OMBWDSMON GWASANAETHAU CYHOEDDUS CYMRU
PUBLIC SERVICES OMBUDSMAN FOR WALES

Information Security Policy

Mae’r ddogfen hon hefyd ar gael yn y Gymraeg
This document is also available in Welsh

Information Security Policy

Contents

Information Security Policy

1. Purpose

1.1. Under data protection legislation the Public Services Ombudsman for Wales (PSOW) must ensure that it has appropriate organisational and technical security controls in place to protect personal data from unauthorised or unlawful processing and accidental loss, destruction or damage.

1.2. All information, including personal data, has value and it is important that PSOW understands what information it processes to consider how best to protect it to ensure the information is protected at rest and in transit.

1.3. Processing broadly means collecting, using, disclosing, sharing, retaining, or disposing of personal data or information.

1.4. Information security incidents can cause damage and distress to those whose personal data is at risk. For PSOW there are legal, financial and reputational risks.

1.5. This policy is a key component of the Ombudsman's overall information governance framework and should therefore be read in conjunction with relevant organisational policies, procedures, and guidance.

2. Scope

2.1. This policy relates to all information, information systems, networks, applications, locations and users of the Ombudsman's services or supplied under contract to it.

2.2. The policy applies to all PSOW staff (including permanent staff, contract staff, temporary staff) and individuals or organisations contracted directly by PSOW).

3. Information security objectives

The PSOW is committed to achieving the appropriate level of confidentiality, integrity and availability of information assets and to maintaining the resilience of critical activities. This policy describes the principles of information security and explains how they shall be implemented in the organisation. The policy sets out how PSOW will:

- Ensure that all members of staff are aware of the need for information security in day-to-day business, that they understand their responsibilities and that they consistently and fully comply with the relevant legislation as described in this and other policies.
- Protect information assets under the control of the organisation, including when working collaboratively with suppliers.
- Create a climate which minimises breaches of this policy but encourages the prompt and open reporting of any such breaches.

4. Abbreviations

COODOI	The Chief Operating Officer and Director of Improvement. For information governance purposes also referred to as Chief Information Security Officer (CISO).
ITM	Information Technology (IT) Manager.
CLADOI	Chief Legal Adviser and Director of Investigations (For information governance purposes also referred to as Senior Information Risk Owner (SIRO).
IGM	Information Governance Manager.

5. Roles and responsibilities

5.1. The COODOI is accountable to the Ombudsman for overall information governance, including the security of the PSOW information, including cyber security and resilience of PSOW networks. The COODOI works with others to advise the Ombudsman and Management Team on how best to manage risk whilst exploiting technology to deliver the PSOW's strategic objectives.

5.2. The CLADoI is the organisation's SIRO with responsibility for monitoring information risk management within the organisation.

5.3. Responsibility for managing and implementing the policy and related procedures rests with the ITM and IGM who are accountable to the CLADoI and COODOI.

5.4. Any breaches of the policy need to be communicated, by the member of staff or manager, to the ITM or IGM as soon as possible after the breach is known.

5.5. The ITM and IGM are responsible for ensuring that all persons who have authorised access to PSOW IT systems are aware of:

- The information security policies applicable in their work areas.
- Their personal responsibilities for information security.
- How to access advice on information security matters.

5.6. All staff shall comply with this Policy and associated information security procedures and guidance listed at the end of this document. Each member of staff shall be individually responsible for the security of their physical environments where information is processed or stored.

5.7. Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

6. Risk Management

6.1. PSOW recognises it has a responsibility to manage both internal and external risks as a key component of good corporate governance. It is committed to embedding risk management into the daily operations of the organisation from the setting of objectives to service and financial planning through to departmental processes. It believes that effective risk management will help it to achieve its corporate objectives. The Risk Management Policy sets out PSOW's approach to managing risk, including risk identification and treatment.

6.2. This includes the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence for each category of information.

6.3. All teams will have identification of risk as a standing item on their team meeting agendas.

7. Human Resources Security

7.1. **Contracts of employment**

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause, restricting the disclosure of confidential information gained during their employment with the Ombudsman.

7.2. **Starters and leavers process**

New staff joining PSOW will be provided with appropriate building and IT access as required by their role. Building and IT access is revoked when staff leave PSOW. The starters and leavers process is managed jointly between Corporate Services and the IT Team.

7.3. **Change of role**

Corporate Services and the IT Team need to be informed of any changes of staff role so that IT / physical access rights can be reviewed.

7.4. **Training and awareness**

Information security is everyone's responsibility. An information governance (IG) training strategy sets out the staff IG training and development requirements. The strategy also includes a communications plan identifying key messages for the forthcoming year. Mandatory refresher training is identified each year and included within the organisational annual training plan.

Information security awareness training, and details of the Staff Standards of Conduct (which includes acceptable IT use), shall be included in the staff induction process. This training shall include understanding of this policy and how it relates to day-to-day work activities.

