Scottish Government IT Security Policy

The purpose of this policy is to set out the Scottish Government aims and objectives for the management of information security.

This policy provides the overarching approach to the management of information security and is the master policy document of the information security framework. All related policies shall be consistent with this policy.

The information security framework (comprising this policy, supporting policies, processes and tools and the requisite management and decision-making structures) shall be an enabling mechanism for information sharing and for reducing information related risk to acceptable levels though the design, implementation and maintenance of a formal Information Security Management System.

The information security framework will deliver a compliant and enabling environment that balances information security with appropriate accessibility and provides the optimum level of risk management to support achievement of the Scottish Government's strategic goals.

Contents

1. Introduction

1.1 Background

Information is one of the Scottish Government's most valuable assets and needs to be proportionately protected against loss or compromise. This policy has been written to provide a mechanism to establish procedures to protect the confidentiality, integrity and availability of our information. It does not in any way amend the requirements placed upon the Scottish Government by the Freedom of Information (Scotland) Act 2002 in relation to the disclosure of official information.

The delivery of efficient public services, including the proper protection of citizen data, requires modern and functional technology. Resilience to cyber threats, compliance with data protection laws and management of national security-related information within these systems will require security to be integral to their design and implementation.

The purpose of this policy is to protect the Scottish Government's information assets from all threats, whether internal or external, deliberate or accidental. This policy covers IT security and encompasses all forms of digital information such as data stored on computers and transmitted across networks (including websites and social media). The policy does not seek to prohibit the appropriate sharing of official information with third party agencies, public bodies and other stakeholders.

1.2 Policy Objectives

This policy is broadly aligned with The Minimum Cyber Security Standard that was developed in collaboration by the UK government and National Cyber Security Centre (NCSC) and introduced in June 2018 to support the HMG Security Policy Framework (SPF).

The objectives of this policy are to establish and maintain the security, confidentiality, integrity and availability of information, information systems, applications and networks owned or held by the Scottish Government by:

- ensuring that all members of staff are aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other Information Governance policies.
- ensuring that all line managers are directly responsible for implementing the policy within their business area and for adherence to the policy by their staff and any third parties undertaking work on behalf of that business area.
- ensuring the responsibility of every staff member to adhere to the policy. Failure to comply with defined policy and procedures may be treated as a disciplinary offence under the principal terms and conditions covered within the Scottish Government Staff Handbook.

2. Scope

The Policy sets out the framework within which the Scottish Government will develop, implement, manage and review its IT security.

The Policy applies throughout the Scottish Government and its core agencies and includes:

- its IT systems;
- its employees, including temporary staff and third parties engaged on Scottish Government business and using Scottish Government IT Systems;
- its information assets.

whether or not they are located within Scottish Government premises.

This document details the scope and objectives of the Policy and sets out which persons and groups within the Scottish Government have responsibility for ensuring achievement of these objectives.

All employees must ensure that IT security issues and organisation are dealt with in accordance with the Policy and with the security requirements specified elsewhere in this document, the Scottish Government IT Security Policy.

A copy of the Scottish Government IT Security Policy shall be published on the Scottish Government Corporate Intranet and shall be readily available to all its employees, including temporary staff and third parties employed by the Scottish Government.

3. Identify

3.1 Governance processes

Objective

The Scottish Government shall put in place appropriate cyber security governance processes to identify and manage the significant risks to sensitive information and key operational services.

Controls

3.1.1 Management commitment to information security.

Management shall actively support security within the organisation through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

3.1.2 Roles and responsibilities

3.1.2.1 Accountable Officer (AO)

The AO has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. Information risks should be handled in a similar manner to other major risks such as financial, legal and reputational risks:

- lead and foster a culture that values, protects and uses information for the public good.
- discuss information risk in the delivery chain regularly with the board.
- cover information risk explicitly in the statement on internal control.
- the AO for the Scottish Government is the Permanent Secretary.

3.1.2.2 Senior Information Risk Owner (SIRO)

The SIRO is responsible for information risk within the Scottish Government and advises on the effectiveness of information risk management across the Organisation.

