Registers of Scotland

Department	Security and Information Assurance (SIA)
Topic	Information Security Policy
Number	SIA05
Date	11 July 2016

Table of Contents

1 Introduction

Information is one of RoS's most valuable business assets and needs to be adequately protected against loss or compromise. We are heavily dependent on using information in whatever form and wherever it exists. This policy has been written to provide a mechanism to establish procedures against **unauthorised** disclosure of information. It does not in any way amend the requirements placed upon us by the Freedom of Information (Scotland) Act 2002 in relation to disclosure of official information or the Data Protection Act 1998 in relation to personal information.

The purpose of this policy is to protect our information assets from all threats, whether internal or external, deliberate or accidental. This policy covers physical and IT security and encompasses all forms of information such as data stored on computers, transmitted across networks (including websites and social media), printed out or written on paper, sent by fax, stored on removable media such as DVDs and memory sticks, or spoken in conversation and over the telephone. The policy does not seek to prohibit the appropriate and authorised sharing of official information with third party agencies, public bodies and other stakeholders.

The purpose of information security is to protect information (in all forms) from a wide range of threats in order to ensure business continuity, minimise risk of disruption to business and maximise return on investment.

There are three basic components of information security:

Confidentiality	Ensuring that information is accessible only to those authorised to have access.
Integrity	Safeguarding the accuracy and completeness of information and processing methods
Availability	Ensuring that authorised users have access to information and associated assets when required.

This Information Security Policy is only part of a range of controls required for an effective Information Security Management System (ISMS). This policy takes cognisance of and uses the ISO/IEC 27002:2013 Information Technology Security Techniques – Code of practice for information security controls as a framework for guiding our approach to managing information security.

We hold two distinct types of information;

- Information held electronically and in other formats created, originated and stored by us in our business capacity. Crown copyright applies to many of these information assets.
- Deeds and other documents belonging to other parties which are submitted to us.

2. Scope

This policy applies to all our information processing facilities and information stored and processed by us.

This policy applies to all RoS employees and third parties including contractors, temporary staff, delivery partners and third party IT suppliers who have access to our premises, equipment and information.

3. Roles & Responsibilities

3.1 Senior Management

Overall operational responsibility lies with the accountable officer who within RoS is also the Senior Information Risk Owner (SIRO). The duty of care for overall security (including information security) is delegated to the Departmental Security Officer (DSO). The Executive Management Team (EMT) are responsible for approving information security policy and major initiatives to enhance information security. The EMT also monitor significant changes in the exposure of information assets to major threats.

3.2 Information Asset Owners

Although the duty of care for overall security at RoS lies with the SIRO and DSO in practice the day to day information, IT, physical and personnel security management is devolved to other postholders.

Information Asset Owners (IAOs) are assigned for all major information assets and will typically be EMT members. IAOs may delegate their authority (power to act) to individual managers or Area Information Managers (AIMs). However they remain ultimately accountable for protecting the security of their information assets and should be able to determine that any delegated responsibility has been discharged correctly. The IAO is responsible for ensuring that the responsibilities are documented for each site, system and service.

3.3 Team Leaders / Managers

Team leaders / 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.

3.4 Employees

Security roles and responsibilities will be defined in job descriptions, role profiles, and individual performance objectives, as appropriate. Definitions will include general responsibilities for implementing or maintaining security policy, and specific responsibilities for the protection of particular assets, or the execution of particular processes or activities.

It is the responsibility of all RoS employees to comply with this policy and any local information security standards and procedures. These can all be found on the RoS intranet;

http://ros-intranet/

4 Information

4.1 Information Classification

To ensure that all information assets receive an appropriate level of protection, security classifications must be used where appropriate to indicate the need and priorities for security protection.

Security classifications and associated protective measures must be based on the business need for sharing or restricting access to the information, and the potential business impact associated with unauthorised access or damage to the information. The business need for confidentiality, integrity and availability of the information will drive the classification.

RoS applies the Government Security Classification system which consists of;

Top Secret

Secret

Official

The definition of the classifications and their descriptions is narrated in our Security Classification guidance.

http://ros-intranet/policiesandprocedures/sia/security_classification_policy.html

IAOs are accountable for;

- Defining the classification of each asset.
- Periodically reviewing the classification for continued appropriateness.

4.2 Information Dissemination

Information held by us may require to be disclosed as a result of a request under the Freedom of Information (Scotland) Act 2002 or, where it is personal information of the requestor, the Data Protection Act 1998. Information may also require to be disclosed under other legislation such as tax enactments.

It is unlawful to disclose some categories of information held by us such as personal information except as permitted by the Data Protection Act 1998, or protected taxpayer information for the purposes of the Revenue Scotland and Tax Powers Act 2014.

We may decide to disclose information for many otherwise lawful purposes including the delivery of commercial products or services, contract management, and criminal investigations.

In all cases it is the responsibility of the manager or team leader for the business area disclosing the information to be satisfied that information is disclosed only where it is lawful and appropriate to do so.

It follows that legal advice must be obtained before any new category of information is disclosed or an existing category of information is disclosed in a new way or if for any other reason you are in doubt about whether information should or should not be disclosed. It also follows that the disclosure must comply with any current RoS policy, or where there is no policy that it must be agreed in advance as appropriate by any or all appropriate governance group / a senior manager / the SIRO.

http://ros-intranet/policiesandprocedures/secretariat/foi_policy.html

5. New IT Facilities

The management approval for new information processing facilities must confirm that new equipment and software has appropriate levels of security protection and will not adversely affect the security of the existing infrastructure.

RoS IT Change Management Policy mandates that the security risks are considered before any IT change is authorised.

6. Policy and Reviews

6.1 Policy Review

The DSO has direct responsibility for maintaining the policy, providing advice and guidance on its implementation. This policy will be reviewed on an annual basis by the Information Assurance Group (IAG) or at any time in response to a significant technological change or security threat.

6.2 Supported Topic Specific Policies

We will produce and publish on the intranet specific policies relating to security topics that are referred to or only covered at a high level in this policy as appropriate.

6.3 Independent Review of Information Security

The practice of information security is reviewed periodically by independent internal auditors to provide assurance that our practices properly reflect our information security policies and guidance.

http://ros-intranet/policiesandprocedures/sia.html

7. Non Compliance

It is 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 and subject to action (including dismissal) under our disciplinary procedures. We will implement sanctions against staff whose acts cause or attempt to cause the compromise of information assets.

8. Advice

For further advice on this policy please contact the Security and Information Assurance team. Contact details can be found on the intranet and / or business directory.