information Technology (I.T.) resources: Includes all computer facilities and devices, networks and data communications infrastructure, telecommunications systems and equipment, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords, and information and data that are owned or leased by the GBPS.

Intellectual Property: Any material which is protected by copyright law and gives the copyright holder the exclusive right to control reproduction or use of the material. For example - books, movies, sound recordings, music, photographs software etc

Internet: A worldwide computer network consisting of smaller networks which facilities the transmission and exchange of information for commercial, educational and governmental purposes etc.

Line manager: The individual a user reports directly to.

Mobile Computer Device: Any handheld computer device including but not limited to laptops, tablets, notebooks, PDA's etc.

Personal Use: The use of the GBPS's Information Technology (IT) resources for any activity(s) which is not GBPS work-related.

Personal information: Information relating to a living individual (i.e. GBPS employee, client and patient) who is or can be identified either from the information or from the information in conjunction with other information. For example: - an individuals name, address, email address, photograph, date of birth, fingerprint, racial or ethnic origin, physical or mental health, sexual life, religious or philosophical beliefs, trade union membership, political views, criminal convictions etc.

Pornography / Pornographic: The description or depiction of sexual acts or naked people that are designed to be sexually exciting.

Privacy: The right of individual or group to exclude themselves or information about themselves from being made public.

Process / Processed / Processing: Performing any manual or automated operation or set of operations on information including:

Obtaining, recording or keeping the information;
Collecting, organizing, storing, altering or adapting the information;
Retrieving, consulting or using the information;
Disclosing the information or data by transmitting, disseminating or otherwise making it available;
Aligning, combining, blocking, erasing or destroying the information.

Restricted Information: (As defined by the *GBPS Information Classification & Handling Policy*) Highly sensitive confidential information**.** The unauthorized or accidental disclosure of this information would seriously and adversely impact the GBPS, its patients, its staff and its business partners. Some examples of restricted information include:

Patient / client / staff sensitive personal information (i.e. mental health status, HIV status, STD/STI status etc)
Childcare / Adoption information
Social Work information
Addiction Services information
Disability Services information
Unpublished financial reports
Strategic corporate plans
Sensitive medical research

Smart Device: A handheld mobile computer device which is capable of wireless connection (via WiFi, 3G, 4G etc), voice and video communication and, internet browsing. (for example: Apple IOS enabled devices (i.e. iPhone & iPad), Google Android enabled devices (i.e. Samsung Galaxy tablet), Windows Mobile enabled devices and, Blackberry RIM enabled devices etc)

Social Media: The name given to various online technology tools that enable people to communicate easily via the internet to share information and resources. It includes the following types of web sites:

1) **Internet Chat Rooms:** Websites that allow interactive messaging, where users can exchange views and opinions in real time on a variety of subject matters.

2) **Internet Discussion Forums/Message Boards:** Websites that allow users to participate in on-line discussions on a particular subject matter.

3) **Internet Social Networking Websites:** Websites that allow users to build on-line profiles, share information, pictures, blog entries and music clips etc. Including but not limited to Bebo, Facebook, Twitter, Myspace, Friendster, Whispurr, LinkedIn and Viadeo.

4) **Internet Video Hosting/ Sharing Websites:** Websites that allows users to upload video clips, which can then be viewed by other users. Including but not limited to Youtube, Yahoo Video, Google Video and MyVideo.

5) **Blogging Websites:** Websites that allow a user to write an on-line diary (known as a blog) sharing their thoughts and opinions on various subjects

Third Party Commercial Service Provider: Any individual or commercial company that have been contracted by the GBPS to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, data management services, patient / client care and management services etc.) to the GBPS.

Third Party Web Based Email Services (Servers): Any internet accessible email facilities which are not managed or hosted by the GBPS. Including both commercial email services (for example, Microsoft Hotmail, Yahoo Mail, GMail (Google Mail), AOL Mail, eircom email, Indigo email and Mail.Com. etc) and non-commercial (for example, third level training and educational institutions etc).

Third Party Internet Facilities: Any internet facilities which are not managed or provided by the GBPS. These include those provided directly by an Internet Service Providers (ISP). For example Eircom, ESAT BT, Irish Broadband, Smart Telecom, Clearwire, Broadband4Ireland, Chorus NTL and UTV etc.

Transmission / Transmitted / Transfer: The process of sending or moving something (information or otherwise) from one location to another location.

Users: Any authorized individual who uses the GBPS's electronic communications, email, internet, intranet and fax services.

PASSWORD STANDARDS POLICY

VERSION 3.0

This policy maybe updated at anytime (without notice) to ensure changes to GBPS's organisation structure and/or business practices are properly reflected in the policy. Please ensure you check theGBPS intranet for the most up to date version of this policy

GLOBAL BP
SOLUTIONS,LLC

Reader Information

Title:	GBPS Password Standards Policy.
Purpose:	To provide clear guidance and present best practice for the creation of strong passwords, the management and protection of those passwords, and the frequency of change.
Author:	Information Security Team (IST).
Target Audience:	All system developers and users (including GBPS staff, students, contractors, sub-contractors, agency staff and authorized third party commercial service providers) of the GBPS's I.T resources.
Superseded Documents:	All local password standard policies and procedures.
Related Documents:	GBPS Information Security Policy. GBPS Information Technology Acceptable Use Policy. GBPS Electronic Communications Policy. GBPS Encryption Policy.

Document History

Version	Owner	Author	Publish Date
1.0	GBPS	Information Security Team (IST)	June 2009

1.0 Purpose

Passwords are one of the primary mechanisms that protect critical GBPS information systems and other resources from unauthorised use. Constructing secure passwords and ensuring proper password management are essential. Poor password management and protection could allow unauthorised access to the GBPS's Information Technology (I.T.) resources, which in turn could lead to the inappropriate disclosure and use of confidential or sensitive GBPS information. The purpose of this policy is provide clear guidance and present best practice for the creation of strong passwords, the management and protection of those passwords, and the frequency of change.

This policy is mandatory and by accessing any Information Technology (IT) resources which are owned or leased by the GBPS, users are agreeing to abide by the terms of this policy.

2.0 Scope

This policy represents the GBPS's national position and takes precedence over all other relevant policies which are developed at a local level. The policy applies to:

All GBPS Information Technology (I.T.) equipment, systems and applications which are capable of being password protected;

All system developers and users (including GBPS staff, students, contractors, sub- contractors, agency staff and authorized third party commercial service providers) of the GBPS's I.T. resources;

All connections to (locally or remotely) the GBPS network Domains (LAN/WAN/WiFi);

All connections made to external networks through the GBPS network.

3.0 Definitions

A list of terms used throughout this policy are defined in *appendix A*.

4.0 Policy

4.1 Principles of Password Security

Where technically feasible all GBPS Information Technology (I.T.) resources must be protected by the use of strong passwords.

All passwords created for use within the GBPS must meet the requirements of this policy.

4.2 Monitoring & Auditing

The ICT Directorate on behalf of the GBPS reserves the right to monitor and audit all password use within the GBPS to ensure compliance with this policy and to identify any weak passwords that could compromise the security of Information Technology (I.T.) equipment, systems, applications or the network.

4.3 Password Standard

All passwords must be unique and meet the following standard:

4.3.1 Password Length

All passwords must be a minimum of 8 characters in length. If existing systems are not capable of supporting 8 characters, then the maximum number of characters allowed within the system must be used.

4.3.2 Password Complexity

Passwords must contain a combination of letters (both upper & lower case), numbers (0-9) and at least one special character (for example: “, £, $, %, ^, &, *, @, #, ?, !, €).

Passwords must not be left blank.

Passwords or part of a password must not contain:

1) Any word(s) found in an English or foreign language dictionary;
2) Any word(s) spelled backwards - (for example: drow, yadnom);
3) Any slang words - (for example: dubs, agro, bling);
4) Any word with numbers appended (for example: deer2000, password2012, Paul2468 etc);
5) Any words with simple obfuscation (for example: p@ssw0rd, l33th4x0r, @dm1n100, g0ldf1sh, etc);
6) Any names of fictional characters - (for example: frodo, shrek);
7) Any common keyboard sequences - (for example: qwerty);

8) Any names of people, places or organisations - (for example: mary100, Liverpool, LFC2005, ManUtd);

9) Any personal information related to a user - (for example: user name, address, date of birth, GBPS personnel number, car registration number, telephone number);

10) A sequence of consecutive numbers or letters (for example: 12345678, abcdefgh, abcd1234);

11) The following sequence of letters - passwrd, passwd, pwrd, paswd, passwd.

4.3.3 Password History

No password may be re-used by a user.

4.3.4 Password Aging

User-level passwords such as those used to access GBPS computer devices, information systems and network domains must be changed at least every 60 days.

System-level passwords such as those used by GBPS information system administrators and network domain administrators must be changed at least every 90 days.

4.4 Password security

Users should avoid using the same password for multiple system or purposes.

Each user is responsible for all activities performed on any GBPS I.T. device, information system or application while logged in under their individual access account and password.

With the exception of generic / group access accounts users must only use user access accounts and passwords which have been assigned to them.

Users must ensure all passwords except those used for generic / group access accounts are kept confidential at all times and are not shared with others including their co-workers or third parties.

Users must not write down their password(s) on or near their computer device. However, in exceptional circumstances where a password has to be written down, the password must be stored in a secure locked place, which is not easily accessible to others.

Users must not send their passwords within email messages unless the email message is encrypted.

Users must change their passwords at least every 60 days or when instructed.

Users who suspect their password is known by others must change their password immediately.

Users must not misuse their own or another users password and knowingly elevate their information system access account or network domain access privileges above those that they have been authorized to use.

User must ensure all default passwords which are supplied by a vendor for new GBPS devices and systems are changed at installation time.

4.5 System & Application Development Standards

System developers (including both GBPS personnel and third party commercial service providers) who are responsible for developing information systems and applications for the GBPS or its customers must ensure that the systems and applications they develop are capable of implementing, supporting and enforcing this policy in full.

System developers (including both GBPS personnel and third party commercial service providers) who are responsible for developing information systems and applications for the GBPS or its customers must ensure that the systems and applications they develop contain the minimum security features:

1) They must support authentication of individual users and not just groups;

2) They must contain controls that can ensure that individuals can be held responsible for their actions;

3) They must not store passwords in clear text or in any easily reversible form;

4) The password should not be displayed on the screen when they are being entered;

5) They must provide for some sort of role management, such that one user can take control of the functions of another without having to know the other users password;

6) They must force users to change their password at their first logon.

7) They must automatically 'lock' a user account after a defined number consecutive failed login attempts.

8) They automatically 'lock' or log out user accounts after a defined period of inactivity.

9) They must provide a logging facility that as a minimum is capable of recording all failed and successful login attempts;

5.0 Roles & Responsibilities

5.1 Information Owners

Information owners are responsible for:

The implementation of this policy and all other relevant policies within the GBPS directorate or service they manage;

The ownership, management, control and security of the information processed by their directorate or service on behalf of the GBPS;

The ownership, management, control and security of GBPS information systems used by their directorate or service to process information on behalf of the GBPS;

Maintaining a list of GBPS information systems and applications which are managed and controlled by their directorate or service.

Making sure adequate procedures are implemented within their directorate or service, so as to ensure all GBPS employees, third parties and others that report to them are made aware of, and are instructed to comply with this policy and all other relevant policies;

Making sure adequate procedures are implemented within their directorate or service to ensure compliance of this policy and all other relevant policies;

5.2 Network Domain Administrators

Each GBPS network administrator is responsible for:

Complying with the terms of this policy and all other relevant GBPS policies, procedures, regulations and applicable legislation;

Ensuring all passwords generated for new user accounts and password resets meet the requirements of this policy;

Notifying users of their passwords in a secure and confidential manner.

5.3 System Administrators

Each GBPS system administrator is responsible for:

Complying with the terms of this policy and all other relevant GBPS policies, procedures, regulations and applicable legislation;

Ensuring all passwords generated for new user accounts and password resets meet the requirements of this policy;

Notifying users of their passwords in a secure and confidential manner;

Complying with instructions issued by the ICT Directorate.

5.4 Users

Each user of GBPS's IT resources is responsible for:

Complying with the terms of this policy and all other relevant GBPS policies, procedures, regulations and applicable legislation;

Respecting and protecting the privacy and confidentiality of the information systems and network they access, and the information processed by those systems or networks;

Ensuring they only use user access accounts and passwords which have been assigned to them;

Ensuring all passwords assigned to them are kept confidential at all times and not shared with others including their co-workers or third parties;

Changing their passwords at least every 60 days or when instructed to do so by designated system administrators, network domain administrators or the ICT Directorate;

Complying with instructions issued by designated information owners, system administrators, network administrators and/or the ICT Directorate on behalf of the GBPS;

Reporting all misuse and breaches of this policy to their line manager.

5.5 Line Managers

In addition to each user's responsibilities, line managers are directly responsible for:

The implementation of this policy and all other related GBPS policies within the business areas for which they are responsible;

Ensuring that all GBPS employees who report to them are made aware of and are instructed to comply with this policy and all other relevant GBPS policies;

Consulting with the HR Directorate in relation to the appropriate procedures to follow when a breach of this policy has occurred.

5.6 System Developers

In addition to the above system developers (including both GBPS personnel and third-party commercial service providers) are responsible for:

Ensuring the systems and applications they develop for the GBPS are capable of implementing, supporting and enforcing this policy in full.

6.0 Enforcement

The GBPS reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. GBPS staff, students, contractors, sub-contractors or agency staff who breach this policy maybe subject to disciplinary action, including suspension and dismissal as provided for in the GBPS disciplinary procedure.

Breaches of this policy by a third-party commercial service provider, may lead to the withdrawal of GBPS information technology resources to that third-party commercial service provider and/or the cancellation of any contract(s) between the GBPS and the third-party commercial service provider.

7.0 Review & Update

This policy will be reviewed and updated annually or more frequently if necessary, to ensure any changes to the GBPS's organization structure and business practices are properly reflected in the policy.

Appendix A

Information: Any data in an electronic format that is capable of being processed or has already been processed.

Information Owner: The individual responsible for the management of a GBPS directorate or service (GBPS RDO, National Director (or equivalent)).

Information Technology (I.T.) resources: Includes all computer facilities and devices, networks and data communications infrastructure, telecommunications systems and equipment, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords, and information and data that are owned or leased by the GBPS.

Line manager: The individual a user reports directly to.

Network Domain Administrators: The individuals responsible for the day to day management of a GBPS network domain. Also includes GBPS personnel who have been authorised to create and manage user accounts and passwords on a GBPS network domain.

Password: A string of characters that a user must supply in order to gain access to an IT resource.

Process / Processed / Processing: Performing any manual or automated operation or set of operations on information including:

Obtaining, recording or keeping the information;
Collecting, organising, storing, altering or adapting the information;
Retrieving, consulting or using the information;
Disclosing the information or data by transmitting, disseminating or otherwise making it available;
Aligning, combining, blocking, erasing or destroying the information.

System Administrators: The individual(s) charged by the designated system owner with the day to day management of GBPS information systems. Also includes the GBPS personnel and third parties who have been authorised to create and manage user accounts and passwords on these applications and systems.

System Developer: Any GBPS personnel or third party commercial service providers who are responsible for developing electronic information systems and application for the GBPS or its customers.

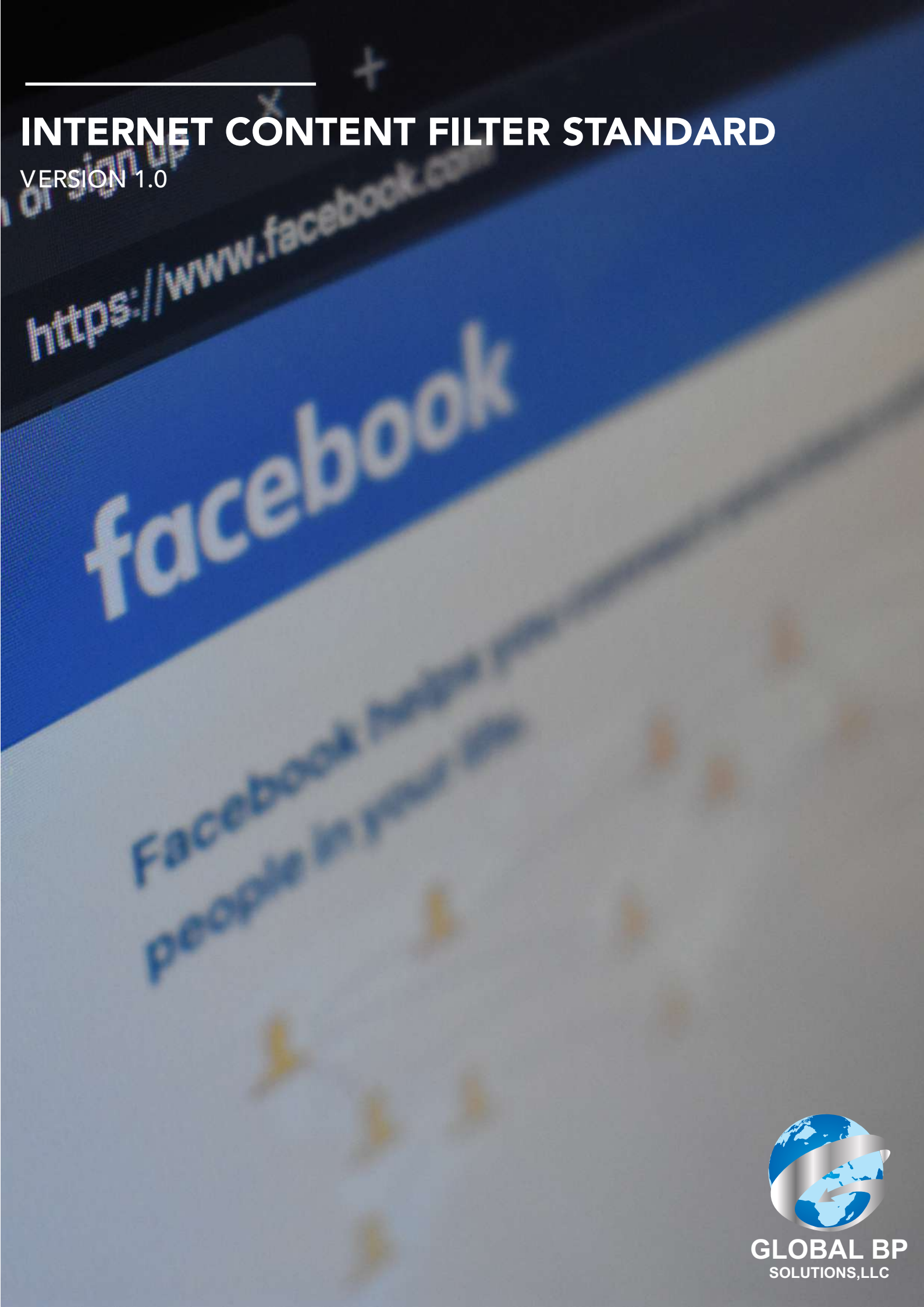
Third Party Commercial Service Provider: Any individual or commercial company that have been contracted by the GBPS to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or

support, supply and/or support of computer software / hardware, equipment maintenance, data management services, patient / client care and management services etc.) to the GBPS.

Users: Any authorized individual who uses the GBPS's I.T. resources.

INTERNET CONTENT FILTER STANDARD

VERSION 1.0



GLOBAL BP
SOLUTIONS,LLC

1.0 Purpose

The purpose of this Internet Content Filter Standard is to define the acceptable use of GBPS's internet services and describe which categories of internet content are accessible to GBPS employees and which are filtered (blocked).

The standard was formulated and developed by GBPS Information Security Team (IST) and sanctioned by the Senior Management of GBPS.

This standard is mandatory and by accessing internet content from any Information Technology (IT) resources which are owned or leased by GBPS, users are agreeing to abide by the terms of this standard.

2.0 Scope

This standard represents GBPS's national position and takes precedence over all other relevant standards which are developed at a local level.