Ensuring that all staff, permanent, temporary and contractor, are aware of the information security policies, procedures and user obligations applicable to their area of work:

- lead and foster a culture that values, protects and uses information for the public good.
- own the overall information risk policy and risk assessment process, test its outcome, and ensure it is used.
- advise the accountable officer on the information risk aspects of his statement on internal control.
- the SIRO for the Scottish Government is Director General Organisational Development and Operations

3.1.2.3 Information Asset Owners (IAO)

IAOs are senior individuals who understand what information is held, what is added and removed, how information is moved, and who has access and why.

They understand and address risks to the information, ensure that information is fully used within the law for the public good, and provide written input to the senior information risk owner annually on the security and use of their asset:

- lead and foster a culture that values, protects and uses information for the public good.
- knows what information the asset holds, and what enters and leaves it and why.
- knows who has access and why, and ensures their use of it is monitored.
- understands and addresses risks to the asset, and provides assurance to the SIRO.
- ensures the asset is fully used for the public good, including responding to requests for access from others.

3.1.2.4 All staff

All staff are responsible for information security and therefore must understand and comply with this policy and associated guidance.

Security mandatory training must be completed by all staff and shall also be encouraged to complete any recommended security learning.

The Scottish Government shall understand and manage security issues that arise because of dependencies on external suppliers or through their supply chain.

3.1.3 Risk management

The Scottish Government shall:

- identify and manage the significant risks to information and operational services,
- recognise that there are risks associated with users accessing and handling information in order to conduct official Government business.
- understand that Information that is collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption.

3.1.4 Protection of information

The implementation of controls to protect information must be based on an assessment of the risk posed to the Scottish Government, and must balance the likelihood of negative business impact against the resources required to implement the controls, and any unintended negative implications of the controls.

3.2 Information asset register

Objective

The Scottish Government shall identify and catalogue sensitive information they hold.

Controls

3.2.1 Information recording

Shall know and record:

- What information they hold or process.
- Why they hold or process that information.
- Where the information is held.
- Which computer systems or services process information.
- The impact of its loss, compromise or disclosure.

3.2.2 Government classification system

Information must be classified and protected using the standard Government protective markings together with appropriate access control measures.

The Government Classification System (GCS) specifies three level of classification that should be used when classifying information assets:

- Official
- Secret
- Top Secret

It is the responsibility of all those who work in the Scottish Government to protect information assets in line with the GCS, including by classifying data to ensure it receives the appropriate protection.

3.2.3 Information communication

All Scottish Government information needs to be appropriately communicated to ensure that information is correctly handled in order to protect it from unauthorised disclosure, unauthorised access, theft, loss or premature destruction, whether internal or external, deliberate or accidental, and to deter deliberate compromise or opportunist attack.

The dissemination of information and assets should be no wider than is necessary for the efficient conduct of the organisation's business and, by implication, should be limited to those individuals who are appropriately authorised to have access to it.

3.2.4 Information responsibility

Everyone who uses information assets has a responsibility to handle them appropriately and in accordance with their classification. Scottish Government information assets should be made available to all who have a legitimate need for them and the integrity of information assets must be maintained at all times.

Classified and Sensitive information at the end period of retention or when no longer required for the business requirements must be disposed or destroyed in line with the Scottish Government standard procedures.

It is the responsibility of all Information Asset Owners to ensure that the correct labelling is applied to the information for which they are responsible.

Information, media and outputs must be labelled with their classification during the creation or printing process, or as soon after as possible.

Whether or not protectively marked, appropriate security measures shall be in place and it is the responsibility of all Employees to be aware of these requirements and manage information in an appropriate manner.

3.3 Operational services

Objective

The Scottish Government shall identify and catalogue the key operational services they provide.

Controls

3.3.1 Recording of services

Shall know and record:

- What their key operational services are.
- What technologies and services their operational services rely on to remain available and secure.
- What other dependencies the operational services have (power, cooling, data, people etc.)
- The impact of loss of availability of the service.

4. Protect

4.1 Authentication and authorisation

Objective

Access to information and operational services shall only be provided to identified, authenticated and authorised users or systems.

Protecting access to IT systems and applications is critical to maintain the integrity of the Scottish Government systems and data and prevent unauthorised access to such resources.

