Information Security Policy for GPSS

Introduction

Context of GPSS

- GPSS as a company is an IT company within the field of primary care offering line of business applications to GP practices across the UK. The content of data on the deployed side will contain patient data but within the company itself will only contain dummy data is used from test server access.
- As the live data is always within the environment of the surgery and not hosted outside, the IG of this data is the responsibility of the Surgery who has the produce and as such will be in the realm of the normal IG policies with in Surgery and it out of the scope of this Policy.
- As an IT company, the appropriate security measures need to be put into place to ensure there is minimal risk to any data which is within the office and mobile environment and this policy is the main document to ensure that GPSS is maintaining robust governance within a small business environment.
- This document is divided into aspect of the business where IG is important to consider with policy references if appropriate

In the Office

Network Security

- Every network within the office will have an approved router with firewalls against intrusion of the internet.
- Only essential services such has HTTP and FTP are accessible via outbound. No other ports will be available both inbound or outbound
- There will be no set up of any web server within the office environment. If one is to be set up it will be via an approved 3rd party with correct security protocols sensitive to the needs of the data it will contain and in line with GDPR guidance.
- There will be no VPN with the network. Access to the network is only by physical presence.
- Default passwords for routers and hardware must be changed on the first install
- Wireless passwords must be of long form factor and there must be no guest networks. WPA-PSK2 must be used as the default security protocol

Passwords

- Please refer to our Password Policy

Access Control

- Access is controlled on the basis of service requirements. Access to information shall be restricted to users who have an authorised business
- need to access the information and as approved by the relevant Information Asset Owner.
- Access must be granted to, and revoked from, information systems in a controlled manner.
- The user list must be reviewed regularly.
- Leavers and those no longer requiring access for their duties must be removed from the system immediately.

- Access to ICT facilities shall be restricted to authorised users who have a business need to use the facilities.
- Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a
- legitimate business need e.g. systems or database administrators.
- Authorisation to use an application shall also depend on the availability of a license from the supplier