8. Asset Management

8.1. Information assets are catalogued according to business functions and managed through the Information Asset Register. Information Asset Owners and Assistants identify, implement and maintain risk management controls for information assets they are responsible for. A list of information assets due for review is identified on an annual basis.

8.2. **Business continuity and Disaster Recovery plans**

The PSOW shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all critical information, applications, systems and networks.

Staff are to save case-related material within the case management system, and other files and records to the relevant systems, or to server drives or the Hub intranet. Staff should not use local file storage on their PC desktop or PC hard disk.

IT back up arrangements are detailed in the 'Management of IT' policy The backup arrangements are detailed in the 'Management of IT' policy and include:

- On site server mirroring – for short term data recovery in the event of a server/application failure.
- On site backup
- Cloud backup
- Back up arrangement of hosted systems

Further information can also be found within the organisation's Business Continuity Plan.

8.3. Systems are designed so that when records reach their relevant retention period they can be safely and securely archived in line with the requirements of the Records Management Policy.

9. Network management

9.1. The PSOW's IT and communications network is designed, configured, maintained and managed by the IT Team in conjunction with the IT Support Service Provider. They oversee the day to day running of the network, ensuring ongoing security, confidentiality, integrity and availability of data and systems. This includes managing the gateways that link the PSOW systems to the Internet to reduce the risks associated with hacking, denial of service attacks, malware, and unauthorised access. These controls are applied to incoming and outgoing traffic.

9.2. Management of computers and networks shall be controlled through standard documented IT team procedures that have been authorised by the ITM.

9.3. Any access to the PSOW Network must be password protected. Systems must be set up to reject passwords that do not meet the required complexity standards.

9.4. **Connecting devices to the PSOW network**

PSOW systems and networks retain records of connected devices and of access. Access to PSOW systems and networks is restricted to PSOW devices and any other device (such as personal smartphones or tablets) specifically authorised by PSOW. All use is subject to acceptable use restrictions as set out in the Staff Standards of Conduct Policy. Device management software will be used on PSOW devices and on personal devices that are permitted to access PSOW systems and networks (other than guest wifi).

9.5. **USB memory stick or similar user media**

Non PSOW issued portable memory devices such as USB memory sticks or similar, require the approval of IT before they may be used on the PSOW systems. Such media must also be fully virus checked before being used on the organisation's equipment. Whilst this does not apply to CD/DVDs sent by Public Bodies due to the lower risk of malicious content, it is still important that CD/DVDs sent in from members of the public are referred to IT to ensure there is no executable files contained within them.

9.6. **Mobile devices (e.g. laptops/tablets/smart phones)**

For business continuity and PSOW meeting purposes, the Ombudsman may issue authorised staff with PSOW owned smart phone and/or tablet PCs.

Staff who have authorised use of Ombudsman's mobile devices must comply with specified settings, update and usage requirements. They should also ensure the physical security of the mobile device against theft and/or unauthorised access of any data contained within the mobile device. Further details of measures to be taken can be found in the How to work securely from home guidance.

9.7. **Change management**

Prior to installation and commencement, all new information systems, applications and networks must be risk assessed for security. Changes to information systems, applications or networks shall be reviewed and approved by the ITM.

A Data Protection Impact Assessment must be undertaken to consider the impact of changes to any personal data processing. The Data Protection Impact Assessment Policy provides more information about this process.

10. Vulnerability management

10.1. Examples of system or software vulnerabilities include software that requires patching to remedy defects, or there may be known system configuration issues. Software vulnerabilities can be exploited. The IT Team will, working with the IT Support Provider, ensure that these are identified, assessed and that updates, patches and fixes are promptly applied.

10.2. **Perimeter security monitoring**

This is detailed in the ‘Management of IT’ policy and includes:

- Blocking email by content and/or attachments
- Authentication checking incoming emails
- Firewalls in place
- Segregation of data on IT systems

10.3. **Vulnerability scanning**

PSOW will ensure regular penetration and vulnerability scans are undertaken and reported on. The schedule and arrangement details for this are detailed in the ‘Management of IT’ policy and includes

10.4. **Malware protection**

Effective malware protection shall be in place for all PSOW IT systems. Further details about management procedures to protect itself against the threat of malicious software are detailed in the ‘‘Management of IT’ policy. Users are by default not able to install software on the organisation’s property without permission from the ITM.

10.5. **Up-to-date systems and software**

PSOW shall ensure that all information products are properly licensed and approved by the ITM. Users shall not install software without permission from the ITM. Staff are to accept and install updates on PSOW, and any own devices connected to PSOW systems or networks (other than guest wifi), regularly and promptly.

10.6. **Patching and updates**

Patching is the subject of a separate Patch Management Policy as per the ''Management of IT' policy to ensure complete and timely patching of software and systems to maintain security.

11. Physical and environmental security

11.1. As well as protecting access to information systems and the PSOW IT Network PSOW also takes steps to protect access to the building, including secure areas.

