Pecyn Cymorth Llywodraethu Gwybodaeth Cymru
Welsh Information Governance Toolkit
IGDC • DHCW

Expectations Guidance Document

3- Information Security

Introduction

This guidance will provide basic information on what will be required from Organisation Administrators and Users to work through and complete the 'Information Security' section of the Welsh Information Governance Toolkit (WIGTK).

Article 5(1)(f) of the UK General Data Protection Regulation (UK GDPR) concerns the 'integrity and confidentiality' of personal information. It says that personal data shall be:

"Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

This means that the organisation should have appropriate technical and organisational security measures in place to prevent personal information that it holds from being deliberately or accidentally compromised. The organisation should ensure an 'appropriate' level of security is in place 'appropriate' to the risk presented by its processing. Whilst information security is sometimes considered as cybersecurity (the protection of your networks and systems from attack), it also covers other things such as organisational or physical security measures.

Organisations must ensure that physical security measures are in place to protect not only personal information but to also ensure the security of hardware and software. It is likely that there may already be established security procedures in place however, these procedures need to be regularly reviewed and made available to staff.

You will need to the organisation's policies, processes and controls in place for this section.

Minimum Expectations

Controlling physical and technical access for staff
The organisation should limit access to personal data to authorised staff only and regularly review users' access rights.

This includes implementing a formal user access procedure to assign access rights for staff and regularly reviewing those access rights and adjusting/removing rights where appropriate.

Your organisation should have a formal process for addressing access rights for all staff, including temporary staff and third-party contractors. You will also need to consider new starters, movers, and leavers for both systems and physical access to confidential information. For example, this could be a 'new starter process' or a 'leavers process'.

Policies and procedures in place should ensure that accounts are promptly deactivated when an employee leaves an organisation, and that role-based access is maintained, and permissions are not carried over into new roles.

The requirements for access controls are set out within the Records management and security section of the ICO's Accountability Framework.

Staff access to systems
Your organisation should know who has access to each system in use and what their access is, such as administrator, read only etc.

This record should be maintained in a register or log. This will allow the organisation to review and audit user access rights to ensure that the assigned access is up to date and correct to their current role.

Organisations should ensure that access to confidential personal information is monitored and audited locally. There should be an agreed process/procedure in place for investigating any issues regarding confidentiality.

Regular monitoring and auditing of systems will help to identify whether confidentiality has been breached or put at risk through deliberate misuse of systems. It can also help to recognise use of weak, non-existent, or poorly applied controls.

Your organisation should ensure that overall responsibility for auditing and monitoring access to personal and sensitive personal information has been assigned to an appropriate senior staff member i.e. Caldicott Guardian, IG Lead or SIRO.

Examples of the types of audits that may be conducted include:

- NIIAS Alert reviews/ audits
- Failed attempts to login
- Dormant or inactive accounts
- Access outside speciality area or department
- Emergency/ access or break glass access controls are triggered

Your organisation should also have an acceptable use or terms and conditions of use procedures in place for staff to read, this should clearly inform staff of the monitoring and auditing which will take place. Understanding of this procedure should be checked regularly.

Administrators of IT system(s) – Third Party Contractors only
The people within your organisation who are IT system administrators may have access to more information than other staff. Therefore, they need to be held accountable in a formal way to higher standards of confidentiality than others. This requirement applies to IT system administrators working in external companies who support your organisation's IT systems.

This formal agreement could be part of a job description or a contract with your IT support company and/or systems supplier/s.

CAF Assessments – HB/Trusts/SHAs and Prison Healthcare only
The NIS Regulations provides legal measures to ensure both cyber and physical resilience of networks and information systems are in place for Operators of Essential Services (OES).

NHS Health Boards, Trusts and Special Health Authorities are classed as an OES and are required to meet the requirements of the NIS Regulations.

Organisations should have in place appropriate and proportionate security measures to manage risks to the network and information systems that support their services, in line with the Welsh Government's Network and Information Systems Regulations 2018 guidance.

In Wales, the NHS Wales Cyber Resilience Unit (CRU) is the appointed competent Authority for the NIS regulations within healthcare in Wales and requires the Cyber Assessment Framework assessment to be completed.