The standard applies to:

All internet services provided by GBPS;

All Information Technology (I.T.) resources provided by GBPS;

All GBPS employees, clients and third parties that use GBPS's I.T. resources.

3.0 Standard

For the purpose of managing internet access, internet sites are grouped together into a number of categories and subcategories depending on the content that each site offers. ***Appendix A*** contains the list of categories and subcategories used and a description of each.

3.1 Filtered Internet Content

GBPS reserves the right to filter and block selected categories of internet content that it considers inappropriate or where access to such categories could lead to legal, security or operational issues.

The following categories / sub-categories of internet content are currently filtered and blocked by GBPS:

Adult Material
- Sex
- Nudity
- Adult Content
- Porn

Gambling

Dating

Nudity & Risqué

Other Adult Materials

Bandwidth Consuming
- Internet Radio & TV
- Streaming Media
- Peer-To-Peer File Sharing

General Interest - Personal
- MP3 & Audio Download Services
- Gambling
- Games
- Illegal or Questionable
- Hacking
- Proxy Avoidance
- URL Translation
- Web Hosting
- Web and Email Spam

Other Categories
- Military & Extremist
- Racism & Hate
- Social Networking
- Personals & Dating
- Tasteless
- Violence
- Weapons
- User Defined

3.2 Internet User Access Groups

Each GBPS employee who has been granted internet access will be assigned to one or more GBPS internet user access groups, depending on their role or function within GBPS. The current GBPS internet user access groups are:

1) Dental Group Policy (custom).
2) Marketing Group Policy (custom).
3) I.T Support Group Policy (custom).
4) Sales Group Policy (custom).
5) Graphics Design and Web Developers Group Policy (custom).
6) Accounting Group Policy(custom).
7) Manager/Directorate Group Policy (custom).
8) **Basic Group Policy (Main Group 1).**
9) **Custom Group Policy (Main Group 2).**
10) **Technical Group Policy (Main Group 3.**

3.2.1 Basic User Access Group

Each GBPS employee who has been granted internet access will by default be assigned to the basic user access group. This group will be allowed to access all unfiltered internet content. The table in ***Appendix B*** outlines the categories of internet content that are accessible by the basic user access group.

3.2.2 Custom User Access Group

A number of 'special interest' custom user access groups will be created to manage the business requirement for access to internet content that is otherwise filtered by GBPS.

Each custom user access group will allow access to an additional specific category or subcategory of internet content that is currently filtered. The table in ***Appendix B*** outlines the categories of internet content that are accessible by the custom user access groups.

3.2.3 Technical User Access Group

A number of additional 'special interest' technical user access groups will be created to manage the business requirement for access to technical information and software that is otherwise filtered by GBPS for legal or security reasons.

Each Technical user access group will allow access to an additional specific category or subcategory of internet content that is currently not available to members of the basic and custom user access groups. The table in ***Appendix B*** outlines the categories of internet content that is accessible by the privilege user access groups.

Access to GBPS technical user access groups will be restricted to the **relevant GBPS ICT personnel only.**

3.3 Access to Filtered Internet Content

Where an individual employee has a valid GBPS worked related reason, they may with the signed approval of their line manager or as requested by client for the employed personnel. All requests must be made in writing using GBPS ***Internet Content Filter Exemption Request Form*** or any other means that will then in turn be documented for future use.

For security reasons open access to third party email servers (i.e. General & Organizational email) is prohibited and as such these internet sites are permanently blocked for all GBPS users. However, employees with a valid GBPS business requirement and the signed approval of their line manager (at General Manager level (or equivalent) or above) may apply for access to specific external Health and/or Governmental email server(s). All requests must be made in writing using GBPS ***Internet Content Filter Exemption Request Form***.

GBPS line managers (at General Manager level (or equivalent) or above) approving internet access requests of behalf of GBPS employees, have a responsibility to ensure they only approve and sign access requests for employees, once they are satisfied that all categories and subcategories of internet content requested by the employee are appropriate, necessary and relevant to the employees current role within GBPS **and client's interest.**

Each 'special interest' user access group will operate independent of the others, and hence, a user's membership of one of the 'special interest' user access groups will not automatically confer membership of the other 'special interest user access groups.

GLOBAL BP SOLUTIONS,LLC

(For example, a user, who is a member of the I.T Support Group, will not be automatically granted membership of the adult material, military or extremist custom user access groups).

3.4 Internet Content Evaluation Team

GBPS Internet Content Evaluation Team (ICET) will be created to

1) Evaluate all other internet access requests which are not covered by GBPS Internet Filter Standard or existing GBPS policies

2) Carry out sample audit of approved internet access requests on a quarterly basis to ensure that internet access is granted in accordance with this standard.

3) Report the results of the sample audits.

3.5 Monitoring

GBPS reserves the right to monitor, record and report on any or all uses of its internet services, in order to:

1) Help trace and resolve technical faults.
2) Protect and maintain network and system security.
3) Maintain system performance and availability.
4) Investigate actual and suspected security incidents.
5) Prevent, detect or minimize inappropriate use.
6) Ensure compliance with GBPS policies, current legislation and applicable regulations.

The ICT Directorate will produce monthly reports on internet usage for each GBPS region and distribute these to the relevant RDO's and GBPS management team.

While GBPS will not routinely monitor an individual user's use of its internet services, it reserves the right to do so when a breach of its policies or illegal activity is suspected. This monitoring may include, but is not limited to, internet sites visited, total time spent on the internet, and attempts to access filtered (blocked) internet content.

The monitoring of an individual user's internet activity must be authorised by the HR Directorate and the individuals line manager (General Manager level or above). The results of all monitoring will be stored securely and will only be shared with those authorised to have access to such information.

3.6 Withdrawal of Internet Services

GBPS employees who are found to have abused their internet access rights may have their internet access withdrawn by GBPS and, depending on the nature of the abuse, could be subject to disciplinary action, including suspension and dismissal as provided for in GBPS disciplinary procedures.

The ICT Directorate reserves the right (without prior notification) to restrict or blo ck access to certain categories or subcategories of internet content, which are identified as having a negative impact on the performance of GBPS network, information systems and/or equipment.

Appendix A

GBPS Internet Categories &

Subcategories Abortion: Sites with neutral or balanced

presentation of abortion.

Pro-Choice: Sites that provide information about or are sponsored by organizations that support legal abortion or that offer support or encouragement to those seeking the procedure.

Pro-Life: Sites that provide information about or are sponsored by organizations that oppose legal abortion or that seek increased restriction of abortion.

Adult Material: Sites which provide adult material.

Adult Content - Sites that display full or partial nudity in a sexual context, but not sexual activity; erotica; sexual paraphernalia; sex-oriented businesses as clubs, nightclubs, escort services; and sites supporting the online purchase of such goods and services.

Lingerie and Swimsuit - Sites that offer images of models in suggestive but not lewd costume, with semi nudity permitted. Includes classic 'cheese-cake,' calendar, and pinup art and photography (Includes site's offering lingerie or swimwear for sale).

Nudity - Sites that offer depictions of nude or semi-nude human forms, singly or in groups, not overtly sexual in intent or effect.

Sex - Sites that depict or graphically describe sexual acts or activity, including exhibitionism; also, sites offering direct links to such sites.

Sex Education - Sites that offer information about sex and sexuality, with no pornographic intent.

Advocacy Groups: Sites that promote change or reform in public policy, public opinion, social practice, economic activities, and relationships.

Business and Economy: Sites sponsored by or devoted to business firms, business associations, industry groups, or business in general.

Financial Data and Services: Sites that offer news and quotations on stocks, bonds, and other investment vehicles, investment advice, but not online trading (Includes banks, credit unions, credit cards, and insurance).

Hosted Business Applications: Sites that provide access to business-oriented web applications and allow storage of sensitive data, excluding those for web collaboration.

Bandwidth PG: Sites providing bandwidth intensive services

Internet Radio and TV - Sites whose primary purpose is to provide radio or TV programming on the Internet.

Internet Telephony - Sites that enable users to make telephone calls via the Internet or to obtain information or software for that purpose.

Peer-to-Peer File Sharing - Sites that provide client software to enable peer-to-peer file sharing and transfer. *(Accessible to the relevant ICT Personnel Only)*

Personal Network Storage and Backup - Sites that store personal files on Internet servers for backup or exchange.

Streaming Media - Sites that primarily provide streaming media content, such as movie trailers (Including Youtube.com)

Drugs: Sites the provide information about regulated and unregulated drugs

Abused Drugs - Sites that promote or provide information about the use of prohibited drugs, except marijuana, or the abuse or unsanctioned use of controlled or regulated drugs; also, paraphernalia associated with such use or abuse.

Marijuana - Sites that provide information about or promote the cultivation, preparation, or use of marijuana.

Prescribed Medications - Sites that provide information about approved drugs and their medical use.

Supplements and Unregulated Compounds - Sites that provide information about or promote the sale or use of chemicals not regulated by the FDA (such as naturally occurring compounds).

Education: Sites that provide educational information

Cultural Institutions - Sites sponsored by museums, galleries, theatres (but not movie theatres), libraries, and similar institutions; also, sites whose purpose is the display of artworks.

Educational Institutions - Sites sponsored by schools and other educational facilities, by non-academic research institutions, or that relate to educational events and activities.

Educational Materials - Sites that provide information about or that sell or provide curriculum materials or direct instruction; also, learned journals and similar publications.

Reference Materials - Sites that offer reference-shelf content such as atlases, dictionaries, encyclopedias, formularies, white and yellow pages, and public statistical data.

Entertainment: Sites that provide information about or promote motion pictures, non-news radio and television, books, humor, and magazines.

MP3 and Audio Download Services - Sites that support downloading of MP3 or other sound files or that serve as directories of such sites.

Gambling: Sites that provide information about or promote gambling or support online gambling, involving a risk of losing money.

Games: Sites that provide information about or promote electronic games, video games, computer games, role-playing games, or online games (Includes sweepstakes and giveaways).

Government: Sites sponsored by branches, bureaus, or agencies of any level of government, except for the armed forces.

Military - Sites sponsored by branches or agencies of the armed services.

Political Organizations - Sites sponsored by or providing information about political parties and interest groups focused on elections or legislation.

Health: Sites that provide information or advice on personal health or medical services, procedures, or devices, but not drugs (Includes self-help groups).

Illegal or Questionable: Sites that provide instruction in or promote non-violent crime or unethical or dishonest behavior or the avoidance of prosecution.

Information Technology: Sites sponsored by or providing information about computers, software, the Internet, and related business firms, including sites supporting the sale of hardware, software, peripherals, and services. *(Accessible to the relevant ICT Personnel Only)*

Computer Security - Sites that provide information about or free downloadable tools for computer security.

Hacking - Sites that provide information about or promote illegal or questionable access to or use of computer or communication equipment, software, or databases. *(Accessible to the relevant ICT Personnel Only)*

Proxy Avoidance - Sites that provide information about how to bypass proxy serve features or to gain access to URLs in any way that bypasses the proxy server. *(Accessible to the relevant ICT Personnel Only)*

Search Engines and Portals - Sites that support searching the Web, news groups, or indices or directories thereof.

URL Translation Sites - Sites that offer online translation of URLs. These sites access the URL to be translated in a way that bypasses the proxy server, potentially allowing unauthorized access. *(Accessible to the relevant ICT Personnel Only)*

Web & Email Spam - Sites whose links are sent in unsolicited commercial email, either as part of campaigns to promote products or services, or to entice readers to click through to surveys or similar sites. Also included are sites that display comment spam. *(Accessible to the relevant ICT Personnel Only)*

Web Collaboration - Sites that provide virtual workspace for purposes of collaboration and conferencing, which may include sites that enable authorized access to a computer or network from a remote location

Web Hosting - Sites of organizations that provide hosting services, or top-level domain pages of Web communities. *(Accessible to the relevant ICT Personnel Only)*

Internet Communication: Sites that support or provide information about internet communication.

Web Chat - Sites that host web chat services or that support or provide information about chat via HTTP or IRC.

General Email - Sites that provide email services open to general use.

Organizational Email - Login sites for corporate or institutional email systems.

Text and Media Messaging - Sites that enable the sending of messages and other content via SMS, EMS, MMS, or similar protocols.

Job Search: Sites that offer information about or support the seeking of employment or employees.

Militancy and Extremist: Sites that offer information about or promote or are sponsored by groups advocating antigovernment beliefs or action.

Miscellaneous:

Content Delivery Networks - Commercial hosts that deliver content to subscribing Web sites.

Dynamic Content - URLs that are generated dynamically by a Web server.

File Download Servers - Web servers whose primary function is to deliver files for download.

Image Servers - Web servers whose primary function is to deliver images.

Images (Media) - URLs ending with image filenames.

Network Errors - URLs with hosts that do not resolve to IP addresses. *(Accessible to the relevant ICT Personnel Only)*

Private IP Addresses - IP addresses defined in RFC 1918, 'Address Allocation for Private Intranets. *(Accessible to the relevant ICT Personnel Only)*

Uncategorized- Sites not categorized in the Fortigate Master Database.

News and Media: Sites that offer current news and opinion, including those sponsored by newspapers, general-circulation magazines, or other media.

Alternative Journals - Online equivalents to supermarket tabloids and other fringe publications.

Productivity PG: Sites that offer access to advertising and internet forums

Advertisements - Sites that provide advertising graphics or other ad content files.

Freeware and Software Download - Sites whose primary function is to provide freeware and software downloads. *(Accessible to the relevant ICT Personnel Only)*

Instant Messaging - Sites that enable instant messaging.

Message Boards and Forums - Sites that host message boards, bulletin boards, and other unaffiliated discussion forums.

Online Brokerage and Trading - Sites that support active trading of securities and management of investments.

Pay-to-Surf - Sites that reward users for Internet activity such as viewing Web Sites, advertisements, or email. *(Accessible to the relevant ICT Personnel Only)*

Racism and Hate: Sites that promote the identification of racial groups, the denigration or subjection of groups, or the superiority of any group.

Religion: Sites that promote or offer views on religion

Non-Traditional Religions and Occult and Folklore - Sites that provide information about or promote religions not specified in Traditional Religions or other unconventional, cultic, or folkloric beliefs and practices.

Traditional Religions - Sites that provide information about or promote Bahai, Buddhism, Christian Science, Christianity, Hinduism, Islam, Judaism, Mormonism, Shinto, and Sikhism, as well as atheism.

Security PG: Sites that contain potentially harmful content

Botnets - sites that host the command-and-control centers for networks of bots that have been infiltrated into users' computers. Excludes Web crawlers. *(Accessible to the relevant ICT Personnel Only)*

Keyloggers - Sites or pages that download programs that run in the background recording all keystrokes, and which may also send those keystrokes (potentially including passwords or confidential information) to an external party. *(Accessible to the relevant ICT Personnel Only)*

Malicious Embedded Link - Sites that are infected with a malicious link. *(Accessible to the relevant ICT Personnel Only)*

Malicious Embedded iFrame - Sites that are infected with a malicious iframe. *(Accessible to the relevant ICT Personnel Only)*

Malicious Web sites - Sites that contain code that may intentionally modify end-user systems without their consent and cause harm. *(Accessible to the relevant ICT Personnel Only)*

Phishing and Other Frauds - Sites that counterfeit legitimate business sites for the purpose of eliciting financial or other private information from users. *(Accessible to the relevant ICT Personnel Only)*

Potentially Unwanted Software - Sites that use technologies that alter the operation of the user's hardware, software, or network in ways that diminish control over the user experience, privacy, or the collection and distribution of personal information. *(Accessible to the relevant ICT Personnel Only)*

Spyware - Sites or pages that download software that, without the user's knowledge, generate HTTP traffic (other than simple user identification and validation). *(Accessible to the relevant ICT Personnel Only)*

Suspicious Embedded Link - Sites suspected of being infected with a malicious link. *(Accessible to the relevant ICT Personnel Only)*

Shopping: Sites that support the online purchase of consumer goods and services except: sexual materials, lingerie, swimwear, investments, medications, educational

materials, computer software or hardware, alcohol, tobacco, travel, vehicles and parts, weapons.

Internet Auctions - Sites that support the offering and purchasing of goods between individuals.

Real Estate - Sites that provide information about renting, buying, selling, or financing residential real estate.

Society and Lifestyles: Sites that provide information about matters of daily life, excluding entertainment, health, hobbies, jobs, sex, and sports.

Alcohol and Tobacco - Sites that provide information about, promote, or support the sale of alcoholic beverages or tobacco products or associated paraphernalia.

Blogs and Personal Sites - Sites that host blogs and personal sites.

Gay or Lesbian or Bisexual Interest - Sites that provide information about or cater to gay, lesbian, or bisexual lifestyles, but excluding those that are sexually or issue-oriented.

Hobbies - Sites that provide information about or promote private and largely sedentary pastimes, but not electronic, video, or online games.

Personals and Dating - Sites that assist users in establishing interpersonal relationships, excluding those intended to arrange for sexual encounters.

Restaurants and Dining - Sites that list, review, advertise, or promote food, dining, or catering services.

Social Networking - Sites of web communities that provide users with means for expression and interaction (For example Facebook.com etc).

Special Events: Sites devoted to a current event that requires separate categorization.

Sports: Sites that provide information about or promote sports, active games, and recreation.

Sport Hunting and Gun Clubs - Sites that provide information about or directories of gun clubs and similar groups, including war-game and paintball facilities.

Tasteless: Sites with content that is gratuitously offensive or shocking, but not violent or frightening. Includes sites devoted in part or whole to scatology and similar topics or to improper language, humor, or behavior.

Travel: Sites that provide information about or promote travel-related services and destinations.

Vehicles: Sites that provide information about or promote vehicles, including those that support online purchase of vehicles or parts.

Violence: Sites that feature or promote violence or bodily harm, including self-inflicted harm; or that gratuitously display images of death, gore, or injury; or that feature images or descriptions that are grotesque or frightening and of no redeeming value.

Weapons: Sites that provide information about, promote, or support the sale of weapons and related items.

User-Defined: User-defined category.

