Archwilio Cymru
Audit Wales

Reference: Version 3.4
Date issued: March 2020
Key contact: [redacted]

Information Security Policy

Contents

Revision history 2

Summary 3

Information Security Management System 3

Staff responsibilities 4

- Usernames and passwords 4
- Connecting personal or non-Wales Audit Office equipment 4
- Care of equipment 4
- Obtaining and communicating information 5
- Memory sticks (also known as USB sticks or drives) 6
- Personal computers, smartphones and tablets 7
- Backing up data 7

Acceptable use 7

Security monitoring 8

Reporting security incidents 8

Getting help 9

Revision history

Version	Summary of changes	Date
V1.0	First version finalised.	February 2006
V1.1	Change of Information Security Officer, amended paragraph 29 such that connection to home broadband network is permitted.	October 2007
V2.0	Major revision including more detailed guidance on 'care of equipment' and 'obtaining business data from audited bodies'.	October 2008
V2.1	Change reflecting that Wales Audit Office equipment eg laptops, memory sticks can be left unattended in vehicles for up to four hours if hidden and locked in the boot, or equivalent.	May 2009
V2.2	Revision to section on Security Monitoring and Enforcement, explaining that routine monitoring will take place. The monitoring will check staff compliance with the law and this Information Security Policy. Access to social networking and external email websites prohibited.	July 2010
V2.3	Inclusion of material to provide clarification of unacceptable use of information processing facilities. Inclusion of new appendix 3 setting out detailed routine monitoring policy.	September 2011
V3.0	Major revision – Information Security Policy now focuses on practical requirements. Higher level information processing principles, together with roles and responsibilities, are now found in the separate Information Governance Policy.	April 2015

V3.1	Inclusion of new paragraph to outline data breach procedures in order to comply with the General Data Protection Regulation.	August 2017
V3.2	Change to advise that how data can be transferred using Microsoft files with strong password protection.	February 2018
V3.3	Changes to more clearly define data categories.	May 2018
V3.4	Clarification of use and protection of personal devices	March 2020

Summary

1 The requirements in this policy apply to all employees, non-executive members and contractors, whether employed via an agency, or directly. For brevity, in this document, 'staff' is defined to mean all of these categories of people.

2 This policy describes the practical steps staff must take in order to keep the organisation's information secure.

3 Whereas this policy has a practical focus, it should be read in conjunction with the Information Governance Policy, a higher-level document which covers the principles of information processing and the related roles and responsibilities.

4 All staff are required to make themselves familiar with this Information Security Policy, and to confirm in an annual declaration to Law & Ethics (or the Board Secretary in the case of board members) that they have read and understood the contents.

5 This document contains the official policy of the organisation. The revision history is shown on the cover sheet.

Information Security Management System

6 The Wales Audit Office has adopted the International Standard for Information Management Security Systems (ISO 27001) whose principles include:

7 systematically examining and assessing the Wales Audit Office's information security risks, taking account of the threats, vulnerabilities and impacts;

8 designing and implementing a coherent and comprehensive suite of information security controls and/or other forms of risk treatment to ensure risks are reduced to an acceptable level; and

9 adopting an overarching management process to ensure that the information security controls continue to meet the organisation's information security needs on an ongoing basis.

Staff responsibilities

Usernames and passwords

10 Each staff member will be provided with a username-password combination for use with Wales Audit Office systems, for example, when logging on to a laptop, or retrieving a monthly payslip. Such passwords must not be shared with colleagues. Please contact the IT team if you are not able to get access to the systems or resources you need.

11 Passwords should be set to something memorable, and never written down.

Connecting personal or non-Wales Audit Office equipment

12 Personal or visitors' smartphones or computers may be connected to the Internet via the Wales Audit Office's guest WiFi – search for 'guest WiFi' on the Hub for details. Non-Wales Audit Office equipment must not be connected in any other way – for example via a network cable.