In line with the regulations, regulation 10 requires an OES to:

- take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies.
- take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services.
- It also requires OES to have regard to any relevant guidance issued by the relevant competent authority when carrying out their duties.

Antivirus/anti-malware software
Having systems infected by malware is one of the most common ways that your IT systems can become compromised.

The organisation should take steps to prevent any unauthorised access to systems and applications, for example by using strong passwords, technical vulnerability management and malware prevention tools.

This includes implementing anti-malware and anti-virus protection across the network and on critical or sensitive information systems if appropriate.

As quoted on the National Cyber Security Centre (NCSC) website:

'Antivirus products work by detecting, quarantining and/or deleting malicious code, to prevent malware from causing damage to your device. Modern antivirus products update themselves automatically to provide protection against the latest viruses and other types of malware.'

Further information regarding antivirus/anti-malware can be found within the Records management and security section of the ICO's Accountability Framework and on the NCSC website.

Your organisation should run regular vulnerability scans to be proactive and identify any potential issues.

Password policies
The organisation should implement a password policy and apply password complexity rules and limited log on attempts to systems or applications processing personal data. The organisation should provide staff with guidance on setting and managing passwords.

This helps to secure systems further and reduces the risk of weak passwords being used by staff which could potentially be compromised.

You should also have password management controls in place, including default password changing at regular intervals, controlled use of any shared passwords with specific processes in place for the sharing of the password, for example who authorised users are and secure password storage (not in plain text).

It is important that all staff are made aware of the password policy and where they can find this.

Enforcing password policies – Not applicable to GPs
Your organisation should have technical controls in place to enforce the password policy.

For example, if your policy states that passwords must contain at least 12 characters, a number and a symbol, your organisation should have technical controls implemented on the system so that only accept passwords meeting that criterion is accepted. Another example is that if your policy states that new passwords should be set every 3 months, having those controls in place to ensure this is carried out by staff.

IT systems – Not applicable to GPs
Systems and software that are no longer supported by the manufacturer can be unsafe as they are no longer being updated by the supplier, which will make your systems vulnerable to viruses and other attacks.

Despite systems still being functional, if they are no longer supported it will mean that there is an increased likelihood of becoming vulnerable to online threats. If a security weakness is discovered, the software can be compromised, and information put at risk of a cyber-attack.

Some examples of unsupported software include Windows XP, Windows Vista, Windows 7, Java, or Windows Server 2008.

This also applies to software systems such as rostering or care planning.

Please Note: For Third Party Contractors, all devices in your organisation should have technical controls that manage the installation of software on the device.

Physical controls and maintaining security measures

Your organisation should have measures in place to protect and secure areas that contain sensitive and/or critical information. This will help to protect the confidentiality, integrity and availability of the information.

There are a few ways that you can implement appropriate physical security measures, some examples are applying entry controls such as locked doors, alarms, security lighting or CCTV.

Additional protection against external and environmental threats should also be implemented in secure areas, and you should consider what controls need to be in place for locations such as server rooms.

Where possible, access to secure areas should be recorded, such as using swipe cards. This information can then be accessed if there were ever to be an incident that needs to be investigated.

Your organisation should have a procedure in place for visitors and ensure that they are signing in when they enter the premises. The sign-in log should record at the minimum the visitors name and what time they entered and left the building. Visitors should be given name badges and escorted while they are on premise. You should ensure all staff are aware of the process regarding visitors.

Staff should also be aware that maintaining the security of their work area is extremely important and is everyone's responsibility. This includes:

- Adhering to clear desk policies
- Locking computer/laptop screens when away from desks
- Ensuring windows/doors are locked where required, and not propped open
- Being vigilant of tailgaters when entering secure areas
- Reporting any other suspicious behaviour

Staff should be reminded frequently that these responsibilities also extend to home and remote working.

Your organisation must make staff aware of their responsibilities and direct them to the appropriate policies for maintaining security when at work.

The organisation should create a positive culture surrounding reporting and escalating any incidents that may occur. There should be a procedure in place so that staff know who to contact and how best to escalate any issues if necessary. Staff should be made aware of this on a regular basis.