Appendix B

Category	Sub category	Basic	Custom	Technical
Adult Material		X		X
	Sex	X		X
	Nudity	X		X
	Adult Content	X		X
	Lingerie and Swimsuit			
	Sex Education			
	ETC			
Advocacy Groups				
Business and Economy				
	Financial Data and Services			
	Hosted Business Applications			
	ETC			
Bandwidth Consuming		X		X
	Internet Radio and TV	X		X
	Streaming Media	X		X
	Peer-to-Peer File Sharing	X	X	
	Personal Network Storage and Backup	X	X	
	Internet Telephony			
Drugs				
	Marijuana			
	Abused Drugs			
	Supplements and Unregulated Compounds			
	Prescribed Medications			
Education				
	Reference Materials			
	Cultural Institutions			
	Educational Institutions			
	Educational Materials			
Entertainment				
	MP3 and Audio Download Services	X		X

GLOBAL BP SOLUTIONS,LLC

Category	Sub category	Basic	Custom	Technical
Gambling		X		X
Games		X		X
Government				
	Military			
	Political Organizations			
Health				
illegal or Questionable		X		X
Information Technology				
	Search Engines and Portals			
	Computer Security			
	Web Collaboration			
	Hacking	X	X	
	Proxy Avoidance	X	X	
	URL Translation Sites	X	X	
	Web Hosting	X	X	
	Web and Email Spam	X	X	
Internet Communication				
	General Email	X		
	Organizational Email	X		
	Web Chat	X		
	Text / Media Messaging	X		
Job Search				
Militancy & Extremist		X		X

GLOBAL BP SOLUTIONS,LLC

Category	Sub category	Basic	Custom	Technical
Miscellaneous		X		X
	Images (Media)	X		X
	Dynamic Content	X		X
	Image Servers	X		X
	Private IP Addresses	X	X	
	File Download Servers	X	X	
	Network Errors	X	X	
	Content Delivery Networks			
	Uncategorized			
News and Media				
	Alternative Journals			
Productivity PG		X		X
	Message Boards and Clubs	X		X
	Advertisements	X		X
	Online Brokerage and Trading	X		X
	Instant Messaging	X		X
	Freeware and Software Download	X	X	
	Pay-to-Surf	X	X	
Racism & Hate		X		X
Religion				
	Traditional Religions			
	Non-Traditional Religions and Occult and Folklore			
Security		X	X	
	Spyware	X	X	
	Malicious Web Sites	X	X	
	Keyloggers	X	X	
	Phishing and Other Frauds	X	X	
	Potentially Unwanted Software	X	X	
	Bot Networks	X	X	
	Suspicious Embedded Link	X	X	
	Malicious Embedded iFrame	X	X	
	Malicious Embedded Link	X	X	
Shopping				
	Internet Auctions			
	Real Estate			

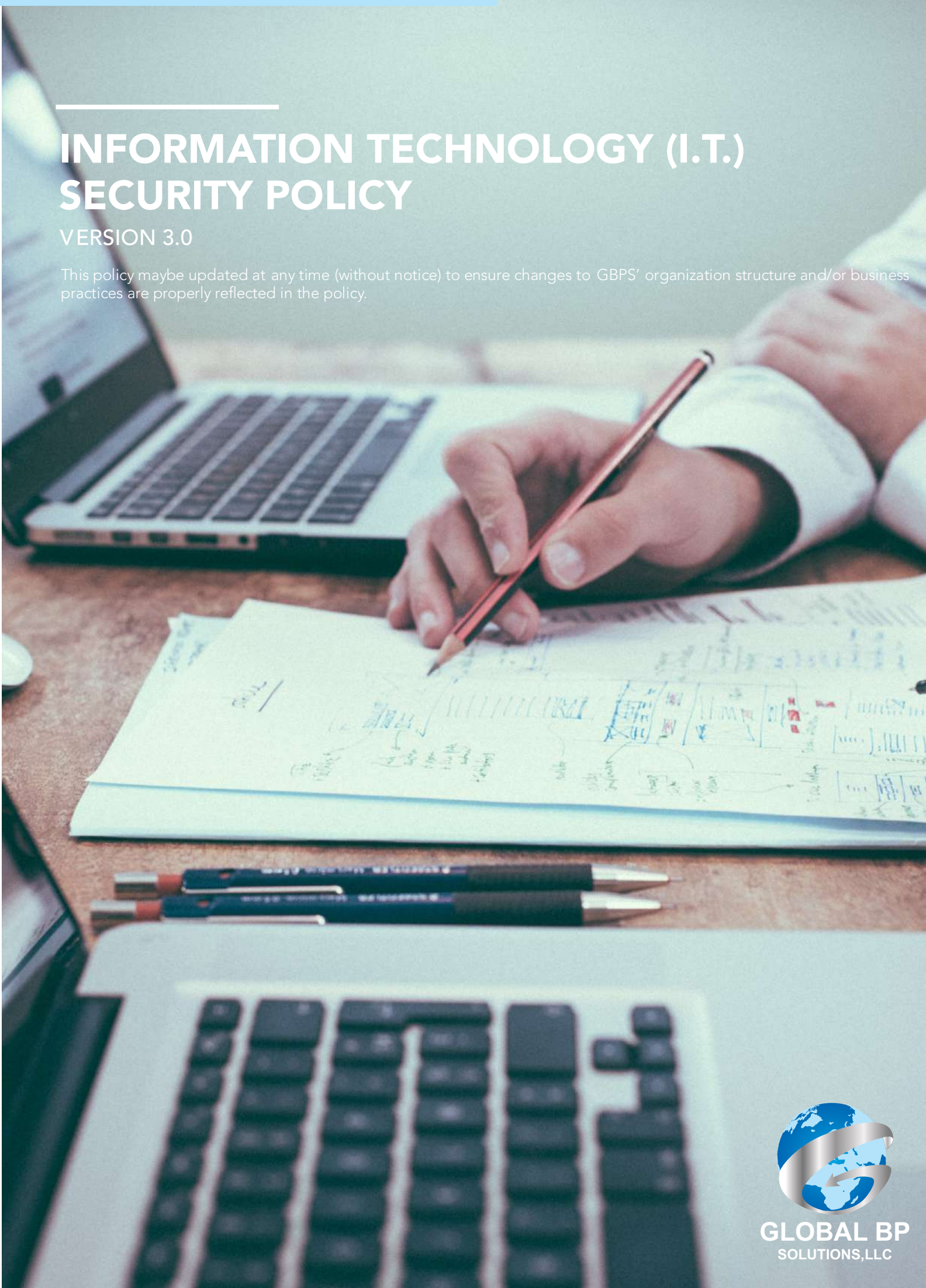
GLOBAL BP SOLUTIONS,LLC

Category	Sub category	Basic	Custom	Technical
Social Organizations				
	Service and Philanthropic Organizations			
	Social and Affiliation Organizations			
	Professional and Worker Organizations			
Society & Lifestyles				
	Alcohol and Tobacco			
	Hobbies			
	Restaurants and Dining			
	Gay or Lesbian or Bisexual Interest			
	Social Networking	X		X
	Blogs and Personal Sites	X		X
	Personals and Dating	X		X
Special Events				
Sports				
	Sport Hunting and Gun Clubs	X		
Tasteless		X		X
Travel				
Vehicles				
Violence		X		X
Weapons		X		X
User Defined		X		X

INFORMATION TECHNOLOGY (I.T.) SECURITY POLICY

VERSION 3.0

This policy maybe updated at any time (without notice) to ensure changes to GBPS' organization structure and/or business practices are properly reflected in the policy.



GLOBAL BP
SOLUTIONS,LLC

Document Information

Title:	GBPS Information Technology (I.T.) Security Policy.
Purpose:	This is a general statement of policy in respect of Information Technology (I.T.) security for GBPS.
Author:	Information Security Team (IST) on behalf of GBPS.
Target Audience:	All GBPS staff, students, contractors, sub-contractors, agency staff and authorized third parties that use the organizations IT resources.
Superseded Documents:	All relevant local GBPS information security policies.
Related Documents:	*GBPS Information Technology Acceptable Use Policy*. *GBPS Electronic Communications Policy.* *GBPS Password Standards Policy.* *GBPS Encryption Policy.* *GBPS Access Control Policy.* *GBPS Remote Access Policy.* *GBPS Mobile Phone Device Policy.* *GBPS Data Classification & Handling Policy.* *GBPS Data Protection Breach Management Policy.* *GBPS Internet Content Filter Standard.* *GBPS Service Provider Confidentiality Agreement.* *GBPS Third Party Network Access Agreement.*
Review Date:	June 2019

GLOBAL BP SOLUTIONS,LLC

Document History

Version	Owner	Author	Publish Date
1.0	GBP	Information Security Team (IST)	June 2019

1.0 Purpose

The use of computer systems and the exchange of information electronically have increased rapidly in the area of healthcare. Within GBPS there is a growing reliance on computer systems to aid treatment, expand communications, and improve management and control. This growing dependence comes at a time when the number of threats and actual attacks on these computer systems is constantly increasing.

Information is one of our most important assets and each one of us has a responsibility to ensure the security of this information. Accurate, timely, relevant and properly protected information is essential to the successful operation of GBPS in the provision of services to our customers.

The purpose of this Information Technology (I.T.) Security Policy and its supporting policies, standards and guidelines is to define the security controls necessary to safeguard GBPS information systems and ensure the security, confidentiality, availability and integrity of the information held therein.

This policy is mandatory and by accessing any information or Information Technology (IT) resources which are owned or leased by GBPS, users are agreeing to abide by the terms of this policy.

2.0 Scope

This policy is authorised by GBPS Senior Management Team, the Managing Partners and represents GBPS' in its entirety.

This policy applies to all GBPS staff, client facing employees, students, contractors, sub-contractors, agency staff and authorized third party commercial service providers that use the organizations I.T. resources and/or process information on behalf of GBPS.

3.0 Definitions

A list of terms used throughout this policy are defined in *appendix A*.

4.0 Policy

It is the policy of GBPS to: -

> Implement human, organizational, and technological security controls to preserve the confidentiality, availability and integrity of its information systems and the information held therein;

Develop and maintain appropriate policies, procedures and guidelines to affect a high standard of information technology security, reflecting industry best practice;

Monitor, record and log all activity on GBPS network and use of its information technology resources

Comprehensively assess and manage risks to GBPS information systems and the information held therein;

Continuously review and improve GBPS information technology security controls, and rapidly determine the cause of any breach of security and minimize damage to information systems should any such incident occur;

Comply with all laws and regulations governing information technology security;

Establish information technology security education and awareness initiatives within GBPS.

5.0 Supporting Policies, Standards and Guidelines

There are a number of supporting GBPS policies, standards and guidelines to accompany this policy document. Each of these accompanying policies, standards and guidelines is published on the GBPS intranet and covers a specific area of information security.

All GBPS staff, client facing employees, students, contractors, sub-contractors, agency staff and third-party commercial service providers authorised to use GBPS's Information Technology (I.T.) resources are required to familiarize themselves with these accompanying policies, standards and guidelines and to work in accordance with them.

The following is a list of the accompanying policies, standards and guidelines.

5.1 Information Technology (I.T.) Acceptable Use Policy

The *Information Technology Acceptable Use Policy* outlines the correct and proper manner in which GBPS's Information Technology (I.T.) resources are to be used. It covers the following areas:

The use of computer accounts and passwords;
Confidentiality and privacy of information;
The use of computer hardware and software;
The use of laptop computers and other mobile computer devices;
The security of GBPS information, systems and computer devices;
Lost, stolen and damaged computer devices;
The use of GBPS telephone system;
Storage of information;
Backup of information;

Security of information;
Transfer and transport of information;
Disposal of information;
Tele-working / home-working;
Virus & Malicious Software Protection;
The unacceptable use of GBPS information technology resources

5.2 Electronic Communications Policy

The *Electronic Communications Policy* outlines the correct and proper manner in which GBPS's Email, Internet and facsimile (fax) facilities are to be used. It covers the following areas:

The confidentiality and privacy of email and fax messages;
The use of GBPS email, internet and facsimile (fax) facilities;
The transmission of confidential or personal information via email, internet and fax;
The legal status of GBPS email and fax messages;
The use and ownership of GBPS email accounts;
The use of third party and web-based email facilities;
Access to restricted and blocked internet content;
The installation or use of third-party internet facilities;
The unacceptable use of GBPS email, internet and facsimile (fax) facilities.

5.3 Password Standards Policy

The *Password Standards Policy* outlines the standard for the creation and use of secure passwords for use on GBPS's Information Technology (IT) resources. It covers the following areas:

The creation of secure passwords;
Minimum password length;
Composition and complexity of passwords;
The use and security of passwords.

5.4 Encryption Policy

The *Encryption Policy* outlines the acceptable use and management of encryption software throughout the Health Service Executive (GBPS). It covers the following areas:

Minimum level of encryption;
Approved Encryption Algorithms and Protocols;
Encryption of GBPS computer devices;
Encryption of GBPS storage devices;
Encryption of GBPS email and internet messages and traffic;
Encryption of GBPS wireless network traffic.

5.5 Access Control Policy

The *Access Control Policy* outlines the correct use and management of user level access controls within GBPS. It covers the following areas:

Ownership and management of GBPS information systems and networks;
Access to GBPS information systems and networks;
Access Account privileges;
Access Account registration;
Access Account management;
Access Account de-registration;
Access Security;
Monitoring and review of access account privileges.

5.6 Remote Access Policy

The *Remote Access Policy* outlines the standard for connecting to GBPS network from a computer or device located outside of GBPS network. It covers the following areas:

Remote access registration and management;
Third party remote access registration and management;
Security of remote access devices;
Monitoring and security of remote access connections.

5.7 Mobile Phone Device Policy

The *Mobile Phone Device Policy* outlines the acceptable use and management of GBPS mobile phone devices. It covers the following areas:

Criteria for assignment of GBPS mobile phone devices;
Approval of assignment, upgrade and replacement of mobile phone devices;
Procurement of mobile phones devices;
Usage requirements and restrictions;
Security;
Confidentiality & Privacy;
Lost or stolen mobile phone devices;
Disposal of mobile phone devices;
Monitoring of mobile phone device usage;
Processing of mobile phone device bills;
Health and safety;

5.8 Information Classification & Handling Policy

The *Data Classification & Handling Policy* outlines how GBPS information must be classified and handled according to its sensitivity. It covers the following areas:

The different classifications of GBPS Information;
How each class of information should be handled and processed;

5.9 Data Protection Breach Management Policy

The *Data Protection Breach Management Policy* outlines the approved management approach to be followed in the event of a GBPS data protection breach. It covers the following areas:

Identification and classification of a breach;
Containment and recovery;
Risk assessment;
Notification of a breach;
Evaluation and response.

5.10 Internet Content Filter Standard

The *Internet Content Filter Standard* outlines the categories of internet content which are accessible to GBPS employees and which are filtered (blocked). It covers the following areas:

Filter internet content;
Internet user access groups;
Access to filtered internet content.

5.11 Service Provider Confidentiality Agreement

The *Service Provider Confidentiality Agreement* outlines the obligations of commercial third-party service providers who are contracted by GBPS to provide data management services (i.e. data storage, hosting, application support, data transcription, data processing etc.). It covers the following areas:

How the service providers should handle GBPS data;
How the service provider should process GBPS data;
How the service provider should store GBPS data;
Data Encryption;
Data Transfer;
International Data Transfers;
GBPS's right to inspect and audit the service provider's data processing facilities.

5.12 Third Party Network Access Agreement

The *Third-Party Network Access Agreement* outlines the specific terms and conditions governing the access and use of Global BP Solutions (GBPS) network and information technology resources by a third party: It covers the following areas:

Terms and conditions governing access;
Default third party access privileges;
Security of third-party computer devices accessing GBPS network;
Monitoring of third-party access.

6.0 Roles & Responsibilities

6.1 Information Security Team (IST)

The IST Directorate is responsible for:

Approving and publishing the policy;

The annual review of policy;

Approving all changes and amendments to the policy.

6.2 ICT Directorate

The ICT Directorate is responsible for:

The identification, implementation and management of appropriate security controls necessary to safeguard GBPS's network (LAN/WAN) and supporting infrastructure;

The implementation of system-level security controls as defined by the information owner;

The provision of facilities for information backups on network file servers and other centralized information stores but excluding backups of the hard disks on individual computers;

The provision of services which enable authorised user's access to appropriate electronic information systems and data;

Liaising with and advising GBPS management, individual users and line managers on the appropriate actions to take in the event of an actual or suspected breach data security.

6.3 Information Owners

Information owners are responsible for:

The implementation of this policy and all other relevant policies within GBPS directorate or service they manage;

The ownership, management, control and security of the information processed by their directorate or service on behalf of GBPS;

The ownership, management, control and security of GBPS information systems used by their directorate or service to process information on behalf of GBPS;

Maintaining a list of GBPS information systems and applications which are managed and controlled by their directorate or service.

Making sure adequate procedures are implemented within their directorate or service, so as to ensure all GBPS employees, client facing employees, contractors, sub-contractors, agency staff and third parties that report to them are made aware of, and are instructed to comply with this policy and all other relevant policies;

Making sure adequate procedures are implemented within their directorate or service to ensure compliance of this policy and all other relevant policies;

6.4 Line Managers

Line Managers are responsible for:

The implementation of this policy and all other relevant GBPS policies within the business areas for which they are responsible;

Ensuring that all GBPS employees who report to them are made aware of and are instructed to comply with this policy and all other related GBPS policies;

Consulting with the HR Directorate in relation to the appropriate procedures to follow when a breach of this policy has occurred;

Consulting with the ICT Directorate in relation to the appropriate actions to be taken when an actual or suspected breach of data security has occurred.

6.5 Users

Each user is responsible for:

Complying with the terms of this policy and all other relevant GBPS policies, procedures, regulations and applicable legislation;

Respecting and protecting the privacy and confidentiality of the

information they process at all times;

Complying with instructions issued by the ICT Directorate on behalf of GBPS;

Reporting all misuse and breaches of this policy to their line manager immediately;

Reporting all actual or suspected breaches of data security to their line manager, GBPS I.T.

6.6 Internal Audit

Internal Audit are responsible for:

Providing assurance that information technology controls and procedures are operated in accordance with the policies, regulations and best practice.

6.7 Consumer Affairs

Consumer Affairs are responsible for:

Providing training and advice on data protection;

Liaising with and advising GBPS management, individual users and line managers on the appropriate actions to take in the event of an actual or suspected breach data security.

7.0 Policy Distribution & Awareness

Hard copies of the policy and its supporting policies, standards and guidelines will be available on request from the local ICT departments.

The ICT Directorate and/or the Information Security Team (IST) may make periodic policy announcements by email.

GBPS line managers will ensure that all existing and new staff, students', client facing employees, contractors, subcontractors, agency staff and third-party commercial service providers who report to them are made aware of and have access to the policy and its supporting policies, standards and guidelines.

8.0 Review & Update

This policy will be reviewed and updated annually or more frequently if necessary, to ensure that any changes to GBPS's organization structure and business practices are properly reflected in the policy.

Updates to the policy and the supporting policies, standards and guidelines will be made periodically and will be posted on GBPS intranet and/or announced by email broadcast.

9.0 Breaches of Security

For security and technical reasons GBPS reserves the right to monitor, record and log all use of its information technology resources and activity on GBPS network.

Any individual suspecting that there has been, or is likely to be a breach of data security must inform their line manager and their local ICT department immediately. The ICT department will advise the individual and their line manager on what action should be taken.

GBPS reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. GBPS staff, students, contractors, client facing employees, sub-contractors or agency staff who breach this policy maybe subject to disciplinary action, including suspension and dismissal as provided for in GBPS disciplinary procedures.

Appendix A

Authorization / Authorised: Official GBPS approval and permission to perform a particular task.

Availability: Ensuring that authorized users have access to information and associated assets whenever required.

Breach of Data Security: The situation where GBPS confidential or restricted data has been put at risk of unauthorized disclosure as a result of the loss or theft of the data or, the loss or theft of a computer or storage device containing a copy of the data or through the accidental or deliberate release of the data.

Confidentiality: Ensuring that information is only accessible to those users who are authorized to access the information.

GBPS Network: The data communication system that interconnects different wired and wireless GBPS Local Area Networks (LAN) and Wide Area Networks (WAN).

GBPS Network Server: A computer on GBPS network used to manage network resources.

Information Technology (I.T.) resources: Includes all computer facilities and devices, networks and data communications infrastructure, telecommunications systems and equipment, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords, and information and data that are owned or leased by GBPS.

Information: Any data in an electronic format that is capable of being processed or has already been processed.

Information Owner: The individual responsible for the management of a GBPS region, directorate or service;

Information Security: The preservation of confidentiality, integrity and availability of information.

Information System: A computerized system or software application used to access, record, store, gather and process information.

Integrity: Ensuring the accuracy and completeness of information and associated processing methods.

Line manager: The individual a user report directly to.

Process / Processed / Processing: Performing any manual or automated operation or set of operations on information including:

Obtaining, recording or keeping the information;
Collecting, organizing, storing, altering or adapting the information;
Retrieving, consulting or using the information;
Disclosing the information or data by transmitting, disseminating or otherwise making it available;
Aligning, combining, blocking, erasing or destroying the information.

Risk: The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.

Third Party Commercial Service Provider: Any individual or commercial company that have been contracted by GBPS to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, data management services, patient / client care and management services etc.) to GBPS.

