Scottish Enterprise

SCOTTISH ENTERPRISE

INFORMATION SECURITY POLICY

VERSION 7

1 Introduction / Purpose

This document is the agreed information security policy for Scottish Enterprise.

This policy is:

- Owned by the Business Security Forum on behalf of the SE Chief Executive.

The Information Security Policy for Scottish Enterprise

Note	Policy Clause
What the policy is – its organisational coverage.	1. Information and information systems are fundamental to Scottish Enterprise in its role as Scotland's main economic development agency supporting business growth and developing the business environment. This Information Security Policy statement lays down the objectives, motivation and direction for Scottish Enterprise to protect its business information, systems and networks. It includes all information and data handled, information systems, and networks operated by, and for, Scottish Enterprise. This covers the organisation of Scottish Enterprise, and includes outlying and international offices.
Alignment with security standards.	2. We have adopted the security framework of the International Standard ISO/IEC 27001:2013. In keeping with the Standard, we define information security as protecting the confidentiality, integrity and availability of information. • confidentiality: ensuring that information is accessible only to those authorised to have access; • integrity: safeguarding the accuracy and completeness of information and processing methods; and • availability: ensuring that authorised users have access to information and associated assets when required. Additionally, we will comply with Government policies and standards where they are applicable to Scottish Enterprise as a Scottish non-departmental public body.
Authority	3. This corporate Information Security Policy has the authority of the Executive Leadership Team of Scottish Enterprise. Substantive change must have Executive Leadership Team approval.
Balancing democratic and commercial security requirements.	4. As a non-departmental public body, reporting to the Scottish Government, we are aware of, and take responsibility for the prudent custody of our business information. While we operate transparently and report publicly on our plans and activities, it is often commercially necessary for us to act in confidence to assure the success of enterprise development activity for the benefit of the Scottish economy.
Compliance with legal requirements - Data Protection Act, Freedom of Information Act etc.	5. In our activities, we also process and store Personal Data as defined by General Data Protection Regulations (GDPR) and the Data Protection Act. We conform to all legal and regulatory requirements relating to our collection and use of personal information in conducting our business and support the use of the privacy impact assessment as recommended by the Information Commissioner. We comply with the Freedom of Information (Scotland) Act 2002 which provides a right of access to information held by Scottish public authorities. Our information security policies and procedures are consistent with this Act, including the general commitment to openness and the exemptions which allow information to be withheld when release would cause harm to legitimate interests. We comply with the Regulations on the re-use of Public Sector Information which came into force on 1 July 2005.

The principal tenets of Information Security.	6. The Information Security policy of Scottish Enterprise is based on the “four As”: • **Assurance** – our security practices will always be demonstrably prudent practice, in keeping with the threats faced by our sphere of activity and by our customers. Scottish Enterprise accepts our responsibility to protect our customers’ systems and information in the interests of each customer. • **Authority** – use of information technology and the management of our systems, and customer information in our care, will always be based on employees and agents of Scottish Enterprise being explicitly authorised to act by the management of Scottish Enterprise. • **Accountability** –employees and agents of Scottish Enterprise can be held accountable for all actions affecting Scottish Enterprise data handling, IT platforms, services and information. • **Availability** – availability of systems, services and information is assured by physical security measures, resilient architectures and by business continuity planning.
Types and scope of information.	7. The information processed by Scottish Enterprise, and in the scope of this policy includes: • Operational information and data for the efficient running of the organisation; • Information and data pertaining to customers of Scottish Enterprise, both business entities and individuals; • Publications and reports which Scottish Enterprise makes available to the public at large, or to closed communities of interest; • Information and data pertaining to business partners and correspondents of Scottish Enterprise. • Information and data entrusted to Scottish Enterprise by other public sector organisations. • Information and data pertaining to employees and ex-employees
The security commitment.	8. Our commitment to the security of Information is as follows: • We take all reasonable precautions to protect our information and infrastructure systems from downtime, corruption or infiltration; • We take all reasonable steps to protect information we hold on our customers, from downtime, corruption or unauthorised disclosure. • We take all reasonable steps to protect our public facing business systems to assure the continuity and accuracy of our public services. • We adhere to all legal and regulatory requirements in relation to operating our business and providing services for our customers. • We adhere to consistent ethical practice as indicated by Government and European Commission guidance for Information Processing and Data Handling.
Risk management principles.	9. The security countermeasures taken by Scottish Enterprise are based on risk management principles – i.e. the security measures are in keeping with the damage that could be caused to Scottish Enterprise, its customers or business partners by a security breach. Where decisions are made by employees or agents of Scottish Enterprise regarding the interpretation of security policy and the selection and operation of security controls, the measures adopted are chosen as a result of risk analysis and / or information classification.

Individual responsibility and accountability – security Awareness.	10. All employees and agents of Scottish Enterprise are expected to act responsibly in accordance with this policy and its associated standards and procedures. They are required to act only within their defined authority with respect to information technology and data handling. There are supervisory procedures to help assure good practice. Disciplinary and/or legal procedures will be invoked for any deliberate or negligent breaches of the policy. Scottish Enterprise will conduct security awareness campaigns across the organisation to ensure everyone is reminded of their responsibility.
The Security Management Infrastructure	11. Scottish Enterprise has an established information security management infrastructure, which includes designated information security management roles. There are standards and procedure documents published internally which indicate specific practices, which must be complied with in adherence to this policy.
Technical procedures – whoever is custodian of systems.	12. The Scottish Enterprise technical security procedures include specific security instructions for the development, operations and deployment of information technology, whether systems and networks are developed, operated and deployed by Scottish Enterprise itself or by a third-party under contract to Scottish Enterprise.
Customer contracts	13. When Scottish Enterprise enters into a contract with an external organisation, the protection of both parties business information will be a mandatory clause in the governing business agreement.