Care of equipment and information

13 Although data on Wales Audit Office laptops and smartphones are protected by encryption, staff must take reasonable care of Wales Audit Office equipment. Staff must also take all reasonable care of Wales Audit Office information processed on personal devices or held in paper form. Theft or loss of Wales Audit Office equipment or information due to a failure to take reasonable care will be treated as a serious matter.

14 Staff must not leave Wales Audit Office equipment or information unattended where it is at risk of theft – for example, open (ie screen unlocked) on the table on a train journey, or in an unlocked hotel meeting room during lunch.

15 Wales Audit Office equipment or information can be left unattended in a car for up to 4 hours, provided it is hidden from view and the car locked – but never overnight.

16 Staff may leave Wales Audit Office equipment or information unattended at office sites where there is reasonable 'perimeter security' ie measures to prevent unauthorised people from getting into the office, or at home.

17 All Wales Audit Office equipment and information must be returned via the line manager when employment finishes, or via Business Services in the case of Board members.

Obtaining and communicating information

18 The Wales Audit Office classifies information into three categories. Different handling precautions apply, depending on the category:

a. **Highly sensitive data – information which, if disclosed inappropriately, has the potential to cause serious distress or damage to individuals or serious damage to the reputation or interests of the Auditor General for Wales, the Wales Audit Office or other parties such as audited bodies, the Welsh Ministers and the National Assembly for Wales.** This will include taxpayer information, as defined by the Tax Collection & Management (Wales) Act 2016, and any significant personal data, for example, an audited body's payroll file containing names, addresses and bank details used with computer-aided audit techniques (CAATs), or information submitted by the Wales Audit Office to the Department for Work and Pensions containing details of employee pension contributions. Such information should only be transferred and processed:

   i. following review by the Wales Audit Office's Data Protection Officer (DPO) who will advise on the security measures required and, where appropriate, liaise with the Data Protection Officer at the audited body;

   ii. by a secure encrypted method, preferably encrypted email (see hub) or web-based encryption[1];

   iii. in accordance with specific procedures authorised for the business process in question. For example, CAATs data are subject to a specific policy, may only be stored on a standalone, encrypted machine which does not leave the Wales Audit Office

[1] If encrypted email or web-based encryption are not practicable, you may pass information hand to hand to pre-arranged named contacts by encrypted memory stick. Alternatively, you may use strong password protection on Microsoft Office files with the password communicated to the recipient separately and by a different method. This may be useful for internal communication of highly sensitive information, such as disciplinary reports. Password protected files entering the WAO will, however, be quarantined, so you will need to ask IT for their release.

premises, and must be deleted as soon as the audit work is completed.

b. **Sensitive data – information which has the potential to have a negative impact on individuals or the interests or reputation of the Auditor General for Wales, the Wales Audit Office or other parties such as audited bodies, the Welsh Ministers and the National Assembly for Wales.** Examples include:

   i. pre-publication reports in which there is press interest, or with significant impact on individuals, which are about wrongdoing, or which are politically sensitive; and

   ii. reports or letters drafted in response to a complaint

   iii. emails or documents which contain personal data.

   Data of this kind may be stored on a Wales Audit Office laptop for as long as it is being worked on but must be deleted from the laptop once work is complete.

   Staff must use a secure means of exchanging data of this type, for example, encrypted email, if the intended recipient is able to use this.

c. **Other data –** these are data not covered by the categories above and include, for example, general audit working information and minutes of meetings.

   This type of data can be stored on laptops as required. Ordinary, internet email can be used to acquire or exchange it.

19 Staff must make themselves aware of, and follow, any specific requirements or policies an audited body has in place, for example, for documents which are protectively marked. If, however, an audited body's requirements appear to be unduly onerous so as to hinder audit access, staff should raise the issue with Law & Ethics.