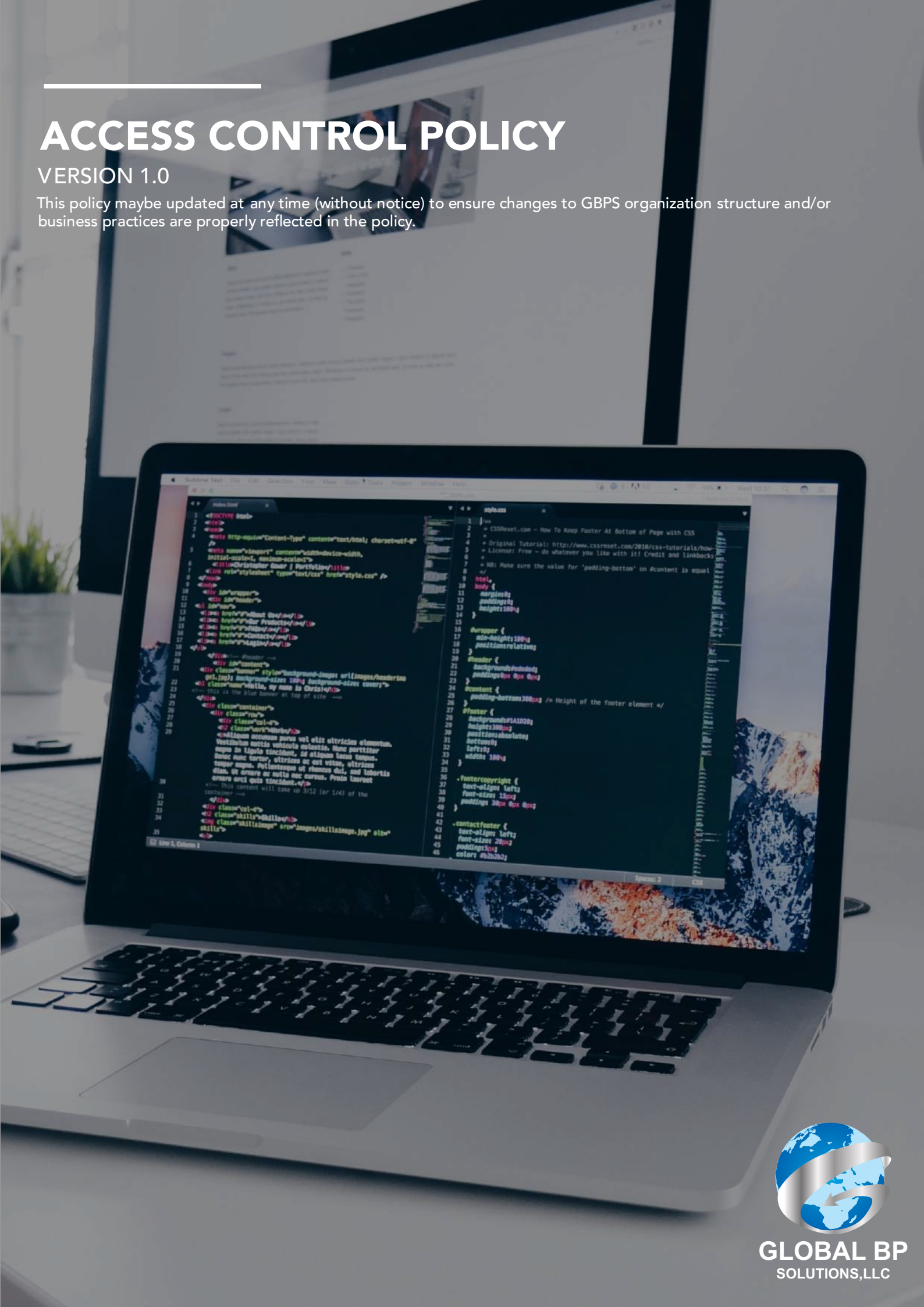
Threat: A potential cause of an incident that may result in harm to a system or organization.

Users: Any individual using any of GBPS's I.T. resources.

ACCESS CONTROL POLICY

VERSION 1.0

This policy maybe updated at any time (without notice) to ensure changes to GBPS organization structure and/or business practices are properly reflected in the policy.



GLOBAL BP
SOLUTIONS,LLC

Reader Information

Title:	GBPS Access Control Policy.
Purpose:	To define the correct use and management of system access controls within the GBPS.
Author:	Information Security Team (IST) on behalf of the GBPS.
Target Audience:	All users (including GBPS staff, students, contractors, sub- contractors, agency staff and authorized third party commercial service providers) of the GBPS's I.T resources.
Superseded Documents:	All local Access Control Policies and Procedures.
Related Documents:	GBPS Information Security Policy. GBPS I.T. Acceptable Use Policy. GBPS Password Standards Policy. GBPS Remote Access Policy. Third Party Network Access Agreement. GBPS Service Provider Confidentiality Agreement. GBPS Information Classification & Handling Policy.

Document History

Version	Owner	Author	Publish Date
1.0	GBPS	Information Security Team (IST)	June 2019

1.0 Purpose

Global BP Solutions (GBPS) is required to ensure the security and confidentiality of the information it processes on behalf of its clients, patients and employees.

GBPS is committed to the correct use and management of access controls throughout the organization. Insufficient access controls or unmanaged access to information could lead to the unauthorized disclosure or theft of this information, fraud and possible litigation. The purpose of this policy is to define the correct use and management access controls within the GBPS.

This policy is mandatory and by accessing any Information Technology (I.T.) resources which are owned or leased by the GBPS, users are agreeing to abide by the terms of this policy.

2.0 Scope

This policy represents the GBPS's national position and takes precedence over all other relevant policies which are developed at a local level. The policy applies to:

All Information Technology (I.T.) resources provided by the GBPS;

All GBPS information systems and network domains;

All users (including GBPS staff, students, contractors, sub-contractors, agency staff and authorized third party commercial service providers) of the GBPS's I.T resources;

All connections to (locally or remotely) the GBPS network Domains (LAN/WAN/WiFi);

All connections made to external networks through the GBPS network.

3.0 Definitions

A list of terms used throughout this policy are defined in *Appendix A*.

4.0 Policy

4.1 Principles of Access Control

Where technically feasible all GBPS Information Technology (I.T.) resources must be password protected.

Each GBPS information system must have a designated information owner who is responsible for managing and controlling access to the system. The information owner must hold a position within the GBPS and he/she must approve and sign all requests for access to the system. Alternatively, the information owner may nominate a member(s) of their management team who will have the authority to sign and approve requests for access to the system on their behalf. The information owner must forward the list of his/her nominees to the designated system administrator.

The ICT Directorate is the designated owner of all GBPS network domains. Each GBPS network domain must have a designated network administrator(s) who is responsible for the day to day administration of the network domain including the creation and management of network domain access accounts for authorized users.

Access to GBPS information systems and networks must be strictly controlled by a formal written registration and de-registration process.

Access to GBPS information systems must be controlled by the use of individual user access accounts. The use of generic or group access accounts to access GBPS Information Systems strictly prohibited.

Access to GBPS network domains will generally be controlled by the use of individual user access account's, however the use of generic / group access accounts will be permitted on nominated computer devices that meet approved criteria.

4.2 Account Privileges

Access rights and privileges to GBPS information systems and network domains must be allocated based on the specific requirement of a user's GBPS role / function rather than on their status

The criteria used for granting access privileges must be based on the principle of "least privilege" whereby authorized users will only be granted access to information system and network domains which are necessary for them to carry out the responsibilities of their GBPS role or function.

Care must be taken to ensure that access privileges granted to users do not unknowingly or unnecessarily undermine essential segregation of duties.

The creation of user access accounts with special privileges such as administrators must be rigorously controlled and restricted to only those users who are responsible for the management or maintenance of the information system or network. Each administrator must have a specific admin level account, which is only used for system administrative purposes, and is kept separate from their standard user access account

4.3 Account Registration

4.3.1 Information System Access Accounts

Access to GBPS information Systems will be controlled by the use of individual user access accounts. The use of generic / group access accounts is not permitted under any circumstances on GBPS information systems.

All new requests for access to information systems must be made in writing using the ***GBPS System Access Request Form***.

Line managers must complete the request on behalf of a new user and send this onto the designated information owner or his/her nominee for their approval. The request must be clearly marked '**New Access**'

Information owners or their nominees must formally authorize and sign all new access requests. Once a request for access has been approved, the information owner or his/her nominee must sign the *GBPS System Access Request Form* and forward this onto the system administrator for the user account to be created.

System administrators must only create new user accounts when they have received a signed *GBPS System Access Request Form.*

4.3.2 Network Domain Access Accounts

Access to GBPS network domains will generally be controlled by the use of individual user access account's, however the use of generic / group access accounts will be permitted on nominated computer devices that meet approved criteria. (*see section 4.3.3*)

All new requests for access to a GBPS network domain must be made in writing using the *GBPS Network Domain Access Request Form.*

Line managers must complete the request on behalf of a new user and send this onto ICT Directorate. The request must be clearly marked **'New Access'.**

Network administrators must only create new user accounts when they have received a signed *GBPS Network Domain Access Request Form.*

4.3.3 Generic / Group Network Domain Access Accounts

The use of generic / group access accounts is permitted on nominated computer devices that satisfy the following criteria:

1) Computers need to remain logged onto the GBPS network throughout the day to facilitate individual users.

2) A single network computer is used by a number of different users throughout the day to facilitate access to information systems using the users individual log on credentials (e.g. computers on a hospital ward)

Where a generic / group access account is created on a GBPS network domain, the generic / group access account must have an identified designated account owner who is responsible for the management and use of the generic / group access account.

GBPS network domain generic / group access accounts will only have access to an agreed set of GBPS information systems and will not under any circumstances have access to GBPS email or internet services**.** Limited network resources will be granted to a local named shared folder.

4.3.4 Third Party Access Accounts

Where there is a business need and with the approval of a GBPS information owner or his/her nominee third party commercial service providers maybe granted access to the GBPS network and information systems.

Third party commercial service provider access requests must be sponsored by a GBPS information owner or his/her nominee and submitted to the ICT Directorate in writing using the *GBPS Third Party Access Request Form.*

The information owner or his/her nominee must complete the request on behalf of the third party and forward it to the ICT Directorate along with the following documents:

1) A copy of the *GBPS Third Party Network Access Agreement* signed by the third-party commercial service provider.

2) A copy of the *GBPS Service Provider Confidentiality Agreement* signed by the third-party commercial service provider.

Under no circumstances will third party commercial service providers be granted access to the GBPS network and information systems until the ICT directorate has received the appropriate documentation.

Third party commercial service provider access privileges will be agreed on a case by case basis. The third-party commercial service provider must liaise with the GBPS to establish the minimum privileges required by them in order for them to complete the service they have been contracted to perform.

Local access (on-site) to the GBPS network and information systems may be granted on a temporary basis only as and when the need arises. Remote access connections may be set up on a more permanent basis for ongoing information system or network support purposes.

4.3.5 Remote Access Accounts

All remote access must be used and managed in accordance with the *GBPS Remote Access Policy.*

Requests from users for password resets must only be performed once the user's identity has been verified by the appropriate system administrator or network administrator (for example: a user's identity maybe verified by the provision of their GBPS personnel number).

Existing users who require additional access privileges on an information system must obtain the written authorization of the designated information owner or

his/her nominee. As per section **4.3.1** of this policy, line managers must initiate the requests using the *GBPS System Access Request Form* and forward this to the designated information owner or his/her nominee. The request must be clearly marked '**Amend Current Access**' to avoid the creation of multiple accounts for the same user.

Existing users who require additional access privileges on a network domain (for example file shares etc.) must make their request in writing. As per section **4.3.2** of this policy, line managers must initiate the request using the *GBPS Network Domain Access Request Form* and forward this to the ICT Directorate. The request must be clearly marked '**Amend Current Access**' to avoid the creation of multiple accounts for the same user.

The access accounts of users taking career breaks, going on maternity leave or those on long term sick leave must be suspended until such a time as they return to work. Requests for account suspensions must be made in writing by the user's line manager using the *GBPS Suspend / Remove Access Request Form* and forwarded to the ICT Directorate and the appropriate system administrator(s). The request should be clearly marked '**Suspend User Account**'.

The access accounts of users who are about to change roles or transfer to another GBPS directorate or service area, must be reviewed to ensure access account privileges that are no longer required by the user in their new role are removed. In such circumstances the user's existing line manager must request the removal of the unnecessary account privileges. The request must be made in writing using the *GBPS Suspend / Remove Access Request Form* and forwarded to the ICT Directorate or the appropriate system administrator before the user changes role or transfers. The request should be clearly marked '**Removal of User Account Privileges'**.

4.5 Account De-Registration

As soon as a user leaves the employment of the GBPS all his/her information systems and network access accounts must be revoked immediately. Line managers must request the deletion of a user's access accounts as soon as they have been informed by the user that they are leaving the employment of the GBPS. The requests must be made in writing using the *GBPS Suspend / Remove Access Request Form*

and forwarded to the ICT Directorate and the appropriate system administrator(s). The request should be clearly marked **'Delete User Account'** and made in advance of the users last day.

System administrators and network administrators must revoke user accounts at the requested date and time after the receipt of a properly completed *GBPS Suspend / Remove Access Request Form.*

4.6 Security

Access to all information systems and networks must be controlled via strong password authentication schemes.

User access accounts must be created in such a way that the identity of each user can be established at all times during their usage. Each user access account must be unique and consist of at least a user name and password set. All passwords created must be in-line with the requirement of the *GBPS Password Standards Policy.*

Where possible GBPS information systems and networks must be configured to:

1) Force users to change their password at their first logon. Where this is not possible, users must be instructed to manually change their password, the first time they logon to a GBPS information system or network.

2) Automatically 'lock' a user account after a number of consecutive failed login attempts.

3) Automatically 'lock' or log out user accounts after 30 minutes of inactivity. Where this is not possible, users must be instructed to manually log off or 'lock' their GBPS computer device (using *Ctrl+Alt+Delete* keys) when they have to leave it unattended for any period of time and at the end of the each working day.

When available audit logging and reporting must be enabled on all information systems and networks.

4.7 Monitoring & Review

Information owners or their nominees must continually monitor access to their information systems. They must perform quarterly reviews of the systems they are responsible for to ensure:

1) That each user access account and the privileges assigned to that account are appropriate and relevant to that user's current role or function;

2) That the information system and the information processed by the system is only accessed and used by authorized users for legitimate reasons.

System administrators and network administrators must conduct a system/network domain review at least once every quarter. User access accounts which have been inactive for 60 consecutive days or more must be suspended unless instructed otherwise by the user's line manager. Suspended user accounts to be marked for deletion, unless instructed otherwise by the user's line manager.

5.0 Roles & Responsibilities

5.1 Information Owner

Each designated information owner is responsible for:

The implementation of this policy and all other relevant policies within the GBPS directorate or service they manage;

The ownership, management, control and security of the information processed by their directorate or service on behalf of the GBPS;

The ownership, management, control and security of GBPS information systems used by their directorate or service to process information on behalf of the GBPS;

Maintaining a list of GBPS information systems and applications which are managed and controlled by their directorate or service.

Making sure adequate procedures are implemented within their directorate or service, so as to ensure all GBPS employees, third parties and others that report to them are made aware of, and are instructed to comply with this policy and all other relevant policies;

Making sure adequate procedures are implemented within their directorate or service to ensure compliance of this policy and all other relevant policies;

Ensuring adequate backup procedures are in place for the information system they are responsible for;

Ensuring all access requests are evaluated based on the approved criteria;

Sponsoring and approving third party access requests (locally or remotely) to the GBPS information system they are responsible for;

Designating system administrator(s) for the information system they are responsible for;

Furnishing the system administrator with a list of nominees who are authorised to approve and sign access requests to the information system on their behalf;

Conducting a quarterly review of the information system in accordance with this policy;

Informing the ICT Directorate & Consumer Affairs immediately in the event of a security incident involving the systems they are responsible for.

5.2 System Administrator

Each system administrator is responsible for:

Complying with the terms of this policy and all other relevant GBPS policies, procedures, regulations and applicable legislation;

Taking appropriate and prompt action on receipt of requests for user registration, change of privileges, password resets and de-registration of users in accordance with this policy and the procedures for the information system;

Taking appropriate and prompt action on receipt of requests for the suspension of a user account in accordance with this policy and the procedures for the information system;

Ensuring all passwords generated for new user accounts and password resets meet the requirements of the *GBPS Password Standards Policy;*

Notifying users of their system account details in a secure and confidential manner;

Ensuring that appropriate records of system activity, including all authorized user registrations, change of privileges and de- registration requests are maintained and made available for review to the appropriate personnel;

Conducting a quarterly review of the information system they are responsible in accordance with this policy;

Notifying the designated information owner, if they suspect a user is responsible for misusing the information system or is in breach of this policy;

Informing the designated information owner immediately in the event of a security incident involving the system;

Complying with instructions issued by the ICT Directorate on behalf of the GBPS.

5.3 Network Administrator

Each network administrator is responsible for:

Complying with the terms of this policy and all other relevant GBPS policies, procedures, regulations and applicable legislation;

Taking appropriate and prompt action on receipt of requests for user registration, change of 'privileges', password resets and de-registration of users in accordance with this policy and the procedures for the network;

Taking appropriate and prompt action on receipt of requests for the suspension of a user account in accordance with this policy and the procedures for the network;

Ensuring all passwords generated for new user accounts and password resets meet the requirements of the *GBPS Password Standards Policy;*

Notifying users of their system account details in a secure and confidential manner;

Ensuring that appropriate records of system activity, including all authorized user registrations, change of 'privileges' and de- registration requests are maintained and made available for review to the appropriate personnel;

Conducting a quarterly review of the network they are responsible in accordance with this policy;

Notifying a user's line manager, if they suspect the user is responsible for misusing the network or is in breach of this policy;

Informing the ICT Information Security Unit immediately in the event of a security incident involving the system.

5.4 ICT Directorate

The ICT Directorate is responsible for:

The management, control, ownership, security and integrity of all GBPS network domain (LAN/WAN) on behalf of the GBPS;

The implementation of this policy and all other relevant policies within the ICT Directorate;

Ensuring adequate procedures are in place to ensure compliance with this policy and all other relevant policies;

Designating a network administrator(s) for each GBPS network domain;

Conducting a quarterly review of the networks in accordance with this policy;

Providing information owners or their nominees with quarterly audit reports and user access lists for information systems which are directly managed by the ICT Directorate.

5.5 Line Managers

Each Line Manager is responsible for:

The implementation of this policy and all other relevant GBPS policies within the business areas for which they are responsible;

Ensuring that all members of staff who report to them are made aware of and are instructed to comply with this policy and all other relevant GBPS policies;

Ensuring complete and timely user access requests, for both permanent and temporary staff, are forwarded to the designated system owner allowing sufficient time for the creation of the required user account prior to the users start date;

Ensuring complete and timely user network access requests, for both permanent and temporary staff, are forwarded to the ICT Directorate allowing sufficient time for the creation of the required user account prior to the users start date;

Ensuring that each user they request access fulfills all the criteria (principle of "least privilege") for the requested information system and/or network;

Ensuring they make timely requests for the suspension of all user accounts belonging to members of their staff who are taking a career break, going on maternity leave or leave or those on long term sick leave;

Ensuring they make timely requests for the deletion of all user accounts belonging to members of their staff who are leaving the employment of the GBPS;

Consulting with the HR Directorate in relation to the appropriate procedures to follow when a breach of this policy has occurred.

5.6 Users:

Each user is responsible for:

Complying with the terms of this policy and all other relevant GBPS policies, procedures, regulations and applicable legislation;

Respecting and protecting the privacy and confidentiality of the information systems and network they access, and the information processed by those systems or networks;

Ensuring they only use user access accounts and passwords which have been assigned to them;

Ensuring all passwords assigned to them are kept confidential at all times and not shared with others including their co-workers or third parties;

Changing their passwords at least every 60 days or when instructed to do so by designated system administrators, network administrators or the ICT Directorate;

Complying with instructions issued by designated information owners, system administrators, network administrators and/or the ICT Directorate on behalf of the GBPS;

Reporting all misuse and breaches of this policy to their line manager.

6.0 Enforcement

The GBPS reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. GBPS staff, students, contractors, sub-contractors or agency staff who breach this policy maybe subject

to disciplinary action, including suspension and dismissal as provided for in the GBPS disciplinary procedure.

Breaches of this policy by a third-party commercial service provider, may lead to the withdrawal of GBPS information technology resources to that third-party commercial service provider and/or the cancellation of any contract(s) between the GBPS and the third-party commercial service provider.

7.0 Review & Update

This policy will be reviewed and updated annually or more frequently if necessary, to ensure any changes to the GBPS's organization structure and business practices are properly reflected in the policy.