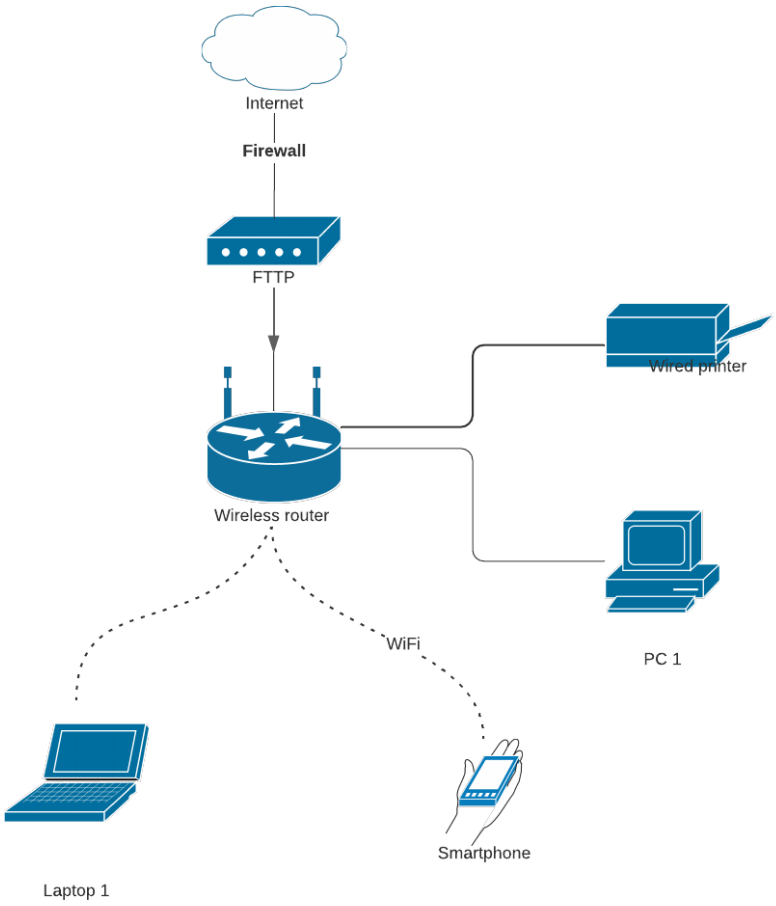
Antivirus and Patching

- Unless completely isolated, computer systems are continually at risk from virus infection. Viruses may be received as:
  - an e-mail message or as an attachment to a message
  - a macro within a word or spreadsheet document
  - an infected program that has been downloaded
  - an addition to removable media
- GPSS shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the Practice’s property without permission from
- the Security Lead. Users breaching this requirement may be subject to disciplinary action.
- If a virus is suspected, prompt action is essential: inform the Security lead immediately
- Unused software must be removed to reduced the number of potential vulnerabilities.
- Antivirus and Antimalware software must be set on update and patched up daily.
- All installed software including Windows operating system must be set to automatic updates
- If a system is more than 5 years old it needs to be re-evaluated in terms of security risk to see if a more up to date system is required.

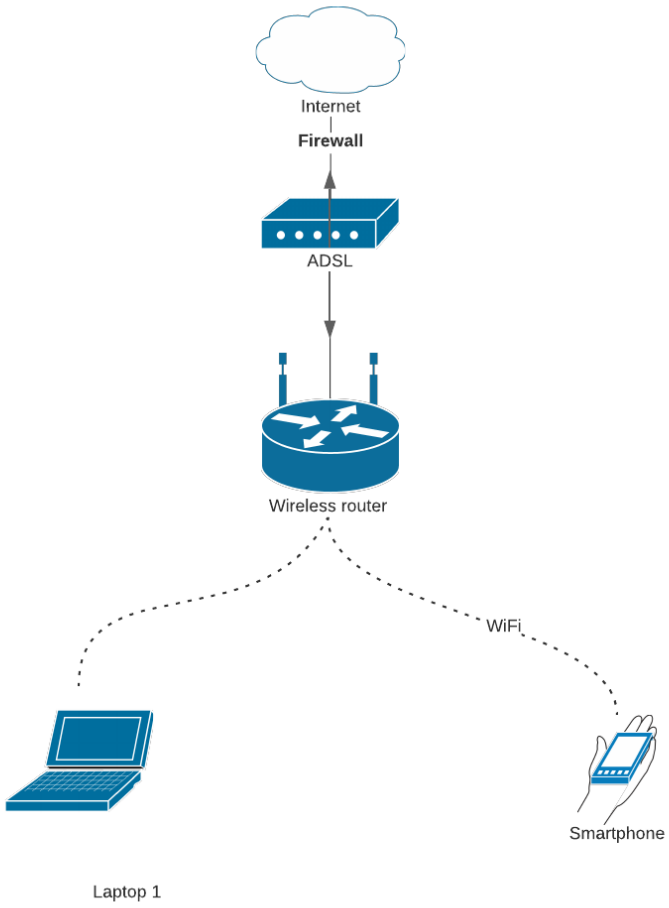
Current Network Maps of Offices within GPSS

- Currently, there are 2 locations for GPSS which represent office environments within the director's home offices. Both are simple with no server.

Office in Purley



-



-

Bring your own devices

- BYOD refers to consumer electronic devices such as smart phones and tablets computers.
- It is important that the data controller must take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction or or damage to personal data
- An asset register of hardware devices must be in place in order to catalogue and ensure every devices has the correct security measures in place
- Devices must be accessible only via passwords as per the password policy or fingerprint reader if the device has this capability. The device must have the option to wipe the data from the device if a certain number of unsuccessful attempts to access the device has been made
- All company data must be stored in cloud storage with the ability to wipe the data from this device if there is a security breach or loss or theft of the device.

- All company data must only be stored within the storage media on the device and not on removable devices
- The device must be locked after non use for 20 minutes with the password required to re-enter the operating system
- Company sensitive Data must only be transferred via cloud storage or within password protected services.
- Where possible the device should stay within the office location and not be used in public wifi locations. If used for demonstration purposes to clients wifi should be turned off
- Find my device services must be enabled for the device to allow the ability to be able to locate it if there is a loss or theft in place.
- The operating system of the device must be up to date and patched regularly with automatic updates turned to on.
- Third party apps must be installed on the authorisation of the data controller to assess the nature of the application in light of security needs.
- Emails must not be stored on the device and only be accessible via cloud services via a password.