Controls

4.1.1 Physical And logical access controls

The Scottish Government shall implement physical and logical access controls across its networks, IT systems and services in order to provide authorised, auditable and appropriate user access, and to ensure appropriate preservation of data confidentiality, integrity and availability.

4.1.2 Identification

Users and systems shall always be identified and authenticated prior to being provided access to information or services. Depending on the sensitivity of the information or criticality of the service, the device being used for access may also need authorisation and authentication.

4.1.3 Multi-factor authentication

Multi-factor authentication shall be used where necessary and technically possible, such as where administrative consoles provide access to manage cloud based infrastructure, platforms or services. Multi-factor authentication shall be used for access to enterprise level social media accounts.

4.1.4 Password policy

The Scottish Government password policy requires users to select secure passwords. Users shall be required to follow good security practices in the selection and use of passwords.

Technical controls will be used to enforce password policy where possible.

The allocation of passwords shall be controlled through a formal management process.

4.1.5 Access management

The need for users to access information or operational services shall be understood and continually managed.

Users shall be given the minimum access to information or operational services necessary for their role.

Access shall be removed when individuals leave their role or the organisation. Line managers are responsible for ensuring that this is carried out. Periodic reviews should also take place to ensure appropriate access is maintained.

4.2 Privileged account management

Objective

Highly privileged accounts should not be vulnerable to common cyberattacks.

Controls

4.2.1 Privilege account allocation

The allocation of privilege service account logon passwords must be controlled by a formal management process.

Users with wide ranging or extensive system privileges shall not use their highly privileged accounts for high-risk functions, in particular reading email and web browsing.

4.3 Vulnerability management

Objective

Systems which handle information or provide operational services shall be protected from exploitation of known vulnerabilities.

Controls

4.3.1 Change control management

All Scottish Government owned and managed equipment must have formal change control procedures, with comprehensive audit trails used for all changes or upgrades to business software.

All changes to operating systems and ancillary software must be properly authorised, and must be tested appropriately before changes are moved to the live environment to ensure there is no adverse impact on Scottish Government operations or security.

4.4 Anti-Malware detection

Objective

Implement and support an anti-malware solution to prevent, detect and remove malicious software on IT systems, as well as individual computing devices.

Controls

4.4.1 End User Device

Installed on endpoint devices to monitor the security and ensure that they are protected against viruses and malware, and where discovered prevent them from running by quarantining them.

4.4.2 Web Browsing

Protect Scottish Government data and systems from breaches of privacy and the introduction of malware by applying security controls to web browsers.

4.4.3 Email

Apply anti-spam and anti-virus email filtering solutions to reduce the Scottish Government's exposure to threats such as phishing, malware and ransomware.

4.5 Software management

Objective

All software, including operating systems and applications must be actively managed.

Controls

There must be an identifiable individual and deputy, or organisational unit, taking current responsibility for every item of software formally deployed.

Software not in use, unauthorised or installed without permission will be removed.

The procurement or implementation of new, or upgraded, software must be carefully planned and managed. Information security risks associated with such projects must be mitigated using a combination of procedural and technical controls.

Business requirements for new software or enhancement of existing software shall specify the requirements for information security controls.

Ensure the appliance of secure configuration and patching, but where this is not possible, then other mitigations (such as logical separation)

Ensure operating systems and software packages are patched regularly, and as a minimum in vendor support.

4.5.1 Software installation

No software product or application, shall be mounted or made available for which a prior licence has not been procured or properly acquired or renewed.

Only approved software applications are allowed to access Scottish Government networks and information resources.

Staff shall not use programs that are not on the approved list of software applications. Any exceptions will be based on special use cases with appropriate justification and approval.

Staff members who introduce a security issue by installing and running an unapproved program risk disciplinary action.

4.5.2 Software development

Software applications shall be developed based on industry best practices and shall incorporate information security throughout the software development lifecycle.

Custom-built software and web code shall conform to Scottish Government policies. If required, security features built into the software shall be developed in compliance with policy.

The Scottish Government will maintain Development and/or test environments separate from the Production environment of its primary enterprise systems.