Appendix A

Access: All local or remote access to the GBPS network and information systems.

Authorization / Authorised: Official GBPS approval and permission to perform a particular task.

Backup: The process of taking copies of important files and other information stored on a computer to ensure they will be preserved in case of equipment failure or loss/theft etc.

Confidential information: (As defined by the *GBPS Information Classification & Handling Policy*) Information which is protected by Irish and/or E.U. legislation or regulations, GBPS policies or legal contracts. The unauthorized or accidental disclosure of this information could adversely impact the GBPS, its patients, its staff and its business partners. Some examples of confidential information include:

Patient / client / staff personal data (Except that which is restricted)
Patient /client / staff medical records (Except that which is restricted)
Unpublished medical research
Staff personal records
Financial data / budgetary Reports
Service plans / service performance monitoring reports
Draft reports
Audit reports
Purchasing information
Vendor contracts / Commercially sensitive data
Data covered by Non-Disclosure Agreements
Passwords / cryptographic private keys
Data collected as part of criminal/HR investigations
Incident Reports

Generic / Group Access Account: An access account that is intended for use by a number of different people and not an individual user and as such is not derived from a single user's name.

GBPS Network: The data communication system that interconnects different GBPS Local Area Networks (LAN) and Wide Area Networks (WAN).

Information: Any data in an electronic format that is capable of being processed or has already been processed.

Information Owner: The individual responsible for the management of a GBPS directorate or service (GBPS National Director **(**or equivalent)).

Information Technology (I.T.) resources: Includes all computer facilities and devices, networks and data communications infrastructure, telecommunications systems and equipment, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords, and information and data that are owned or leased by the GBPS.

Information System: A computerized system or software application used to access, record, store, gather and process information.

Line manager: The individual a user report directly to.

Network Administrators: These are the individuals responsible for the day to day management of a GBPS network domain. Also includes GBPS personnel who have been authorised to create and manage user accounts and passwords on a GBPS network domain.

Network Domain: A set of connected network resources (Servers, Computers, Printers, Applications) that can be accessed and administered as group with a common set of rules

Personal Information: Information relating to a living individual (i.e. GBPS employee, client or patient) who is or can be identified either from the Information or from the information in conjunction with other information. For example: - an individual's name, address, email address, photograph, date of birth, fingerprint, racial or ethnic origin, physical or mental health, sexual life, religious or philosophical beliefs, trade union membership, political views, criminal convictions etc.

Privacy: The right of individual or group to exclude themselves or information about themselves from being made public.

Process / Processed / Processing: Performing any manual or automated operation or set of operations on information including:

Obtaining, recording or keeping the information;
Collecting, organizing, storing, altering or adapting the information;
Retrieving, consulting or using the information;
Disclosing the information or data by transmitting, disseminating or otherwise making it available;
Aligning, combining, blocking, erasing or destroying the information.

Remote Access: Any Connection to the GBPS network(s) or information systems that originates from a computer or device located outside of the GBPS network.

Restricted Information: (As defined by the *GBPS Information Classification & Handling Policy*) Highly sensitive confidential information**.** The unauthorized or accidental disclosure of this information would seriously and adversely impact the GBPS, its patients, its staff and its business partners. Some examples of restricted information include:

Patient / client / staff sensitive restricted information (i.e. mental health status, HIV status, STD/STI status etc)
Childcare / Adoption information
Social Work information
Addiction Services information
Disability Services information
Unpublished financial reports
Strategic corporate plans
Sensitive medical research

System Administrator: The individual(s) charged by the designated system owner with the day to day management of GBPS information systems. Also includes the GBPS personnel and third parties who have been authorised to create and manage user accounts and passwords on these applications and systems.

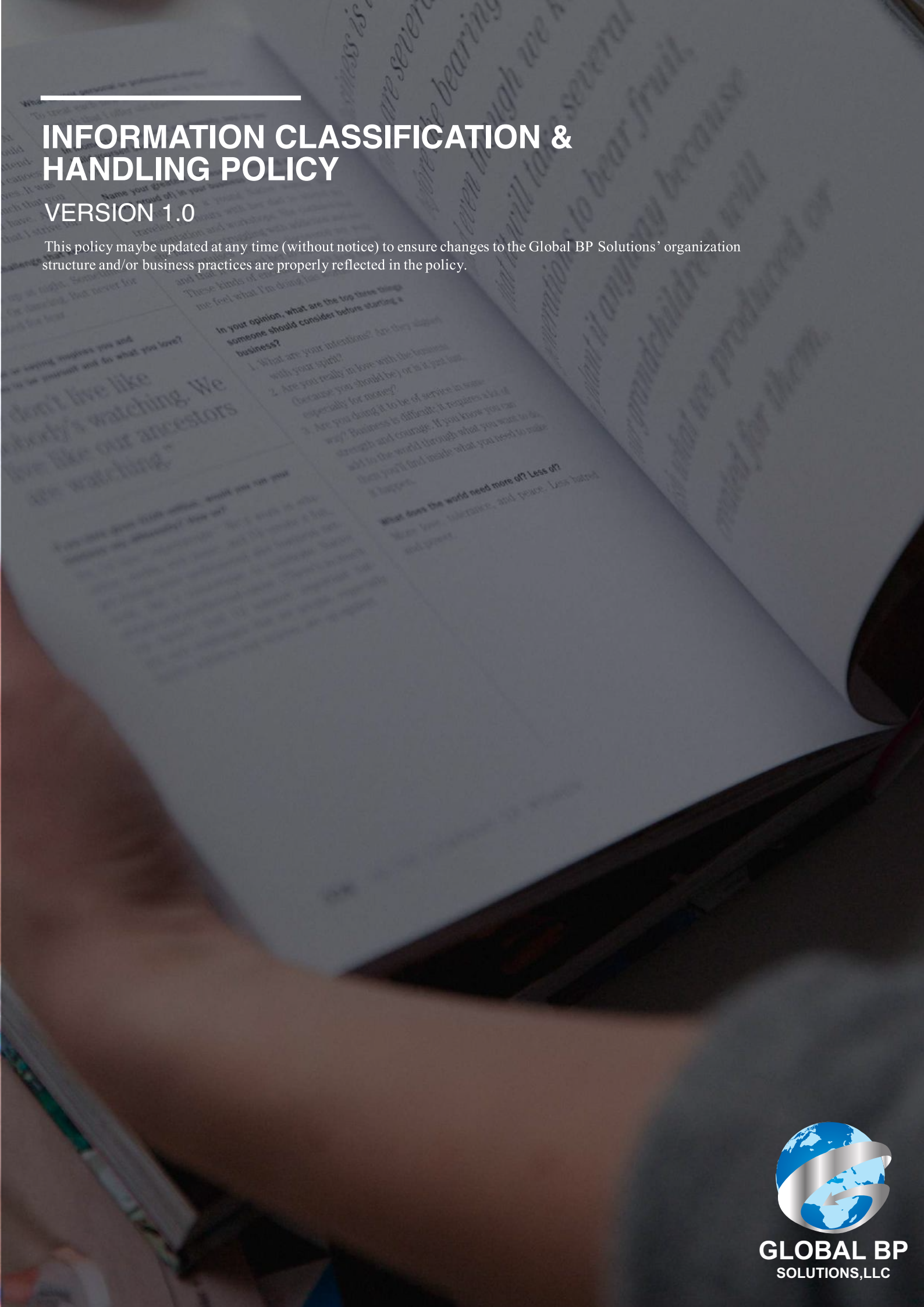
Third Party Commercial Service Provider: Any individual or commercial company that have been contracted by the GBPS to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, data management services, patient / client care and management services etc.) to the GBPS.

Users: Any authorized individual using any of the GBPS's IT resources.

INFORMATION CLASSIFICATION & HANDLING POLICY

VERSION 1.0

This policy maybe updated at any time (without notice) to ensure changes to the Global BP Solutions' organization structure and/or business practices are properly reflected in the policy.



GLOBAL BP
SOLUTIONS,LLC

Reader Information

Title:	GBPS Information Classification & Handling Policy.
Purpose:	To ensure all the information processed within the GBPS is classified and handled appropriately.
Author:	Information Security Team (IST) on behalf of the GBPS.
Target Audience:	All GBPS staff, students, contractors, sub-contractors, agency staff and authorized commercial service providers that use the organizations IT resources.
Superseded Documents:	All relevant local GBPS information classification policies and procedures.
Related Documents:	GBPS Information Security Policy. GBPS Electronic Communications Policy. GBPS Password Standards Policy. GBPS Encryption Policy. GBPS Mobile Phone Device Policy. GBPS Access Control Policy. GBPS Service Provider Confidentiality Agreement.

Document History

Version	Owner	Author	Publish Date
1.0	GBPS	Information Security Team (IST)	June 2019

1.0 Purpose

The Health Service Executive (GBPS) creates, collects and processes a vast amount of information in multiple formats every day. The GBPS has a responsibility to protect this information and ensure its confidentiality, integrity and availability.

The GBPS is committed to the correct and proper classification and handling of this information. This policy has been developed to assist the GBPS in applying a degree of sensitivity and criticality to all the information created, collected, processed and disseminated within the organization. The classification assigned places controls relating to the type of information and its need to remain confidential and secure.

The appropriate classification, handling and storage of information is the responsibility of every GBPS staff member. This policy is mandatory and applies to all GBPS staff, students, contractors, sub-contractors, agency personnel and third parties that have access to GBPS information

2.0 Scope

This policy represents the GBPS and takes precedence over all other relevant policies which are developed at a local level. The policy applies to all:

- GBPS Information;
- Client Information;
- Directorates and Service Areas;
- GBPS staff and students/interns/trainees;
- GBPS contractors and sub-contractors;
- Agency personnel working on behalf of the GBPS;
- Third party commercial service providers.

3.0 Definitions

A list of terms used throughout this policy are defined in *Appendix A*.

4.0 Policy

4.1 Information Classification

All information (irrespective of its format) owned, created, received, stored and processed by GBPS must be classified according to the sensitivity of its contents. Classification controls should take account of the organizational needs for sharing or restricting the information and the associated impacts and risks (e.g. consequences if information is handled inappropriately). All information owned, created, received, stored or processed by GBPS must be classified into one of following categories:

1) **Public**
2) **Internal**
3) **Confidential**
4) **Restricted**

The information classification matrix on *page 7* outlines the different categories of GBPS information and lists some examples of each.

4.1.1 Public Information

Public information is defined as information that is available to the general public and is intended for distribution outside the GBPS. There would be no impact on the GBPS, its staff, clients or patients if this type of information was mishandled or accidentally released. Some examples of public information include:

- Company brochures;
- Staff Brochures;
- News or media releases;
- Pamphlets;
- Advertisements;
- Web content;
- Job postings;
- Pastoral postings and care information;
- Public Health Information.

4.1.2 Internal Information

Internal information is defined as information that is only intended for internal distribution among GBPS staff, students, contractors, sub-contractors, agency staff and authorized third parties (i.e. service providers etc). In the majority of instances there would be no significant impact on the GBPS, its staff, clients or patients if this type of information was mishandled or accidentally released. Some examples of internal information include:

- Internal telephone directory;
- Internal policies & procedures;
- User manuals;
- Training manuals and documentation;
- Staff newsletters via mail-chimp & magazines;
- Inter-office memorandums (depending on the content);
- Business continuity plans.

4.1.3 Confidential Information

Confidential information is defined as information which is protected and solely for GBPS policies or legal contracts. The unauthorized or accidental disclosure of this information could adversely impact the GBPS, its patients, its staff and its business

partners.

Some examples of confidential information include:

- Patient / client / staff personal information (Except that which is restricted);
- Patient /client / staff medical records (Except that which is restricted);
- Unpublished medical research;
- Staff personal records;
- Financial information / budgetary reports;
- Service plans / service performance monitoring reports;
- Draft reports;
- Audit reports;
- Purchasing information;
- Vendor contracts / commercially sensitive information;
- Information covered by non-disclosure / confidentiality agreements;
- Passwords / cryptographic private keys;
- Information collected as part of criminal / HR investigations;
- Incident reports.

4.1.4 Restricted Information

Restricted information is defined as highly sensitive confidential information. The unauthorized or accidental disclosure of this information would seriously and adversely impact the GBPS, its patients, its staff and its business partners. Some examples of restricted information include:

- Patient / client / staff sensitive personal information (i.e. health status, Blood status, etc.);
- Childcare / adoption information;
- Social work information;
- Addiction services information;
- Disability services information;
- Unpublished financial reports;
- Strategic corporate plans;
- Sensitive medical research.

GBPS Information Classification Matrix				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Definition	Information that is available to the general public and intended for distribution outside the GBPS. This information may be freely disseminated without potential harm.	Information that is only intended for internal distribution among GBPS staff and authorised third parties (i.e. service providers, contractors/sub-contractors and agency staff).	Information that is protected by GBPS policies or legal contracts.	Highly sensitive confidential information
Examples The examples listed are only provided for guidance purposes and should not be seen as an exhaustive list.	• Patient/Client brochures; • Staff brochures; • News or media releases; • Pamphlets; • Advertisements; • Web content; • Job postings; • Public Health Information.	• Internal telephone directory; • Internal policies & procedures (excluding those published on the web); • User manuals; • Training manuals and documentation; • Staff newsletters & magazines; • Inter-office memorandums (depending on the content); • Business continuity plans.	• Patient / client / staff personal information (Except that which is restricted); • Patient / Client / Staff medical records (Except that which is restricted); • Unpublished medical research; • Staff personnel records; • Financial information / budgetary reports; • Service plans / service performance monitoring reports; • Audit reports; • Draft reports; • Vendor contracts / commercially sensitive information; • Information covered by non-disclosure / confidentiality agreements; • Passwords / cryptographic private keys; • Incident reports; • Information collected as part of criminal/HR investigations.	• Patient / client / staff sensitive personal information (i.e. health status, Blood status, etc.) • Patient services information; • Disability services information; • Unpublished financial reports; • Strategic corporate plans; • Sensitive medical research.
Possible consequences if information is mishandled	None	In the majority of instances, the unauthorized would not significantly impact the GBPS, its staff, its patients, or clients.	Unauthorized disclosure could adversely impact the GBPS, its patients, its staff, its clients and its business partners.	Unauthorized disclosure would seriously and adversely impact the GBPS, its staff, its patients, its clients and its business partners.

GLOBAL BP SOLUTIONS,LLC

4.2 Information Handling

All Information (irrespective of its format) owned, created, received, stored and processed by the GBPS must be handled appropriately according to its classification. The information handling matrix in ***Appendix B*** specifies how the different classifications of information must be handled.

5.0 Roles & Responsibilities

5.1 Information Owners

Information owners are responsible for:

- The full implementation of this policy and all other relevant policies within the GBPS directorate or service they manage;
- Ensuring all information (irrespective of its format) owned, created, received, stored and processed within the GBPS directorate or service they manage is classified and handled in accordance with this policy;
- Making sure adequate procedures are implemented within their directorate or service, so as to ensure all GBPS staff, students, contractors, sub-contractors, agency staff, third parties and others that report to them are made aware of, and are instructed to comply with this policy and all other relevant policies;
- Making sure adequate procedures and training programs are implemented within their directorate or service to ensure on-going compliance of this policy and all other relevant policies;

5.2 Line Managers

Line managers are responsible for:

- The implementation of this policy and all other relevant GBPS policies within the business areas for which they are responsible;
- Ensuring all information (irrespective of its format) owned, created, received, stored and processed within the GBPS business area they manage is classified and handled in accordance with this policy;
- Ensuring that all GBPS staff, students, contractors, sub-contractors and agency staff who report to them are made aware of, understand and have access to this policy and all other relevant GBPS policies;

- Ensuring that all GBPS staff, students, contractors, sub-contractors and agency staff who report to them are instructed to comply with this policy and all other relevant GBPS policies;

- Ensuring that all GBPS staff, students, contractors, sub-contractors and agency staff who report to them are provided with adequate information and training regarding the implementation of this policy and all other relevant GBPS policies

- Consulting with the HR Directorate in relation to the appropriate procedures to follow when a breach of this policy has occurred.

5.3 Staff

Each staff member is responsible for:

- Complying with the terms of this policy and all other relevant GBPS policies, procedures, regulations and applicable legislation;

- Ensuring all information (irrespective of its format) for which they are responsible is classified and handled in accordance with this policy;

- Reporting all misuse and breaches of this policy to their line manager.

5.4 Contractors, Sub-contractors & Agency Staff

Each contractor, sub-contractor or agency staff member is responsible for:

- Complying with the terms of this policy and all other relevant GBPS policies, procedures, regulations and applicable legislation;

- Ensuring all information (irrespective of its format) for which they are responsible is classified and handled in accordance with this policy;

- Reporting all misuse and breaches of this policy to their contracted GBPS line manager.

5.5 Third party commercial service providers

Third party commercial service providers are responsible for:

- Complying with the terms of this policy and all other relevant GBPS policies, procedures, regulations and applicable legislation;

- Ensuring all information (irrespective of its format) for which they are responsible is classified and handled in accordance with this policy;

- Reporting all misuse and breaches of this policy to their GBPS contact.

6.0 Enforcement

- The GBPS reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. GBPS staff, students, contractors, sub-contractors or agency staff who breach this policy maybe subject to disciplinary action, including suspension and dismissal as provided for in the GBPS disciplinary procedure.

- Breaches of this policy by a third-party commercial service provider, may lead to the withdrawal of GBPS information technology resources to that third-party commercial service provider and/or the cancellation of any contract(s) between the GBPS and the third-party commercial service provider.

7.0 Review & Update

This policy will be reviewed and updated annually or more frequently if necessary, to ensure any changes to the GBPS's organization structure and business practices are properly reflected in the policy.

Appendix A

Anonymized / Anonymization: The process of rendering information into an irrevocable form which does not identify any individual and can no longer be linked to an individual.
.

Authorization / Authorised: Official GBPS approval and permission to perform a particular task.

Backup: The process of taking copies of important files and other information stored on a computer to ensure they will be preserved in case of equipment failure, loss or theft etc.

Breach of Confidentiality: The situation where GBPS confidential or restricted information has been put at risk of unauthorized disclosure as a result of the loss or theft of the information or, the loss or theft of a computer device containing a copy of the information or through the accidental or deliberate release of the information.

Electronic Media: Any information that has been created and is stored in an electronic format, including but not limited to software, electronic documents, photographs, video and audio recordings.

Encryption / Encrypt: The process of converting (encoding) information from a readable form (plain text) that can be read by everyone into an unreadable form (cipher text) that can only be read by the information owner and other authorised persons.

Encryption Key: A piece of information (parameter usually a password) used to encrypt/decrypt information.

GBPS Network: The information communication system that interconnects different GBPS Local Area Networks (LAN) and Wide Area Networks (WAN).

GBPS Network Server: A computer on GBPS network used to provide network services and/or manage network resources.

Incinerate: Destruction by burning.

Information: Any information irrespective of the format that is capable of being processed or has already been processed.

Information Owner: The individual responsible for the management of a GBPS operation or directorate or service.

Information System: A computerized system or software application used to access, record, store, gather and process information.

Information Technology (I.T.) resources: Includes all computer facilities and devices, networks and information communications infrastructure, telecommunications systems and equipment, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords, and information and information that are owned or leased by the GBPS.

Line manager: The individual a user report directly to.

Macerate / Macerated: Destruction by dissolving in chemicals.

Mobile Computer Device: Any handheld computer device including but not limited to laptops, notebooks, tablet computers, iPads, smartphone devices (e.g. PDA, iPhone and Blackberry enabled devices, etc).

Mobile Phone Device: Any wireless telephone device not physically connected to a landline telephone system. Including but not limited to mobile phones, smartphone devices (e.g. PDA, iPhones, Blackberry enabled devices etc.), 3G/4G/GPRS mobile information cards. This does not include cordless telephones which are an extension of a telephone physically connected to a landline telephone system.