Cloud Storage and BCP

- There are an increasing number of services offering ‘cloud storage’ where you can upload documents, photos, videos and other files to a website to share with others or to act as a backup copy. These files can then be accessed from any location or any type of device (laptop, mobile phone, tablet etc).
- Once you have registered for an account you typically create a folder on your computer and every file you place in that folder is copied to the servers of the storage provider. Any changes made to these files are automatically copied across and immediately accessible from other devices you may have.
- All company sensitive files will be stored on the cloud storage service.
- Patient related data must never be stored on the cloud storage service
- Access is via he synced folder and the device which holds the cloud storage must be password protected in line with the password policy
- Cloud storage is useful as an off site store in case data is lost on the device in question due to failure or fire or flood or theft this can be restored back from the cloud.
- Where appropriate files and folders from the cloud storage may be shared by other parties who have access to them with the correct sensitivity in order to ensure smooth running of the business for example photos to share for the graphics designer.
- The password for cloud storage must be unique to any other passwords and strong in nature.
- The cloud storage must have the correct level of security and accessible via https with a minimum of 256bit AES Encryption
- Business continuity plans will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident. The Practice must ensure it has appropriate Business Continuity management arrangements for information assets that include but are not limited to answers to the following queries:
    - Who would the police call “out-of-hours” if the alarm goes off? What about other emergencies discovered at your premises?
    - Who are the key personnel who would need to be involved if an emergency occurs at the practice?

    - Who is your Clinical IT System Supplier who would need to be involved if an emergency occurs at the practice?
    - Ensure that your keyholder details with the police, local authorities (if applicable) or Alarm Company are up-to-date.
    - Maintain a list in priority order of designated keyholders who may be contacted in the event of an emergency. Review and update this list regularly.
    - There are appropriate disaster recovery plans in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis.

Backups

- This is in line with the Cloud Storage section above
- It is important to be able to back up your data in light of fire, flood or theft to be able to be able to get back up running as quickly as possible.
- All data which relates to the company should use cloud storage which yields several advantages
    - easy restoration of data in light of loss
    - back up is off site and also within the device in use
- However
    - It is important the correct password policy is in place to ensure minimum risk of theft and unauthorised access
    - No patient data is ever stored within any back up storage service.
- Examples of approved Storage Services
    - DropBox
    - OneDrive
    - Git for Software

Training

- GPSS will ensure that all users of the network are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities.
- List documents to read and course to attend. To include Training Matrix from this
- The following sections will require training and new employee are expected to go over these sections when starting as part of their induction together with this policy
    - Small Business Guide: Cyber Security - NCSC.GOV.UK
        - Backing up Data
            - Step 1 - Backing up your data - NCSC.GOV.UK
        - Password Protection
            - Step 4 - Using passwords to protect your data - NCSC.GOV.UK
        - Securing Devices
            - Step 3 - Keeping your smartphones (and tablets) safe - NCSC.GOV.UK

Monitoring

- Unauthorised network access will be monitored from the router log which will be reviewed at regular intervals to ensure that no breech as potentially occured

- Any company data on cloud storage will also have a monitoring feature to ensure when each device as last accessed
- On this list GPSS will ensure that devices are removed if they are not longer in use to access cloud storage

Risk Assesement

- Refer to our Risk Assessment Policy. Available on Request

Minimise Data

- It is important to identify the minimum amount of personal data you need to fulfil the indended purpose. That much information should be held and no more.
- Periodically GPSS will review your processing to check that the personal data you hold is still relevant and adequate for purpose, and delete anything that is no longer needed. This is closely linked with the storage limitation principle.
- Anonymise personal data will be erased when no longer needed when it will reduce the risk that it becomes irrelevant, excessive, inaccurate or out of date. Apart from helping with the data minimisation and accuracy principles, this also reduces the risk that GPSS will use such data in error – to the detriment of all concerned.
- GPSS does not need a retention policy as it is small business and will remove data where appropriate and in line wit the storage limitation principle.

IT Contractor Governance

- Refer to our Third Party Contractor Policy. Available on request