If there is connectivity with the Scottish Government Production environment network, access controls will be in place to enforce separation.

Modifications to vendor supplied software shall be avoided as far as possible, and only strictly controlled. Essential changes shall be permitted, after agreement with the vendor, and the development of interfacing software shall only be undertaken in a planned and controlled manner.

Upgrades or other changes to locally developed software must be assessed to mitigate any potential risk to information security.

4.5.3 Software acquisition and maintenance

All Scottish Government's software acquisitions, development, installations and disposals are maintained to ensure that they provide an adequate level of security protection and

- must not adversely affect the security of the existing infrastructure
- must comply with current legal and regulatory requirements.

4.6 Remote and home working

Objective

It is Scottish Government policy to provide secure and resilient remote access to the Scottish Government's information systems, to preserve the integrity, availability and confidentiality of the Scottish Government's information and information systems and mitigate against the risks.

Controls

4.6.1 Information security risks

The Scottish Government recognises the business benefits brought by working from outside of the office and the greater flexibility this provides to employees. It also recognises the new risks and vulnerabilities that are exposed by mobile and remote working.

Information security risks will need to be considered carefully to help staff manage the varied workloads when working off site:

- Increased risk of equipment damage, loss or theft
- Accidental or deliberate overlooking and overhearing by unauthorised individuals
- Unauthorised access to sensitive information
- Introduction of malicious software and viruses
- Potential sanctions against the Scottish Government or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse
- Potential legal action against the Scottish Government or individuals as a result of information loss or misuse
- Scottish Government reputational damage as a result of information loss or misuse.

4.7 Web browsing

Objective

It is Scottish Government policy to provide Internet access for authorised users and services on the SCOTS network.

Controls

4.7.1 Monitoring of communications

The current policy extends to allow personal use of the service. Conditions and acceptable use are generally outlined within the IT Code of Conduct published on Saltire

It is the policy of the Scottish Government that all electronic communications across the SCOTS network is monitored for all lawful purposes including:

- to ensure that their use is authorised;
- for management of the system;
- to facilitate protection against unauthorised access;
- to verify security procedures, survivability and operational security.

The Scottish Government reserves the right to examine the content of any electronic communication transmitted via its networks.

Anyone found to be abusing their privileges or engaging in unlawful or unacceptable use of the Scottish Government's computer facilities will be dealt with under Scottish Government's disciplinary procedures.

4.8 Physical security

Objective

It is Scottish Government policy to prevent unauthorised access to systems, data and information and to reduce exposure to risk, whilst maintaining effective operations and connectivity.

Controls

4.8.1 Clear desk and clear screen

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

Removable media must be locked away and not left unattended attached to ports.

4.8.2 Unattended user equipment

Users shall ensure that unattended equipment has appropriate protection.

4.9 Equipment security

Objective

To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

Controls

4.9.1 Equipment siting and protection

Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

4.9.2 Security of equipment off premises

Security shall be applied to off-site equipment taking into account the different risks of working outside the organisation's premises.

4.10 IT Outsourcing

Objective

The Scottish Government shall implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

Controls

4.10.1 Security responsibilities

Where services are outsourced, the Scottish Government shall understand and accurately record which security related responsibilities remain with the Scottish Government and which are the supplier's responsibility.

4.10.2 Service delivery

It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

4.10.3 Monitoring and review of third party services

The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.

4.10.4 Managing changes to third party services

Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

4.10.5 Cloud computing

The Scottish Government shall consider and fully evaluate potential cloud solutions first before considering any other option.

The Scottish Government shall ensure that security requirements are satisfied and maintained when a particular environment or service is delivered by an outsource provider, and that all relevant individuals are aware of the security requirements regarding the purchase and use of cloud services.

5. Detect

5.1 Protective monitoring and event detection

Objective

Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.

Controls

5.1.1 Event monitoring

The Scottish Government IT security systems monitor and log events that shall capture events that could be combined with common threat intelligence sources to detect known threats.

The Scottish Government shall have a clear definition of what must be protected and why.

Attackers attempting to use common cyber-attack techniques should not be able to gain access to data or any control of technology services without being detected.

Any monitoring solution should evolve with the Scottish Government's business and technology changes, as well as changes in threat.