Personal information: Information relating to a living individual (i.e. GBPS employee, client or patient) who is or can be identified either from the information or from the information in conjunction with other information. For example: - an individual's name, address, email address, photograph, date of birth, fingerprint, racial or ethnic origin, physical or mental health, sexual life, religious or philosophical beliefs, trade union membership, political views, criminal convictions etc.

Personal Use: The use of the GBPS's Information Technology (IT) resources for any activity(s) which is not GBPS work-related.

Pulverize / Pulverized: Destruction by grinding into very small pieces or power**.**

Privacy: The right of individual or group to exclude themselves or information about themselves from being made public.

Process / Processed / Processing: Performing any manual or automated operation or set of operations on information including:

- Obtaining, recording or keeping the information;
- Collecting, organizing, storing, altering or adapting the information;
- Retrieving, consulting or using the information;
- Disclosing the information or information by transmitting, disseminating or otherwise making it available;
- Aligning, combining, blocking, erasing or destroying the information.

Removable Storage Device: Any optical or magnetic storage device or media, including but not limited to floppy disks, CD, DVD, magnetic tapes, ZIP disk, USB flash drive (i.e. memory stick/pen/keys), external/portable hard drives.

Third Party Commercial Service Provider: Any individual or commercial company that have been contracted by the GBPS to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, information management services, patient / client care and management services etc.) to the GBPS.

Appendix B

Information Handling Matrix

Information Classification & Handling Procedures				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Document Marking	No marking required	No marking required	The front page of all documents to be clearly marked "Confidential" and all subsequent pages to be marked "Confidential" in the header/footer section of the page or stamped appropriately.	The front page of all documents to be clearly marked "Restricted" and all subsequent pages to be marked "Restricted & Confidential" in the header/footer section of the page or stamped appropriately.
Printing, Scanning & Photocopying	No special precautions required.	No special precautions required.	Printing, scanning and photocopying of confidential information **must be kept to a minimum** and only when absolutely necessary. 1) Printers, Scanners and Photocopiers should be located within an area which is not accessible by the general public. 2) Always ensure original documents and copies are removed from printer, scanner or photocopier as soon as possible.	Printing, scanning and photocopying of restricted information **must be kept to a minimum** and only when absolutely necessary. 1) Printers, Scanners and Photocopiers should be located within an area which is not accessible by the general public. 2) Always ensure original documents and copies are removed from printer, scanner or photocopier as soon as possible.
Backup & Recovery	Backed up **DAILY**.	Backed up **weekly** & backup tapes should stored in a safe location when not in use	Backed up **daily**, preferably onto a secure GBPS network server. If backed up locally onto a backup tape instead of a server, then the backup tapes must be stored in a secure location such as a locked filing cabinet, drawer or a safe (preferably a fireproof safe) when not in use. The backup should be tested at least once a month to ensure you can recover the information from the backup tapes in the event of a system crash etc.	Backed up **daily**, preferably onto a secure GBPS network server. If backed up locally onto a backup tape instead of a server, the backup tapes must be stored in a secure location such as a locked filing cabinet, drawer or a safe (preferably a fireproof safe) when not in use. The backup should be tested at least once a month to ensure you can recover the information from the backup tapes in the event of a system crash etc.

GLOBAL BP SOLUTIONS,LLC

Information Classification & Handling Procedures				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Access to / disclosure of the information	Available to the general public	Generally made available to all staff, contractors, sub-contractors, agency staff and authorised third parties (i.e. service providers etc) on a need to know basis.	Confidential information must only be accessible **On a need to know basis.** Confidential information must only be: 1) Accessible to **GBPS staff** who have a valid GBPS business need to access the information or have been authorised to access the information by the designated GBPS information owner. 2) Released and disclosed to the **general public** in accordance with the relevant legislation 3) Released and disclosed to **outside organization's** in accordance with the relevant legislation and ACT. ***4)*** Processed (collected, hosted, disposed etc) by **third party service providers** who have a legal contract in place with the GBPS to provide information management services and have signed a copy of the *GBPS Server Provider Confidentiality Agreement*	Restricted information must only be accessible **On a need to know basis.** Restricted information must only be: 1) Accessible to **GBPS staff** who have a valid GBPS business need to access the information or have been authorised to access the information by the designated GBPS information owner. 2) Released and disclosed to the **general public** in accordance with the relevant legislation. 3) Released and disclosed to **outside organization's** in accordance with the relevant legislation and ACT. ***4)*** Processed (collected, hosted, disposed etc) by **third party service providers** who have a legal contract in place with the GBPS to provide information management services and have signed a copy of the *GBPS Server Provider Confidentiality Agreement*

GLOBAL BP SOLUTIONS,LLC

Information Classification & Handling Procedures				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Publication on the Intranet / Internet	Public information which is to be published on the GBPS intranet and internet sites must be authorised by the line manager of the GBPS section or service area who is responsible for the information.	Internal information which is to be published on the GBPS intranet and internet sites must be authorised by the line manager of the GBPS section or service area who is responsible for the information.	In accordance with the *GBPS Electronic Communications Policy* confidential information **must never** be published, posted or discussed on **any** internet sites, forums, message boards or chat rooms including those sites which are officially sanctioned by the GBPS	In accordance with the *GBPS Electronic Communications Policy* restricted information **must never** be published, posted or discussed on **any** internet sites, forums, message boards or chat rooms including those sites which are officially sanctioned by the GBPS
Breach of Confidentiality • Loss of information • Theft of information • Loss / theft of a computer device containing the information • Actual or suspected unauthorized access • Accidental disclosure	No special requirements	No special requirements	All information breaches involving the actual or suspected loss, theft or disclosure of confidential information must be reported and handled in accordance with the *GBPS Data Protection Breach Management Policy*	All information breaches involving the actual or suspected loss, theft or disclosure of restricted information must be reported and handled in accordance with the *GBPS Data Protection Breach Management Policy*

Storage of Electronic Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
GBPS network server	No special precautions required.	No special precautions required.	1) In accordance with the *GBPS I.T. Acceptable Use Policy* confidential information and GBPS information systems that store or process such information **should be stored/hosted on a GBPS network server** and not stored locally on the hard drive of a laptop or desktop computer. 2) Confidential information stored on a GBPS network server which is not stored as part of a GBPS information system, must be held within a secure folder which is only accessible by authorised staff.	1) In accordance with the *GBPS I.T. Acceptable Use Policy* restricted information and GBPS information systems that store or process such information **should be stored/hosted on a GBPS network server** and not stored locally on the hard drive of a laptop or desktop computer. 2) Restricted information stored on a GBPS network server which is not stored as part of a GBPS information system, must be held within a secure folder which is only accessible by authorised staff.
GBPS desktop computer	No special precautions required.	No special precautions required.	Strictly **prohibited** except where the 1) Storage is necessary for business or technical reasons and, *2)* Desktop computer is password protected in accordance with the *GBPS Password Standards Policy* and, 3) Desktop computer has been encrypted in accordance with the *GBPS Encryption Policy* and, 4) Information is backed up on a daily basis.	Strictly **prohibited** except where the 1) Storage is necessary for business or technical reasons and, *2)* Desktop computer is password protected in accordance with *the GBPS Password Standards Policy* and, 3) Desktop computer has been encrypted in accordance with the *GBPS Encryption Policy* and, 4) Information is backed up on a daily basis.

GLOBAL BP SOLUTIONS,LLC

Storage of Electronic Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
GBPS laptop computer	No special precautions required.	No special precautions required.	Strictly **prohibited** except where the 1) Storage is necessary for business and/or technical reasons and, *2)* Laptop is password protected in accordance with the *GBPS Password Standards Policy* and, 3) Laptop computer has been encrypted in accordance with the *GBPS Encryption Policy* and, 4) Information is backed up on a regular basis	Strictly **prohibited** except where the 1) Storage is necessary for business and/or technical reasons and, *2)* Laptop is password protected in accordance with the *GBPS Password Standards Policy* and, 3) The laptop computer has been encrypted in accordance with the *GBPS Encryption Policy* and, 4) Information is backed up on a regular basis
GBPS mobile computer device • Smart phone device, • Blackberry's • Tablet computer • Notebook computer • PDA • iPhone / iPad	No special precautions required.	No special precautions required.	Strictly **prohibited** except where the 1) Storage is necessary for business or technical reasons and, *2)* Mobile computer device is password protected in accordance with the *GBPS Password Standards Policy* and, 3) Mobile computer device has been encrypted in accordance with the *GBPS Encryption Policy* and, 4) Information is backed up on a regular basis	Strictly **prohibited** except where the 1) Storage is necessary for business or technical reasons and, 2) Mobile computer device is password protected in accordance with the *GBPS Password Standards Policy* and, 3) Mobile computer device has been encrypted in accordance with the *GBPS Encryption Policy* and, 4) Information is backed up on a regular basis

Storage of Electronic Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
GBPS removable storage devices • CD/DVD • External / portable hard drive • USB Memory Stick	No special precautions required.	No special precautions required.	Strictly **prohibited** except where the 1) Storage is necessary for business or technical reasons and, 2) Removable storage device or the confidential information stored on the device has been encrypted in accordance with the *GBPS Encryption Policy* and, 3) Information is backed up on a regular basis **Only GBPS approved USB memory sticks which are distributed by the ICT Directorate maybe used to store or transfer GBPS information**	Strictly **prohibited** except where the 1) Storage is necessary for business or technical reasons and, 2) Removable storage device or the restricted information stored on the device has been encrypted in accordance with the *GBPS Encryption Policy* and, 3) Information is backed up on a regular basis **Only GBPS approved USB memory sticks which are distributed by the ICT Directorate maybe used to store or transfer GBPS information**
GBPS photographic or video recording device • Digital cameras • Video cameras • Any devices which are capable of taking still or video recording	No special precautions required.	No special precautions required.	1) In accordance with the *GBPS I.T. Acceptable Use Policy* photographic and video recordings taken as part of patient/client treatment and care must be transferred from the photographic or video recording device onto a GBPS network server as soon as is practical. When the transfer is complete the photographic / video recording on the device should be deleted. 2) In the event that this cannot be carried out immediately the photographic or video recording device should be locked away securely when not in use.	1) In accordance with the *GBPS I.T. Acceptable Use Policy* photographic and video recordings taken as part of patient/client treatment and care must be transferred from the photographic or video recording device onto a GBPS network server as soon as is practical. When the transfer is complete the photographic / video recording on the device should be deleted. 2) In the event that this cannot be carried out immediately the photographic or video recording device should be locked away securely when not in use.

Storage of Electronic Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
GBPS audio recording device • Dictaphones • Recorders • Any devices which are capable of taking audio recordings	No special precautions required.	No special precautions required.	1) In accordance with the *GBPS I.T. Acceptable Use Policy* audio recordings taken as part of patient/client treatment and care must be transferred from the audio recording device onto a GBPS network server as soon as is practical. In the event that this cannot be carried out immediately the audio recording device should be locked away securely when not in use. 2) When the audio recordings have been transferred to a GBPS network server all local copies stored on the audio recording device should be deleted	1) In accordance with the *GBPS I.T. Acceptable Use Policy* audio recordings taken as part of patient/client treatment and care must be transferred from the audio recording device onto a GBPS network server as soon as is practical. In the event that this cannot be carried out immediately the audio recording device should be locked away securely when not in use. 2) When the audio recordings have been transferred to a GBPS network server all local copies stored on the audio recording device should be deleted
Staff personal devices (i.e. Where the device is the staff members personal property and is not owned or leased by the GBPS)	No special precautions required.	No special precautions required.	**Strictly prohibited in accordance with the** *GBPS I.T. Acceptable Use Policy*	**Strictly prohibited in accordance with the** *GBPS I.T. Acceptable Use Policy*
Third party off-site storage (i.e. where the storage of the information has been outsourced to a third-party company)	No special precautions required.	No special precautions required.	In accordance with the *GBPS I.T. Acceptable Use Policy* confidential information may only be hosted and stored off-site by third parties, provided the third party has signed a copy of the ***GBPS Server Provider Confidentiality Agreement***	In accordance with the *GBPS I.T. Acceptable Use Policy* confidential information may only be hosted and stored off-site by third parties, provided the third party has signed a copy of the the ***GBPS Server Provider Confidentiality Agreement***

GLOBAL BP SOLUTIONS,LLC

Storage of Electronic Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Email messages	No special precautions required.	No special precautions required.	Confidential information which is received via email **should not** remain permanently on a local computer once it has been read by the intended recipient. 1) Once the email has been read the confidential information contained within the email message should be moved to a secure folder (with restricted access) on a GBPS network server. 2) When the information has been moved to the server all local copies of the email message should be deleted (i.e. delete the copy of the email message in your email inbox and ensure you empty the contents of deleted emails folder). 3) Alternatively the email message and/or the confidential information maybe printed out and stored away in a secure manner (i.e. stored in locked filing cabinets or a secure lockable area with restricted access)	Restricted information which is received via email **should not** remain permanently on a local computer once it has been read by the intended recipient. 1) Once the email has been read the restricted information contained within the email message should be moved to a secure folder (with restricted access) on a GBPS network server. 2) When the information has been moved to the server all local copies of the email message should be deleted (i.e. delete the copy of the email message in your email inbox and ensure you empty the contents of deleted emails folder). 3) Alternatively the email message and/or the restricted information maybe printed out and stored away in a secure manner (i.e. stored in locked filing cabinets or a secure lockable area with restricted access)

GLOBAL BP SOLUTIONS,LLC

Storage of Paper Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Paper documents and other printed material	No special precautions required.	Reasonable precautions to prevent the risk of deterioration, loss and access by unauthorized third parties.	The information must be stored in such a way so as to ensure it is protected against: 1) Unauthorized access. The information should be locked away in a filing cabinet, drawer, safe or records room when it is not in use. 2) Environmental hazards (i.e. fire, flooding, temperature, humidity, atmospheric pollution etc) 3) Deterioration and/or loss	The information must be stored in such a way so as to ensure it is protected against: 1) Unauthorized access. The information should be locked away in a filing cabinet, drawer, safe or records room when it is not in use. 2) Environmental hazards (i.e. fire, flooding, temperature, humidity, atmospheric pollution etc) 3) Deterioration and/or loss
Microfilm and other image photo negative materials	No special precautions required.	Reasonable precautions to minimize the risk of deterioration, loss and access by unauthorized third parties.	The information must be stored in such a way so as to ensure it is protected against: 1) Unauthorized access. The information should be locked away in a filing cabinet, drawer, safe or records room when it is not in use. 2) Environmental hazards (i.e. fire, flooding, temperature, humidity, atmospheric pollution etc) 3) Deterioration and/or loss	The information must be stored in such a way so as to ensure it is protected against: 1) Unauthorized access. The information should be locked away in a filing cabinet, drawer, safe or records room when it is not in use. 2) Environmental hazards (i.e. fire, flooding, temperature, humidity, atmospheric pollution etc) 3) Deterioration and/or loss

Transmission of Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Spoken word • Conversations • Meetings • Telephone/ mobile calls	No special precautions required	No special precautions required	1) Confidential information should only be discussed with authorised individuals within a private setting. 2) Avoid discussion in public areas such as elevators, hallways, staircases and cafeterias etc. 3) If you have to discuss on the phone ensure you can positively identify the person you are talking to, and preferably use a landline instead of a mobile phone.	1) Restricted information should only be discussed with authorised individuals within a private setting. 2) Avoid discussion in public areas such as elevators, hallways, staircases and cafeterias etc. 3) If you have to discuss on the phone ensure you can positively identify the person you are talking to, and preferably use a landline instead of a mobile phone.

GLOBAL BP SOLUTIONS,LLC

Transmission of Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Internal Post	No special handling required	No special handling required	**Standard internal postal procedure:** 1) If possible, notify recipient in advance. 2) Ensure you have the correct name and address of the intended recipient on the envelope. 3) Send in a sealed inter-office envelope marked "confidential". **Removable storage media:** All CD's, DVD's, tapes and other removable storage media containing confidential information must be encrypted in accordance the *GBPS Encryption Policy* prior to being sent in the post, and, A process must be in place to ensure the appropriate disposal of the information on removable storage media once the transfer is complete.	**Standard internal postal procedure:** 1) If possible, notify recipient in advance. 2) Ensure you have the correct name and address of the intended recipient on the envelope. 3) Send in a sealed inter-office envelope marked "confidential". **Removable storage media:** All CD's, DVD's, tapes and other removable storage media containing confidential information must be encrypted in accordance the *GBPS Encryption Policy* prior to being sent in the post, and, A process must be in place to ensure the appropriate disposal of the information on removable storage media once the transfer is complete.

GLOBAL BP SOLUTIONS,LLC

Transmission of Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
External Post	No special handling required	No special handling required	**Standard external postal procedure:** 1) If possible, notify recipient in advance. 2) Ensure you have the correct name and address of the intended recipient on the envelope. 3) Send in a sealed envelope marked "Private & Confidential" and add on a return address where this will not compromise privacy. 4) Send by normal post. **Removable storage media:** All CD's, DVD's, tapes and other removable storage media containing confidential information must be encrypted in accordance the *GBPS Encryption Policy* prior to being sent in the post, and, A process must be in place to ensure the appropriate disposal of the information on removable storage media once the transfer is complete. **Bulk postal procedure:** When sending bulk confidential information by post to the same address you must use an approved courier or a registered postal service.	**Standard external postal procedure:** 1) If possible, notify recipient in advance. 2) Ensure you have the correct name and address of the intended recipient on the envelope. 3) Send in a sealed envelope marked "Private & Confidential" and add on a return address where this will not compromise privacy. 4) Send by normal post. **Removable storage media:** In addition to the above, 1) All CD's, DVD's, tapes and other removable storage media containing confidential information must be encrypted in accordance the *GBPS Encryption Policy* prior to being sent in the post, and, 2) A process must be in place to ensure the appropriate disposal of the information on removable storage media once the transfer is complete. **Bulk postal procedure: same as that for confidential information**

GLOBAL BP SOLUTIONS,LLC

Transmission of Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Internal Email	No special handling required	No special handling required	1) Ensure that the name and email address of the intended recipient are correct. 2) The email message is clearly marked as "Private & Confidential"; 3) Only the minimum amount of confidential information as is necessary for a given function(s) to be carried out is to be sent;	1) Ensure that the name and email address of the intended recipient are correct. 2) The email message is clearly marked as "Private & Confidential"; 3) Only the minimum amount of restricted information as is necessary for a given function(s) to be carried out is to be sent;
External Email	No special handling required	No special handling required	*1)* The information transfer must be legally justifiable in accordance with the *Data Protection Act* 2) Ensure that the name and email address of the intended recipient are correct. 3) The email must consist of a title in the subject line to include the word "Confidential" and have an appropriate email disclaimer at the end of the email message. 4) All confidential information included with the email message is encrypted in accordance with the *GBPS Encryption Policy* unless the intended recipient email address is hosted on a network which connected to the GBPS via a secure connection (for example: VPN, TLS connection etc)	*1)* The information transfer must be legally justifiable in accordance with the *Data Protection Act* 2) Ensure that the name and email address of the intended recipient are correct. 3) The email must consist of a title in the subject line to include the word "Confidential" and have an appropriate email disclaimer at the end of the email message. 4) All confidential information included with the email message is encrypted in accordance with the *GBPS Encryption Policy* unless the intended recipient email address is hosted on a network which connected to the GBPS via a secure connection (for example: VPN, TLS connection etc)

GLOBAL BP SOLUTIONS,LLC

Transmission of Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Fax	Use standard GBPS fax coversheet and take reasonable care in dialing fax number.	1) Use standard GBPS fax coversheet and take reasonable care in dialing fax number. 2) Should not be sent from a fax machine which is located within an area that is accessible to the general public	In accordance with the *GBPS Electronic Communications Policy* confidential information should only be sent by fax in exceptional circumstances such as a (1) Medical emergency, (2) Where a legal obligation exists, (3) Informed consent, (4) Where there is no alternative. When confidential information **has** to be sent by fax: 1) The fax machine used to send/receive confidential information should be located within a secure area which is not accessible by the general public. 2) Make sure you are using the correct fax number for the intended recipient. 3) Ensure you use the *GBPS Fax CoverSheet* 4) Where possible, you should telephone the intended recipient before the transmission to ensure they are waiting by the fax machine for the transmission. Subsequent telephone call to confirm receipt of the transmission. 5) Ensure you remove the all documents from the fax machine immediately after faxing.	In accordance with the *GBPS Electronic Communications Policy* restricted information should only be sent by fax in exceptional circumstances such as a (1) Medical emergency, (2) Where a legal obligation exists, (3) Informed consent, (4) Where there is no alternative. When restricted information **has** to be sent by fax: 1) The fax machine used to send/receive confidential information should be located within a secure area which is not accessible by the general public. 2) Make sure you are using the correct fax number for the intended recipient. 3) Ensure you use the *GBPS Fax Cover Sheet* 4) Where possible, you should telephone the intended recipient before the transmission to ensure they are waiting by the fax machine for the transmission. Subsequent telephone call to confirm receipt of the transmission. 5) Ensure you remove the all documents from the fax machine immediately after faxing.