Bring Your Own Device (BYOD) policy and mobile devices

BYOD is the concept of staff using their personal devices for work purposes.

With BYOD, the organisation has ownership of the business data and resources that may be accessed or stored on a device, but the device itself is the property of the user.

BYOD can bring about security risks, however, with the right technical controls and policies in place, the risks with BYOD can be minimised.

Further guidance on BYOD is available on the National Cyber Security Centre website.

Where the organisation provides access to mobile devices, such as mobile phones, for work purposes, appropriate controls in the case of lost and stolen mobile devices should be in place to ensure that inappropriate access and use is minimised.

Controls should include:

- Security PINs/ Passcodes/ Face Scan
- Ability to remote wipe device contents.

Use of public Wi-Fi

Your organisation should provide guidance to all staff members on the use of public Wi-Fi (e.g. Wi-Fi freely available at cafes and train stations etc) or unsecured Wi-Fi (Wi-Fi where no password is required to access it).

As there is no way to identify who owns or controls the public Wi-Fi, there is an increased risk that unauthorised users could be accessing the connections and see what you are working on whilst connected to the Wi-Fi. This could lead to unauthorised access of personal data if staff are using work devices, and hackers could potentially be able to access the user's log in details and passwords.

Staff should be encouraged to avoid using public Wi-Fi and use safer methods if required to work outside of office locations, such as using a work issued Virtual Private Network (VPN) connection to access information.

Wi-Fi passwords

Networking components include routers, switches, hubs, and firewalls at all your organisation's locations. These should have their passwords reset from the manufacturers default before they are used. Your organisation may just have a Wi-Fi router, but this will still need to have its password updated before you start to use it.

This also includes any equipment such as new laptops or PCs if they have a manufacturers password applied. These passwords should be updated before they are issued to staff for use.

Please note that this does not apply to Wi-Fi routers for people working from home.

Encryption – Not applicable to GPs

The organisation must ensure that any devices such as laptops and tablets that hold or allow access to personal data are encrypted. Where your organisation has a need to store personal data on removable media, such as USB drives or CDs, these must be encrypted. You should minimise the personal data transferred and stored on these devices and implement a

software solution that can set permissions or restrictions for individual devices as well as an entire class of devices.

Paper records
The security of your paper records should be considered with the same importance that information held electronically is.

All paper records should be appropriately stored and protected to reduce the risks of environmental threats and opportunities for unauthorised access. This could be implemented by having secure storage rooms in your organisation where sensitive documents are stored, and the rooms are secured with appropriate pin-codes or swipe card access.

You should have a robust procedure in place for when paper records are transferred outside of the building that clearly states who now has the record, their contact details, and the date that the record left the building, which can be referred to should any issues arise. Keeping these audit logs will help to maintain good records management as you can keep track of where your records are at all times. You should ensure that the person has the correct authority to access the files and take them offsite.

All staff should be made aware of the procedure, so they understand their responsibilities and what steps need to be carried out to allow the transfer of paper records outside of premises.

Penetration Testing – Third Party Contractors only
Annual IT penetration testing is scoped through negotiation between the person responsible for IT, management and testing team, and includes a vulnerability scan and a check that all networking components have had their default passwords changed.

Exceeded Expectations

This section is not required to be completed; however, it will help to further demonstrate your compliance and provide assurance.

These questions build on those you will have answered in the minimum expectations section; however, they are slightly more in depth.

Routine Information Security Checks/Audits
Your organisation should carry out regular spot checks to ensure staff are undertaking their responsibilities in line with the policies and procedures set. This will help to identify whether these policies are working effectively or need to be amended in any way. These checks should be undertaken at least every year.

Evidence of the spot checks/audits carried out should be retained, with key areas of concern highlighted. This may include any actions, and who is responsible for the action. Areas of concern should be included in an information security improvement plan and escalated appropriately.

Outcomes of information security audits should be reported to the senior management team or Board to ensure appropriate oversight.

Surveying Software/Hardware – Third Party Contractors only
The organisation should hold an up to date list of all your end user devices and removable media.