Monitoring systems are responsible for controlling and logging the technology and communications used by the Scottish Government in order to analyse their operation and performance, to detect and prevent unauthorised access, and effectively respond to attacks.

Monitoring allows the Scottish Government to ensure that systems are being used appropriately in accordance with organisational policies.

Information placed on, or sent over Scottish Government networks may be examined, recorded and used by automated systems and ICT staff for all lawful purposes.

6. Respond

6.1 Incident management

Objective

The Scottish Government shall have a defined, planned and tested response to cyber security incidents that impact information or operational services and shall apply a consistent and effective approach to the management of information security incidents.

Controls

6.1.1 Incident Response and Communication

The Scottish Government shall develop an incident response and management plan, with clearly defined actions, roles and responsibilities. It should be tested at regular intervals. Post testing findings should inform the immediate future technical protection of the system or service, to ensure identified issues cannot arise in the same way again. Systemic vulnerabilities identified shall be remediated.

The Scottish Government shall have communication plans in the event of an incident which includes notifying the relevant bodies.

The Scottish Government shall effectively handle Information Security incidents in a manner that minimises the adverse impact to the Scottish Government and the risk of data loss. This applies to all of the Scottish Government's information and to all methods of accessing that information.

In the event of an incident that involves a personal data breach, the Scottish Government shall comply with any legal obligation to report the breach to the Information Commissioner's Office without undue delay.

In the event of an incident, mitigating measures shall be applied at the earliest opportunity. Access to any device, system or data shall be required by an authorised administrator in order to isolate and contain any damage, identify and investigate the cause, and to assess and recover from the event.

6.1.2 Security Reporting

It is Scottish Government policy to report all actual or suspected information security incidents immediately upon discovery.

It is Scottish Government policy to report any observed or suspected security weaknesses in systems or services.

The responsibility for reporting incidents and weaknesses lies with all staff and visitors. That is any person who has access to Scottish Government IT Facilities, Scottish Government information and information systems.

Cyber security incidents affecting SCOTS and other Scottish Government owned IT systems can be reported by emailing cyber security and defence. This mailbox is monitored Monday to Friday during office hours.

Out with normal working hours, cyber security incidents affecting SCOTS and other Scottish Government owned IT systems should be reported to the Victoria Quay security control room on 0131 244 5203.

6.1.3 Learning from Information Security Incidents

The Scottish Government shall put in place mechanisms to evaluate and monitor information security incidents, including lessons learned.

A copy of all incidents and weaknesses shall be recorded.

7. Recover

7.1 Disaster recovery and Business continuity

Objective

The Scottish Government shall have well defined and tested processes in place to ensure the continuity of key operational services in the event of failure or compromise.

Controls

7.1.1 Contingency Procedures

The Scottish Government shall identify and test contingency procedures to continue to deliver essential services in the event of any failure, forced shutdown, or compromise of any system or service, and shall:

- maintain a strategy for reacting to, and recovering from, adverse situations which is in line with an agreed level of acceptable risk
- ensure that, whenever practical, action is taken to prevent the occurrence or recurrence of an adverse situation through adopting appropriate risk controls
- maintain a programme of activity which ensures the Scottish Government has the ability to react appropriately to, and recover from, adverse situations in line with predefined business continuity objectives
- maintain appropriate response plans underpinned by a clear escalation process
- rehearse response and recovery plans at least annually. Restoring the service to normal operation should be a well-practised scenario
- maintain a level of resilience to operational failure in line with the risks faced
- maintain employee awareness of the Scottish Government's expectations of them during an emergency or business continuity threatening situation
- take account of changing business needs and ensure that the response plans and business continuity strategies are revised where necessary
- remain aligned with good industry practice in business continuity management.

The Scottish Government shall review all incidents for lessons learned and to identify improvements in policies and procedures.

8. Policy review

The Scottish Government IT Security Policy is reviewed:

a. every six months following its first approval.
b. where there are any proposals for significant organisational, supported service or customer base change.

9. Document control

Status	Published
Version	1.0
Classification	Official
Release Date	9th March 2020
Owner	Cyber Security Unit
Review	9th September 2023