Transmission of Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Electronic File Transfer (EFT)	No special handling required	No special handling required	1) Transmission must be authorised by a GBPS line manager (at grade 8 level or above) 2) Information transfer must take place via a secure channel (i.e. Secure FTP, TLS, VPN etc) or the information must be encrypted email in accordance with the GBPS Encryption Policy	1) Transmission must be authorised by a GBPS line manager (at General Manager level or above) 2) Information transfer must take place via a secure channel (i.e. Secure FTP, TLS, VPN etc) or the information must be encrypted email in accordance with the GBPS Encryption Policy
Text Message	No special handling required	No special handling required	Under **no** circumstances whatsoever should confidential information be transmitted by text. However, patients and service users who provide the GBPS with prior **explicit consent** maybe reminded by text message of their GBPS appointments. Where patients and service users have consented to be contacted by text of their appoints, the text message should only contain the minimum amount of information, for example, the **appointment date & time and the name of hospital**. The specific GBPS clinic the patient or service user is to attend may also be included in the text where this will not compromise privacy. **The text message should not contain any personal information belonging to patient or service user.**	Under **no** circumstances whatsoever should restricted information be transmitted by text

GLOBAL BP SOLUTIONS,LLC

Physical Security				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Office / Workplace	No special precautions required.	No special precautions required.	1) Access to areas containing confidential information should be restricted to authorised staff only (i.e. manned reception desk, access to office controlled via keypad or swipe card access) 2) Where practical a **clear desk policy** should be in operation where all confidential information (irrespective of format) is cleared from desks and locked away securely when it is not in use.	1) Access to areas containing confidential information should be restricted to authorised staff only (i.e. manned reception desk, access to office controlled via keypad or swipe card access) 2) Where practical a **clear desk policy** should be in operation where all restricted information (irrespective of format) is cleared from desks and locked away securely when it is not in use
Desktop Computers	Desktops computers must be: 1) Password protected in accordance with the ***GBPS Password Standards Policy.*** 2) Logged off or "locked" (using *Ctrl+Alt+Delete* keys) when they have to be left unattended for any period of time and at the end of each working day	Desktop computers must be: 1) Password protected in accordance with the ***GBPS Password Standards Policy.*** 2) Logged off or "locked" (using ***Ctrl+Alt+Delete*** keys) when they have to be left unattended for any period of time and at the end of each working day	Desktop computers must be: 1) Password protected in accordance with the ***GBPS Password Standards Policy.*** 2) Password must not be written down on or near the desktop computer 3) Logged off or "locked" (using *Ctrl+Alt+Delete* keys) when they have to be left unattended for any period of time and at the end of each working day 4) Positioned in such a way as to minimize the risk of unauthorized individuals accessing the computer or viewing information displayed on the screen.	Desktop computers must be: ***1)*** Password protected in accordance with the ***GBPS Password Standards Policy.*** 2) Password must not be written down on or near the desktop computer 3) Logged off or "locked" (using *Ctrl+Alt+Delete* keys) when they have to be left unattended for any period of time and at the end of each working day 4) Positioned in such a way as to minimize the risk of unauthorized individuals accessing the computer or viewing information displayed on the screen.

GLOBAL BP SOLUTIONS,LLC

Physical Security				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Laptop Computers	Laptop computers must be: 1) Encrypted in accordance with the ***GBPS Encryption Policy*** ***2)*** Password protected in accordance with the ***GBPS Password Standards Policy.*** 3) Locked with a laptop cable lock when left in the office overnight or stored in a locked drawer or cabinet 4) Kept with you at all times when working off-site	Laptop computers must be: 1) Encrypted in accordance with the ***GBPS Encryption Policy*** ***2)*** Password protected in accordance with the ***GBPS Password Standards Policy.*** 3) Locked with a laptop cable lock when left in the office overnight or stored in a locked drawer or cabinet 4) Kept with you at all times when working off-site	Laptop computers must be: ***1)*** Encrypted in accordance with the ***GBPS Encryption Policy*** ***2)*** Password protected in accordance with the ***GBPS Password Standards Policy.*** 3) Password must not be written down on or near the desktop computer 4) Logged off or "locked" (using ***Ctrl+Alt+Delete*** keys) when they have to be left unattended for any period of time and at the end of each working day 5) Locked with a laptop cable lock when left in the office overnight or stored in a locked drawer or cabinet 6) Kept with you at all times when working off-site	Laptop computers must be: ***1)*** Encrypted in accordance with the ***GBPS Encryption Policy*** ***2)*** Password protected in accordance with the ***GBPS Password Standards Policy.*** 3) Password must not be written down on or near the desktop computer 4) Logged off or "locked" (using ***Ctrl+Alt+Delete*** keys) when they have to be left unattended for any period of time and at the end of each working day 5) Locked with a laptop cable lock when left in the office overnight or stored in a locked drawer or cabinet 6) Kept with you at all times when working off-site

Physical Security				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Mobile Computer Devices • Smart phones, Blackberry's • Tablet Computer • PDA • iPhone • iPad	Mobile computers devices must be: *1)* Encrypted in accordance with the ***GBPS Encryption Policy*** *2)* Password protected in accordance with the ***GBPS Password Standards Policy.*** 3) Kept with you at all times when working off-site 4) Locked away in a filing cabinet or drawer when left in the office overnight	Mobile computers devices must be: *1)* Encrypted in accordance with the ***GBPS Encryption Policy*** *2)* Password protected in accordance with the ***GBPS Password Standards Policy.*** 3) Kept with you at all times when working off-site 4) Locked away in a filing cabinet or drawer when left in the office overnight	Mobile computers devices must be: *1)* Encrypted in accordance with the ***GBPS Encryption Policy*** 2) Password protected in accordance with the ***GBPS Password Standards Policy.*** 3) Password must not be written down on or near the desktop computer 4) Kept with you at all times when working off-site 5) Locked away in a filing cabinet or drawer when left in the office overnight	Mobile computers devices must be: *1)* Encrypted in accordance with the ***GBPS Encryption Policy*** *2)* Password protected in accordance with the ***GBPS Password Standards Policy.*** 3) Password must not be written down on or near the desktop computer 4) Kept with you at all times when working off-site 5) Locked away in a filing cabinet or drawer when left in the office overnight
Removable Storage Devices • CD/DVD • Tapes • External hard drive • USB Memory Stick	No special precautions required.	No special precautions required.	1) Encrypted in accordance with the ***GBPS Encryption Policy*** 2) Stored in a secure location such as a locked filing cabinet, drawer or a safe (preferably a fireproof safe) when not in use.	1) Encrypted in accordance with the ***GBPS Encryption Policy*** 2) Stored in a secure location such as a locked filing cabinet, drawer or a safe (preferably a fireproof safe) when not in use.

Physical Security				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Photographic, Video & Audio Recording Devices	Stored in a safe location when not in use	Stored in a safe location when not in use	Stored in a secure location such as a locked filing cabinet, drawer or a safe when not in use.	Stored in a secure location such as a locked filing cabinet, drawer or a when not in use

Destruction & Disposal of Information

Note: Any decision to destroy and dispose of GBPS information (irrespective of format) should be made in accordance with the appropriate GBPS record retention policies.

Topic	Public	Internal	Confidential	Restricted
Paper & Film based information • Paper records & printed material • Microfilm • Micro fiche • Other image photo negative materials	No special requirements, maybe disposed along with general office waste	No special requirements, maybe disposed along with general office waste	Once a senior GBPS manager has made the decision to destroy confidential information stored on paper or film material, the material containing the confidential information must be destroyed and disposed of in a secure manner that protects the confidentiality of the information (i.e. shredding (preferably using a cross cut shredder), pulverized, macerated or incineration etc) Where the destruction and disposal of the confidential information is outsourced to a third party service provider, the third party service provider must 1) Sign the the ***GBPS Server Provider Confidentiality Agreement*** 2) Provide the subscribing GBPS department with a **certificate of information destruction/ disposal**	Once a senior GBPS manager has made the decision to destroy restricted information stored on paper or film material, the material containing the confidential information must be destroyed and disposed of in a secure manner that protects the confidentiality of the information (i.e. shredding (preferably using a cross cut shredder), pulverized, macerated or incineration etc) Where the destruction and disposal of the restricted information is outsourced to a third party service provider, the third party service provider must 1) Sign the the ***GBPS Server Provider Confidentiality Agreement*** 2) Provide the subscribing GBPS department with a **certificate of information destruction / disposal**

GLOBAL BP SOLUTIONS,LLC

Destruction & Disposal of Information

Note: Any decision to destroy and dispose of GBPS information (irrespective of format) should be made in accordance with the appropriate GBPS record retention policies.

Topic	Public	Internal	Confidential	Restricted
Computer devices • Laptop Computers • Desktop Computers, • Mobile Computer Devices, • External / Portable Hard Drives, • USB Memory Keys	Must be disposed in accordance with environmental regulations i.e **a certificate of information destruction / disposal**	Must be disposed in accordance with environmental regulations i.e **a certificate of information destruction / disposal**	All traces of confidential information must be removed from old / obsolete laptop/desktop computers, mobile computer devices, removable storage devices (i.e. external hard drives, USB memory sticks) before they are reused within the GBPS, sold off to staff, donated to charity, or disposed of. **The deletion or formatting of the confidential information stored on the old/ obsolete device is not sufficient to remove all traces of the information** 1) Where the old / obsolete devices are to be re-used within the GBPS, sold off to employees or donated to charity, the information on the devices must be overwritten using special **sanitation software** which is available from the ICT Directorate. 2) Where the old / obsolete devices have come to the end of their working life and are to be disposed off, the devices must be physically destroyed in such a way that it is almost impossible to recover any confidential information stored on the device. This process is usually carried out by a specialist waste disposal company. All computer devices must be disposed in accordance with environmental regulations i.e **a certificate of information destruction**	Restricted information should be disposed in the same way as confidential information

GLOBAL BP SOLUTIONS,LLC

Destruction & Disposal of Information

Note: Any decision to destroy and dispose of GBPS information (irrespective of format) should be made in accordance with the appropriate GBPS record retention policies.

Topic	Public	Internal	Confidential	Restricted
Photocopiers, Scanners and Fax Machines	Must be disposed in accordance with environmental regulations i.e **a certificate of information destruction / disposal**	Must be disposed in accordance with environmental regulations i.e **a certificate of information destruction / disposal**	Most multifunctional photocopiers and scanners contain a hard disk which stores a copy of every document that was ever copied, scanned or faxed on the device. For this reason, old and end of life photocopiers must have their hard disk physically destroyed to ensure any confidential information cannot be recovered from the hard drive. This process is usually carried out by a specialist company. All photocopiers, scanners and fax machines devices must be disposed in accordance with environmental regulations i.e a **certificate of information destruction / disposal**	Most multifunctional photocopiers and scanners contain a hard disk which stores a copy of every document that was ever copied, scanned or faxed on the device. For this reason, old and end of life photocopiers must have their hard disk physically destroyed to ensure any restricted information cannot be recovered from the hard drive. This process is usually carried out by a specialist company. All photocopiers, scanners and fax machines devices must be disposed in accordance with environmental regulations i.e **a certificate of information destruction / disposal**

GLOBAL BP SOLUTIONS,LLC

Destruction & Disposal of Information

Note: Any decision to destroy and dispose of GBPS information (irrespective of format) should be made in accordance with the appropriate GBPS record retention policies s

Topic	Public	Internal	Confidential	Restricted
CD's & DVD's	No special requirements	No special requirements	The deletion or formatting of old CD/DVD's is not sufficient to remove all traces of confidential information stored on the CD/DVD Old CD/DVD's that contain confidential information must be physically destroyed in such a way that it is almost impossible to recover any of the confidential information stored on the device. For example: • Shredded using a disc shedder • Cut up with a scissors into small pieces • Using sand paper to destroy both surfaces of the CD/DVD • Incineration	The deletion or formatting of old CD/DVD's is not sufficient to remove all traces of restricted information stored on the CD/DVD Old CD/DVD's that contain restricted information must be physically destroyed in such a way that it is almost impossible to recover any of the restricted information stored on the device. For example: • Shredded using a disc shedder • Cut up with a scissors into small pieces • Using sand paper to destroy both surfaces of the CD/DVD • Incineration

GLOBAL BP SOLUTIONS,LLC

Destruction & Disposal of Information

Note: Any decision to destroy and dispose of GBPS information (irrespective of format) should be made in accordance with the appropriate GBPS record retention policies.

Topic	Public	Internal	Confidential	Restricted
Floppy Magnetic Tapes (i.e. backup tapes)	No special requirements	No special requirements	The deletion or formatting of old floppy diskettes and magnetic media is not sufficient to remove all traces of confidential information stored on the floppy diskette or magnetic tape. Old floppy diskettes and magnetic media that contain confidential information must be physically destroyed in such a way that it is almost impossible to recover any confidential information stored on the device. For example: • Degaussing • Pulverised • Incineration	The deletion or formatting of old floppy diskettes and magnetic media is not sufficient to remove all traces of restricted information stored on the floppy diskette or magnetic tape. Old floppy diskettes and magnetic media that contain confidential information must be physically destroyed in such a way that it is almost impossible to recover any confidential information stored on the device. For example: • Degaussing • Pulverised • Incineration

GLOBAL BP SOLUTIONS,LLC

Destruction & Disposal of Information

Note: Any decision to destroy and dispose of GBPS information (irrespective of format) should be made in accordance with the appropriate GBPS record retention policies.

Topic	Public	Internal	Confidential	Restricted
Video & Audio Tapes	No special requirements	No special requirements	The deletion or formatting of old video or audio is not sufficient to remove all traces of confidential information stored on the tape. Old video and audio tapes that contain confidential information must be physically destroyed in such a way that it is almost impossible to recover any confidential information stored on the tape. For example: • Pulverized • Incineration	The deletion or formatting of old video or audio is not sufficient to remove all traces of restricted information stored on the tape. Old video and audio tapes that contain restricted information must be physically destroyed in such a way that it is almost impossible to recover any restricted information stored on the tape. For example: • Pulverized • Incineration

SERVICE PROVIDER CONFIDENTIALITY AGREEMENT

VERSION 1.0

GLOBAL BP
SOLUTIONS,LLC

THIS AGREEMENT is dated ..... and made between:

(1) **Global BP Solutions** a corporate body dealing in outsourcing and providing versatile services to its wide client tell in U.S.A

(2) ……
(the **Service Provider's** name **(**Block Capitals**)**)

……
(the **Service Provider's** registration number **(**Block Capitals**)**)

……
(the **Service Provider's** registered office **(**Block Capitals**)**)

This Agreement is an addendum to the ***GBP Standard Terms for Services & Supplies*** (and/or title of bespoke contract).

……..

……..
(Title of bespoke contract, the "Tender Contract" **(**Block Capitals**)**)

RECITALS

A. In connection with a current or proposed Service between the GBPS and the Service Provider, whereby the Service Provider is supplying, or proposes to supply, goods or services (the **Service**) to GBP. GBPS may directly make available to the Service Provider from time to time the *Information* (as defined below), or the Service Provider or its employees, agents, affiliates, subsidiaries or sub-contractors may indirectly acquire or have access to the *Information* by virtue of the Service.

B. It is intended that this Agreement will govern the terms and conditions applying to the Service Provider's use of the *Information* and other related matters.

NOW IT IS HEREBY AGREED by and between the parties hereto as follows:

1 Definitions:

In this Agreement, unless the context otherwise requires:

Contact Data means personal data limited to the business contact details of any employee of the GBPS or a GBPS Agency who will communicate with Service Provider personnel regarding the *Service;*

Data Breach has the same meaning as "personal data breach";

Data Protection Directive means protection of individuals with regard to the processing of personal data and on the free movement of such data;

Delete for the purposes of this agreement means removing all Information which is electronically held in such a way that it can never be retrieved from the device on which it is held;

Information means all information, (irrespective of the format, paper, electronic or otherwise) that is provided to the Service Provider by or on behalf of GBPS in connection with the *Service*. *Information* may include *Personal Data* concerning GBPS and GBPS Agency clients, patients and staff, and confidential codes or any other information concerning the security of the GBPS's ICT infrastructure, but shall exclude Contact Data*;*

Personal Data relates only to personal data, or any part of such personal data, of which the GBPS is the Data Controller or joint Data Controller and in relation to which the Service Provider is providing the Service, and includes Sensitive Personal Data and Special Categories of Data;

Special Categories of Data has the meaning given to this term and/or such Personal Data as referred and any reference to **third party** in this Agreement includes, for the avoidance of doubt, subcontractors.

2 Obligations of the Service Provider:

In consideration of the GBPS directly making the *Information* available to the Service Provider, or the Service Provider otherwise acquiring the *Information*, and in consideration of the award of the Tender Contract, the Service Provider shall:

2.1 Not take or remove any *Information* from GBPS premises without having received the written consent of the GBPS. Such written consent must be issued in advance of the first instance and will apply thereafter;

2.2 Manage and *Process* any *Information* which they acquire from GBPS in accordance with the documented instructions of GBPS as set out in this Agreement and the obligations of the *Data Protection Acts* and in so far as these obligations apply to a *Data Processor*, including with regard to transfers of *Personal Data* to a third country or an international organization, unless required to do so; in such a case, the Service Provider shall inform GBPS of that legal requirement before *Processing*, unless that law prohibits such information on important grounds of public interest;

2.3 Maintain secret and confidential all *Information* furnished to it or otherwise acquired by its servants, employees, agents, affiliates, subsidiaries or sub-contractors save and to the extent that such *Information* has been made available to the public by the GBPS or by any third party lawfully in possession thereof and entitled to make such disclosure without restriction;

2.4 Take appropriate measures to ensure the reliability of the Service Providers servants, employees, agents, affiliates, subsidiaries or sub-contractors who have access to the Information;

The Service Provider must be in a position to provide GBPS with a named list of their employees, agents, affiliates, subsidiaries or sub-contractors authorised to have access to *Information*.