11.2. Access to network and communication facilities, including server rooms and data centres must be adequately protected against accidental damage (such as from fire or flood), theft or other malicious acts. Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

11.3. External doors into the building are secured and accessed by use of a numeric code. Members of the public cannot walk into the common areas of the building.

11.4. All doors to PSOW-occupied areas are secured by physical lock or by the ID card entry system managed by Corporate Services.

- Reception: This is open to the public only during office hours, but accessible only when admitted through external doors. Access from PSOW Reception to PSOW offices is also controlled by the card entry system.

- General Office: Authorisation for access to the PSOW open plan office may be given by any member of staff during office hours, but the visitor must be accompanied to the relevant member of staff they are visiting. The default access is for PSOW staff only plus the relevant office cleaner.

- IT Comms room: Authorisation for this access is managed by IT team. The default access is ‘no access’ apart from PSOW IT staff.

- Archive room: Authorisation for this access is managed by Corporate Services. The default access is ‘no access’ apart from Corporate Service/Casework Support and CAT Casework Officers.

11.5. To minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards and subject to security marking. All PCs when located in the open office environment (i.e. not stored in a restricted access secure storage room) are to be secured using lock and security cable.

11.6. An inventory of all PSOW IT equipment that is marked for disposal that has stored personal information contained within it must be maintained by PSOW IT Team, detailing the disposal company used. A written agreement is required to be in place with PSOW and the disposal company detailing the requirements for the disposal which must include mention of the disposal company as the ‘data processor’ under the control of PSOW as the ‘data controller’. A requirement for the disposal company to destroy personal information in a secure manner and provide PSOW with a destruction certificate must also be included in the agreement.

11.7. All staff must be aware of the need to employ physical security measures such as:

- Locking filing cabinets and side filers.
- Locking PC screens when taking a break and switching off the PC and monitor when desk is going to be unattended for some time (such as the end of the day).
- Close PSOW office blinds at the end of the day.

- Ensure that confidential PSOW information is cleared from the desk at the end of the day or when unattended. Original medical records must be stored securely in the fire-proof safe outside of normal office hours. Staff should discuss arrangements for this with Casework Support or Corporate Services.
- Securely dispose of confidential PSOW information when it is no longer required.
- Always keeping access cards, keys and keycodes secure.

Further guidance for staff is available in the How to work securely from home guidance.

12. Identity and access management

12.1. To ensure the security of PSOW information and information systems it is essential that user access accounts and access rights are effectively managed according to business need. The IT Team manage the registration and deregistration of user accounts through Active Directory.

12.2. Access rights will be restricted to the minimum required to enable the user to fulfil their role.

12.3. Multi Factor Authentication

Levels of access to PSOW Systems including third party hosted systems, shall be controlled and restricted to those authorised users who have a legitimate business need. Further information on this can be found in the ‘‘Management of IT’ policy

13. Information Security Incident Management

13.1. PSOW is committed to minimising information security incidents and their impact. Suspected incidents are to be reported promptly to the IGM, and to the ITM if they relate to IT. All incidents are investigated to establish their cause and impact with a view to avoiding similar events and to identify improvement opportunities. The process is set out in the Information Security Incident Management Policy and Procedure.

13.2. The IGM maintains a central log of incidents so that progress with the management and investigation of the incident can be monitored.

13.3. IT staff must immediately report any cybersecurity incidents to the COODOI and IGM for recording centrally.

13.4. The monthly IG (and IT) reports to Management Team provide a summary of incidents reported and subsequent actions. Quarterly reports to the Audit and Risk Assurance Committee also include reference to incident management.

13.5. The IGM, with the assistance of the IG Training Group analyses incident trends to inform further information security training and communication needs.

14. Supply chain security

14.1. Contracts with external contractors that allow access to the PSOW's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

14.2. It is important that supply chain risks are explored with the potential suppliers and security controls are understood. All contracts must include reference to the requirement for the supplier to report any information security risks or incidents immediately to PSOW.

15. Monitoring and Reporting

15.1. Testing of the security of all IT systems will be conducted regularly as detailed in the ''Management of IT' policy …

15.2. Internal Audits on information security related areas including cyber security shall be included in the internal 3-year audit workplan.

15.3. The ITM and/or IGM shall keep the Management Team informed of any issues that seriously affect the information security status of the organisation.

15.4. There will also be an annual report to management team and subsequently to the Audit & Risk Assurance Committee which will contain the following:

- IT access: external penetration tests.
- IT access: internal compliance with this policy.
- Monitoring of visitors.
- Compliance testing on transfer of information.
- Any data loss incidents and subsequent actions since the last report.

16. Review

16.1. The Information Security Policy shall be maintained, reviewed every two years and updated by the ITM and IGM.

17. Related policy / process / guidance

- Management of IT policy
- Staff Standards of Conduct Policy
- Security of emails (and other correspondence)
- Working securely from home
- Information Security Incident Management Policy and Procedure.
- Risk Management Policy
- Business Continuity Policy