Reference: Version 3.5
Date issued: July 2024
Key contact: Matthew Jubb

Information Security Policy

Contents

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 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
V3.5	Edited for readability, removed references to old product names e.g. Skype, Insight and replaced "Wales Audit Office" with "Audit Wales". Updated guidance on memory sticks. Updated guidance on passwords, use of laptops whilst travelling, screen protectors.	July 2024

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 to keep the organisation's information secure.

3 Whereas this policy has a practical focus on information security, it should be read in conjunction with the Information Governance Policy (including Data Protection Policy), a comprehensive 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 ensure 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 Audit Wales has adopted appropriate controls from the International Standard for Information Management Security Systems (ISO 27001) whose principles include:

- systematically examining and assessing Audit Wales' information security risks, taking account of the threats, vulnerabilities and impacts;
- 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, including replacing or updating systems that have developed cyber vulnerabilities, and preparing in advance to facilitate recovery, should a cyber attack happen;
- 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

7 Each staff member will be provided with a username-password combination for use with Audit Wales systems, for example, when logging on to a laptop, or retrieving a monthly payslip. Colleagues will be asked to change the password at their IT induction session. 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.

8 Passwords should be set to something memorable, and never written down. Google "NCSC three random words" for guidance from the National Cyber Security Centre on how to choose a strong password that is easy to remember.

9 You must not use the same password as on any personal accounts you use e.g. Amazon, Gmail, Ebay etc.

Connecting personal or non-Audit Wales equipment

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

Care of equipment and information

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

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

13 Confidential work information must be protected and therefore staff must be careful about their laptop screen being visible to others. When travelling, staff must not work on confidential matters or documents with personal data when there is a risk of their screen being seen.

14 Staff must lock their laptop screen when stepping away from their laptop, whether they are working in an office, from home or other locations. If there is a business need for screen protectors (which helps prevent information being visible to others), for example if office space is being shared with staff from another body, staff must contact IT with their request.

15 Audit Wales 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 Audit Wales equipment or information unattended at office sites where there is reasonable 'perimeter security' i.e. measures to prevent unauthorised people from getting into the office, or at home.

17 All Audit Wales 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 Audit Wales 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, Audit Wales 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 information submitted by Audit Wales to the Department for Work and Pensions containing details of employee pension contributions. Such information should only be transferred and processed following review by Audit Wales'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.

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, Audit Wales 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 an Audit Wales 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 By default, memory sticks are blocked on Audit Wales laptops. If you are considering using a memory stick for any purpose, please contact the IT Team for advice.

Use of "own devices" such as personal smartphones for Audit Wales work

21 Audit Wales appreciates that it is convenient and effective for the organisation (as well as staff), for staff to use their own devices for Audit Wales work. Audit Wales remains, however, responsible for the processing of its data, even if it is done on such devices. The processing of Audit Wales data, such as use of the Audit Wales 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 Audit Wales information they process on their own devices is secure. To do this, staff must refer to the Audit Wales ***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

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

23 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. This will guard against information loss if the laptop fails, which can occasionally happen without warning.

Acceptable use

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

a. is obscene or pornographic;

b. is likely to cause widespread offence;

c. is malicious, abusive or defamatory in nature;

d. 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

e. constitutes harassment.

25 Staff may use ’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’. Personal webmail on ’laptops is blocked for cyber security reasons.

26 Where personal use of Audit Wales' 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.

27 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.

28 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. There is guidance available on remote access in the ‘information handling’ section of the Digital Skills framework.

29 It is prohibited for staff to transfer information obtained in the course of their work outside the work domain to unauthorised recipients or devices, including their own personal email or storage. These transfers would amount to unauthorised processing of information and could result in personal data breaches. This prohibition applies during the course of employment, during notice period for leavers and after employment has ended.[2]

Security monitoring

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

[2] **The Information Governance Policy sets out the requirements for information handling and data protection, the Staff Code of Conduct and employment contracts set out requirements relating to confidentiality.**

31 Audit Wales will ensure monitoring arrangements are reasonable and proportional to the risks.

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

Reporting security incidents

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

34 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 the data protection checklist, which includes assessing the level of risk presented by the incident. The Data Protection Officer will provide advice on whether a personal data breach has occurred and whether this requires reporting to the Information Commissioner's Office.

Getting help

35 If you need advice on anything within this policy, or any practical aspect of working with information on Audit Wales equipment, please contact the IT team on 02920 320690, email "IT Support" or contact a team member directly via Teams.