2.5 Not disclose *Information* to any of the Service Provider's servants, employees, agents, affiliates, subsidiaries or sub-contractors unless and only to the extent that such persons need to know such *Information* for the purposes of providing services in connection with the *Service*, and provided that such person has been made aware of the restrictions in this Agreement on the disclosure of the *Information* and has agreed in writing to comply with such restrictions or materially similar restrictions;

2.6 Not disclose any *Information* to any third party without the prior written consent of GBPS unless the Service Provider is legally required to do so;

2.7 Not engage any third party to process the *Information* or any part thereof on its behalf without the prior written consent of GBPS. In the event that the third party fails to fulfil its obligations set out in of this Agreement, the Service Provider shall remain fully liable to GBPS for the performance;

2.8 Not use the *Information* directly or indirectly for any purpose other than in connection with the provision of services to GBPS regarding the Service;

2.9 Not reverse engineer, de-compile or disassemble *Information* or attempt to use the *Information* in any form other than machine readable object code, or allow a third party to do any of the above;

2.10 Not make any press announcement or otherwise publicize the business relationship with the GBPS in any way including, without limitation, using the name of GBPS in any publicity material, unless authorised to do so by GBPS;

2.11 Only use the *Information* solely for the purposes of fulfilling the requirements of the Service.

2.12 Take the necessary precautions for the prevention of unauthorized access to, unauthorized disclosure of or other unauthorized processing of the *Information* and in particular:

2.12.1 Keep all *Information* obtained from the GBPS or otherwise relating to the Service separate from all documents and other records of the Service Provider. The GBPS accepts that this requirement would be achieved by the Service Provider through logical electronic separation using role-based access controls;

2.12.2 Only make such copies of the *Information* as are necessary for the provision of services to GBPS regarding the Service; and

2.12.3 Ensure that any notices related to the confidentiality or privacy of the *Information* provided by GBPS are not removed or altered; and

2.12.4 Have all necessary access controls in place to include authentication and authorization for access to *Information* to ensure its security and confidentiality; and

2.12.5 Have all necessary systems in place to ensure the ongoing confidentiality, integrity, availability and resilience of *Processing* systems and services; and

2.12.6 Have the ability to restore the availability and access to the *Information* in a timely

manner in the event of a physical or technical incident; and

2.12.7 Have a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the *Processing* of the *Information*;

2.13 Ensure, upon termination or the completion of this Agreement, that all documents, data, other records or tangible objects containing or representing *Information* which have been disclosed by the GBPS to the Service Provider ("***Information Records***"), and all copies thereof which are in the possession of the Service Provider and their subcontractors, shall at the written request and election of the GBPS, be returned to the GBPS or securely *Deleted*. Without prejudice to the generality of the foregoing:

2.13.1 Where the GBPS has requested that the Service Provider return *Information Records*, the *Information Records* shall be returned from the Service Provider to the GBPS in a commonly used electronic format;

2.13.2 Where the GBPS has requested that the Service Provider securely *Delete Information,* the Service Provider shall ensure the Information is permanently *Deleted* from any of the Service Providers systems or devices which were used to store the *Information* and from those of third parties to whom the Service Provider has disclosed and/or permitted access to the *Information* or *Information Records*;

2.13.3 Where the Service Provider is required for legal or regulatory compliance to retain a copy of any *Information*, the Service Provider shall provide the GBPS in writing with full details of any *Information* they are proposing to retain and the details of the legal and regulatory obligations governing this action.

2.14 Taking into account the nature of the processing, assist GBPS by appropriate technical and organizational measures, insofar as this is possible, to enable GBPS to fulfil its obligations to respond to requests from Data Subjects exercising their rights.

2.15 For the purposes of Freedom of Information / transparency obligations placed upon the GBPS:

2.15.1 Procure that it and its employees, agents, subsidiaries or sub-contractors shall assist GBPS, at no additional charge and within such timescales as the GBPS may reasonably specify, in meeting any requests for *Information* which are made to GBPS such assistance to include (but not be limited to) the provision of a copy of the requested *Information.*

2.15.2 Notwithstanding anything to the contrary in this Agreement, if GBPS receives a request for *Information* pursuant by legal authorities (court cases, police etc), GBPS shall be entitled to disclose all *Information* (in whatever form) as is necessary to comply.

2.15.3 If, at the request of the Service Provider, the GBPS seeks to withhold *Information* protected by this Agreement and a competent authority determines, or the parties subsequently agree, that the *Information* is not exempt, then the Service Provider shall reimburse the GBPS for all costs (including but not limited to legal costs) incurred by the GBPS in seeking to withhold such *Information* from a request.

2.16 Ensure the security of Information stored on all fixed and mobile devices, including medical devices, desktop computers, servers and mobile computer devices (i.e. laptops, notes, tablets, personal data assistants, Blackberry enabled devices, iPads, iPhones and other smart type devices etc) and removal storage devices (i.e. CD, DVD, portable hard drives, ZIP disks, Magnetic tapes etc).

2.16.1 Only in exceptional circumstances and with the written consent of the GBPS, should the Service Provider hold *Information* on mobile computing or removable storage devices. Should the business requirements necessitate the holding of *Information* on such devices then the Service Provider shall ensure that only *Information* absolutely necessary for their purpose is stored in this format. The Service Provider will *Delete* or return all copies of the *Information* after the business requirements have been fulfilled, or earlier upon the written request of the GBPS.

2.16.2 Where the use of mobile computing or removal storage devices is a necessity then the Service Provider will take all necessary precautions to ensure the safety of these devices from theft, loss and unauthorized access. As a minimum all mobile computing and removal storage devices must be appropriately secured including by means of strong encryption and protected by the use of strong complex passwords.

2.16.3 The encryption used by the Service Provider on the Service Providers laptops must satisfy or better the requirements of the *GBPS Encryption Policy*. GBPS will notify the Service Provider of any relevant changes to the *GBPS Encryption Policy*. At any time during the term of this Agreement the GBPS may request the Service Provider to set out in writing the current encryption measures used and the Service Provider will provide this information within 5 days. If, in the reasonable opinion of GBPS, the encryption standard employed by the Service Provider is not sufficient, the Service Provider will implement, at their expense, whatever encryption standards are proposed by GBPS. At no time should cipher keys be held on the mobile computing or removal storage device for the data which they secure. In addition, the Service Provider will at all times hold cipher keys in a secure fashion.

2.16.4 Under no circumstances encrypted or otherwise is the Service Provider sanctioned by GBPS to download or store *Information* on USB memory sticks/keys.

2.17 Ensure the security of the *Information* in transit (including by way of electronic transit/ transit by way of electronic communication). Where it is necessary to transfer the *Information*, the Service Provider must take all necessary precautions to ensure the security of the *Information* before, during and after transit.

2.17.1 The Service Provider shall ensure that all transfers of the *Information* are legal, justifiable, and only the minimum *Information* absolutely necessary for a given purpose is transferred.

2.17.2 All transfers of *Information* should, where possible, only take place electronically via secure on-line channels or electronic mail. Where the Service Provider transfers *Information* electronically, in any form and by any means, the *Information* must be encrypted using strong encryption. The encryption methods used must satisfy or better the requirements of the *GBPS Encryption Policy*. The current GBPS encryption standard for electronic transfer is SSL (Secure Socket Layer) and TLS

(Transport Layer Security) and Advanced Encryption Standard (AES) 256 in the case of encrypted email. The GBPS will notify the Service Provider of any relevant changes to the *GBPS Encryption Policy*.

2.17.3 Where it is not possible to transfer the *Information* electronically, the *Information* may be encrypted and copied to a mobile storage device (with the exception of USB memory sticks/keys) and transported manually. The encryption methods used must satisfy or better the requirements of the *GBPS Encryption Policy*. The current GBPS encryption standard for mobile storage devices is Advanced Encryption Standard (AES) 256. The GBPS will notify the Service Provider of any relevant changes to the *GBPS Encryption Policy*. Encrypted mobile storage media, should wherever possible, be hand delivered by the Service Provider to, and be signed for by, the intended recipient. If this is not possible, the use of registered post or some other certifiable delivery method must be used**.**

2.18 In relation to transfers of *Information* outside of the Republic of Ireland.

2.18.1 The Service Provider must seek the written consent of the GBPS prior to the Service Provider transferring *Information* outside the jurisdiction of the Republic of Ireland. The GBPS may, at its discretion, prohibit the Service Provider from transferring *Information* outside the jurisdiction of the Republic of Ireland.

2.19 Make available to the GBPS all information necessary to demonstrate the Service Providers compliance with the obligations laid down allow for and contribute to audits, including inspections, conducted by GBPS or another auditor mandated by GBPS. The Service Provider and GBPS agree to negotiate in good faith the scope and implementation details of this provision at the time GBPS decides to exercise its rights under this provision.

3 **Disclosure Required by Law**: In the event that the Service Provider is legally required to disclose any of the *Information* to a third party, the Service Provider undertakes to notify the GBPS of such requirement prior to any disclosure and, unless prohibited by law, to supply the GBPS with copies of all communications between the Service Provider and any third party to which such disclosure is made. The Service Provider must co-operate with GBPS in bringing any legal or other proceedings to challenge the validity of the requirement to disclose Information.

4 **Breach of Agreement**: The Service Provider hereby indemnifies and agrees to keep indemnified GBPS against any costs, expenses, damages, harm or loss suffered or incurred by reason of any disclosure of the *Information* in breach of the terms and conditions of this Agreement and shall account to the GBPS for any moneys received by the Service Provider directly or indirectly arising out of the disclosure or use of any of the Information in breach of the terms and conditions of this Agreement.

5 **No Warranty:** Nothing in this Agreement shall constitute a warranty by the GBPS as to the accuracy of any of the *Information,* and the GBPS will not be liable to the Service Provider or to any other party to which any of the Information may be disclosed for any loss or damage howsoever caused, arising directly or indirectly out of the inaccuracy of any of the Information.

6 **No License**: The Service Provider acknowledges that the Information is of a special and unique character and that the *Information* and any patent, copyright or other intellectual property rights of whatever nature attaching thereto are and will remain the property of the GBPS and nothing in

this Agreement will be construed as giving the Service Provider a license in respect of such patent, copyright or other intellectual property rights.

7 **Survival of Obligations**: The non-disclosure obligations of this Agreement will survive and continue and will bind the Service Provider's legal representatives, successors and assigns notwithstanding that the Service may not be actually implemented by the parties.

8 **Waiver:** The rights of the GBPS under this Agreement will not be prejudiced or restricted by any indulgence or forbearance extended to the Service Provider or other parties, and no waiver by the GBPS in respect of any breach of the terms of this Agreement will operate as a waiver in respect of any subsequent breach.

9 **Variation:** This Agreement may not be released, discharged, supplemented, amended, varied or modified in any manner except by an instrument in writing signed by a duly authorised officer or representative of each of the parties hereto**.**

10 **Notice:** Any notice or other communication given or made under this Agreement shall be in writing and may be sent by email, delivered to the relevant party, or sent by pre-paid registered post airmail or fax to the address of that party specified in this Agreement or to that party's fax number thereat or such other address or number as may be notified hereunder by that party from time to time for this purpose and will be effective notwithstanding any change of address or fax number not so notified.

11 **Severance:** If any provision of this agreement is found by any court or administrative body of competent jurisdiction to be invalid, unenforceable or illegal, the other provisions of this agreement will remain in force. If any invalid, unenforceable or illegal provision would be valid, enforceable or legal if some part of it were deleted, the provision will apply with whatever modification is necessary to make it valid, enforceable or legal.

12 **Governing Law**: This Agreement will be governed by and construed in accordance with the laws of Ireland and the parties hereto hereby irrevocably submit to the exclusive jurisdiction of the courts of Ireland.

IN WITNESS where of this Agreement has been entered into the day and year first herein written.

SIGNED on behalf of the
Health Service Executive

In the presence of

…….
Signature

…….
Name (printed)

…….
Title

…….
Signature

…….
Name (printed)

…….
Title

SIGNED on behalf of

…….
(the **Service Provider)**

In the presence of

…….
Signature

…….
Name (printed)

…….
Title

Date: …….

…….
Signature

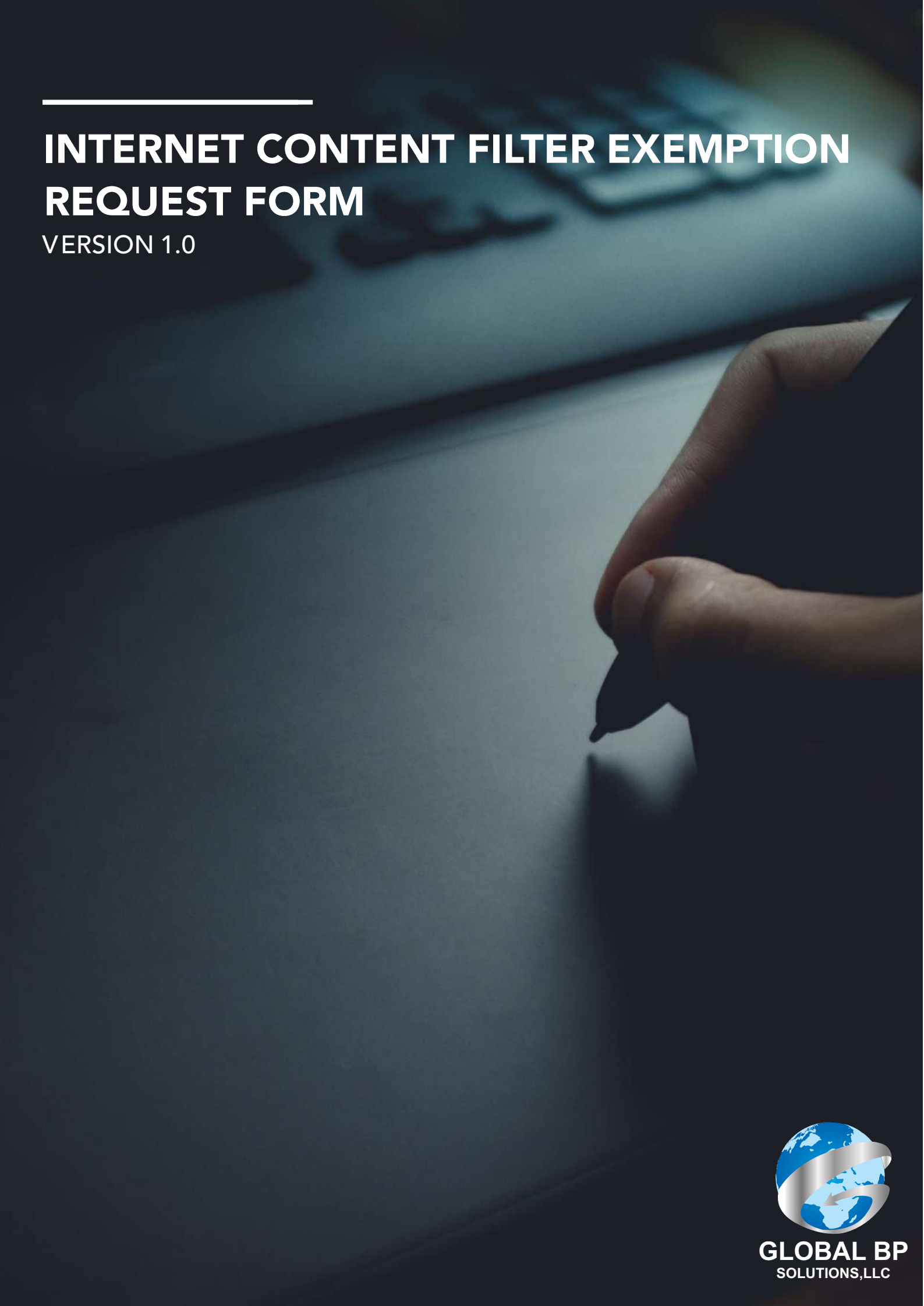
…….
Name (printed)

…….
Title

Date: …….

INTERNET CONTENT FILTER EXEMPTION REQUEST FORM

VERSION 1.0



GLOBAL BP
SOLUTIONS,LLC

About this request form

This request form must be completed in full (**in block capitals**) by GBPS employees who have a valid GBPS work-related reason to access internet content that is otherwise filtered (blocked) by GBPS. The form must be completed on an individual basis, as group requests using a single request form will not be processed.

The request must be approved and signed by the employee's line manager (at General Manager level (or equivalent) or above). **Line managers have a responsibility to ensure they only approve and sign access requests on behalf of GBPS employees, once they are satisfied the employee has a valid GBPS worked related reason to access all categories and subcategories marked on the access request form.**

GBPS employees are not permitted to approve their own access requests except the Line Manager or equivalent.

Employee' should note, access to the technical user access groups (see section 2B of this form) is restricted to the **relevant GBPS ICT personnel only unless there is a special need and reason.**

The ICT Directorate reserves the right (without prior notification) to restrict or block access to certain categories or subcategories of internet content, which are identified as having a negative impact on the performance of GBPS network, information systems and/or equipment.

The completed request form must be handed to the ICT Helpdesk / Call Centre. Incomplete and/or illegible request forms will not be processed and will be returned to the sender.

Section 1.0: GBPS Employee Details

Name (Block Capitals): …….....

Personnel Number: …….....

Position:…….. …….....

Directorate / Service Function: ……

Location: ……..

……

Work Number:……..……..

GBPS email address: ……..

GLOBAL BP SOLUTIONS,LLC

Section 2.0: Internet Access Details

Please tick each category **and** subcategory of blocked (filtered) internet content you require access to

2A. Custom User Access Groups

Please tick each category/subcategory of blocked (filtered) internet content that you wish to have access to.

Adult Material Sex Nudity Adult Content	**Bandwidth Consuming** Internet Radio & TV Streaming Media	**Entertainment** **MP3 & Audio Download**
Miscellaneous Image Servers Dynamic Content Images (Media)	**Productivity** Message Boards & Clubs Advertisements Online Brokerage & Trading Instant Messaging	**Internet Communications** Web Chat
Society & Lifestyles Social Networking Blogs & Personal Sites Personals & Dating	**Gambling** **Games** **Weapons** **Military & Extremists**	**Illegal / Questionable** **Racism & Hate** **Tasteless** **Violence** **User Defined**

OTHER USER DEFINED ACCESS:

……

……

……

……

……

GLOBAL BP SOLUTIONS,LLC

2B. Technical User Access Groups

This section is for the use of the ICT Directorate only

Access to these categories / subcategories is restricted to the relevant ICT personnel only. If this section of the form is ticked by non-ICT personnel, the entire request form will be considered **null and void.**

Bandwidth Consuming Peer-To-Peer File Sharing Personal Network Storage & Backup	**IT Technology** Hacking Proxy Avoidance URL translation Web Hosting Web & Email Spam	**Security** Bot Networks Spyware Malicious Software & Websites Malicious Embedded Link Malicious Embedded iFrame Keyloggers Phishing & Other Frauds Potentially Unwanted Software Suspicious Embedded Link
Miscellaneous Private IP Addresses File Download Servers Network Errors	**Productivity** Freeware & Software Download	

Section 3.0: Business Rationale

This section must be completed in full, as failure to do so, may result in your request being denied.

Please give a detailed business reason (in block capitals) for **each category and /or subcategory** of blocked internet content you require access to. As a minimum the business case for each category / subcategory should include (1) why you need access to each category / subcategory, and (2) how access to each category / subcategory is relevant to your current GBPS role;
However in other cases a detailed business reason is over-ridden if employee's line manager has requested so 0r Directorate.

……

……

……

……

……

……

GLOBAL BP SOLUTIONS,LLC

Section 3.0: Business Rationale (Cont.)

……

……

……

……

……

……

……

……

……

……

……

……

……

Section 4.0: GBPS Employee Declaration

I have read and I understand GBPS ***Electronic Communications Policy*** and all other relevant IT related policies and I agree to be bound by the terms therein. I understand and agree that the internet access which I have requested must only be used by me for official GBPS business purposes and must not be shared with others including my GBPS work colleague's. I also understand that any abuse of this internet access by me may lead to the removal of my internet access depending on the nature of the abuse and violation, lead to disciplinary action, including suspension and dismissal as provided for in GBPS disciplinary procedures. I further understand that this level of internet access will be the subject of additional monitoring and the results of this monitoring maybe passed onto my line manager if need be and requested.

Signature: ……

Print Name: …… Date: ……

GLOBAL BP SOLUTIONS,LLC

Section 5.0: GBPS Line Manager Authorization

This section must be completed (In block capitals) by a GBPS employee holding the position of General Manager (or equivalent) or above.

Name (Block Capitals): ……

Grade / Job Title:.....

Location: ……

Contact Telephone Number: ……

GBPS Email Address: ……

I have reviewed this access request submitted on behalf of the above (as outlined in section 1.0) named GBPS employee and I am satisfied that all categories and subcategories of internet content requested by the employee are appropriate, necessary and relevant to the employees current role within GBPS.

Signature: ……

Print Name: …… Date: ……

An email attachment of correspondence can be used to override this!

It is the responsibility of individuals to ensure that all sections of the request form are completed in full as incomplete or illegible request forms will not be processed and will be returned to the sender.

The completed request form must be handed to ICT Helpdesk / Call Centre.

GLOBAL BP SOLUTIONS,LLC