Memory sticks (also known as USB sticks or drives)

20 Unencrypted memory sticks, which do not require a password, must never be used with Wales Audit Office data.

21 Staff should also avoid the use of encrypted memory sticks. However, such a stick may be used if it is the only reasonably secure practical option; for example, if the use of encrypted email or secure file transfer by web-based portal (e.g. Egress) is not practicable.

Use of “own devices” such as personal smartphones for WAO work

22 The WAO appreciates that it is convenient and effective for the organisation (as well as staff), for staff to use their own devices for WAO work. The WAO remains, however, responsible for the processing of its data, even if it is done on such devices. The processing of WAO data, such as use of the WAO Outlook app for email, on own devices is therefore subject to the requirements of the Information Governance Policy and the “Staff responsibilities” and “Reporting security incidents” sections of this policy. Staff must make all reasonable effort to ensure that WAO information they process on their own devices is secure. To do this, staff must refer to the WAO ***Bring Your Own Device Policy & Guidance*** on the Hub to check whether their use of their device is sufficiently secure, and, if necessary, take advice from the IT team.

Backing up data

23 Information held on Wales Audit Office systems, for example, Insight and Sharepoint online are automatically backed up. There is no need for staff to take specific backup action.

24 Staff must take steps to back up work, where the only up-to-date copy is on an individual’s laptop. For example, at the end of a day during which a staff member has been updating a particular report, the latest version should be saved to Sharepoint or the Insight system. This will guard against information loss in the event that the laptop fails, which can occasionally happen without warning.

25 Note that unlike the main mailbox, ‘personal folders’ within Outlook, also known as PST files, are **not** backed up automatically. Staff should back these up manually if they are used.

Acceptable use

26 Staff must not use Wales Audit Office equipment in any way that may harm the organisation’s reputation. For example, staff must not send, store or deliberately access material that:

- is obscene or pornographic;
- is likely to cause widespread offence;
- is malicious, abusive or defamatory in nature;
- is racist, sexist or otherwise constitutes unlawful discrimination in terms of protected characteristics defined by the Equality Act 2010 (ie in terms of

age, impairment (disability), gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex (gender) and sexual orientation); or

- constitutes harassment.

27 Staff may use Wales Audit Office equipment for personal purposes, for example, online banking, shopping or reading the news, provided the time spent doing so is a reasonably short 'break from work'. Staff must not use personal webmail on Wales Audit Office laptops.

28 Where personal use of Wales Audit Office equipment incurs a cost, for example, personal calls on mobile or desk telephones, this must be limited to £5 per staff member per month or be reimbursed.

29 Staff may use social media, subject to the organisation's Social Media Policy, which is on the Hub. In general, staff should be aware that the rules and principles of conduct which govern the real world also apply to the online world.

30 Staff must make themselves aware of and follow any specific requirements or policies an audited body has in place when using its computers or systems.

Security monitoring

31 Wales Audit Office uses a range of monitoring techniques to ensure information and systems are properly protected, and that staff comply with Wales Audit Office policies and the law.

32 The Wales Audit Office will ensure monitoring arrangements are reasonable and proportional to the risks.

33 Staff must accept that any use of Wales Audit Office equipment, whether business or personal, may be recorded, scrutinised or investigated by these automated or manual means.

Reporting security incidents

34 Staff must report security incidents to the IT helpdesk. These could include instances where, eg staff of an audited body have sent personal and sensitive information via ordinary internet email, or where a laptop has been stolen. Prompt reporting should enable corrective action to be taken and help the Wales Audit Office and other bodies to learn and make any necessary changes to avoid a repeat.

35 The IT helpdesk will inform the Information Security Officer and the Head of Law & Ethics of any incident, who will liaise regarding its handling. Law & Ethics will assess and record the incident and consider next steps in accordance with a data breach checklist, including any communication required with internal and external stakeholders and the Information Commissioners Office.

Getting help

36 If you need advice on anything within this policy, or any practical aspect of working with information on Wales Audit Office equipment, please contact the IT team on 02920 320690 or via Skype or email to “IT Support”.