Forestry Commission

Agenda Item 7 | Executive Board Meeting 3 December 2014 | Memo No 20/14

STATUS – OFFICIAL

INFORMATION SECURITY MANAGEMENT FORUM

Purpose

1. To inform the Board of an update to the terms of reference of the Information Security Management Forum (ISMF) and to allow an opportunity to review the updated Information Security Policy.

Background

2. The ISMF is responsible to the Executive Board for co-ordinating and controlling the implementation of information security. Each part of the FC has a Senior Information Risk Owner (SIRO) responsible to the Accounting Officers for implementation of information security in their respective business areas with the assistance/support of the Departmental Security Officer/IT Security Officer.

Terms of Reference

3. The ISMF will meet three times per annum and is responsible for:

- Ensuring that the Forestry Commission has effective policies and management arrangements covering all aspects of information handling in line with the Commission's overarching Security Policy;
- Ensuring that the Forestry Commission's approach to information handling is communicated to all staff and made available where appropriate to the public;
- Co-ordinating Forestry Commission information security activities including the specific security requirements arising from data protection, confidentiality, information quality, records management and freedom of information;
- Ensuring that appropriate training is made available and taken up by staff as necessary to support their role;
- Monitoring the Forestry Commission's information handling activities to ensure compliance with the law and guidance;
- Reviewing major incidents - and any other events that have serious security implications - and the proposed measures to prevent recurrence;
- Assisting SIROs in their reports to their respective Audit and Risk Committees;
- Assisting SIROs in their annual assessment of information risk and written advice to their respective Accounting/Accountable Officer;

- Providing an Annual Report to the Executive Board. This will constitute the GB SIRO's Annual Report to the GB Accounting Officer.

Information Security Policy

4. The updated Information Security Policy is attached at Appendix 1, for information.

Membership

5. Director Corporate and Forestry Support, as SIRO for the FC as a whole (and for Central Services (except FR)), chairs the ISMF. The other members are:

- Head of Executive Office England (England SIRO)
- Head of Finance Scotland (Scotland SIRO)
- Head of Operations Forest Research (FR SIRO)
- IT Security Officer (ITSO) and the Departmental Security Officer (DSO) (Secretary).

6. The Head of Internal Audit or deputy also attends and the Data Protection Officer is also invited to attend as necessary.

Impact on Resources and Risks

7. None.

Communications

8. ISMF will be contacted when the new terms of reference have been agreed by the EB. The updated terms of reference and policy will be published on the Intranet.

Recommendation

9. The Board is asked to approve the updated terms of reference and policy document.

Wilma Harper
Head of Corporate and Forestry Support
November 2014

Appendix 1

Information Security Policy

Table of Contents

Introduction

1. This document defines the Information Security Policy for the Forestry Commission (FC). Information and information systems are critical and vitally important assets. Without reliable information assets, the Commission would be severely disadvantaged. Therefore this policy states the requirements that all employees; contractors and management **MUST** comply with in order to secure our information, whether it is held electronically or on paper.

2. This document:

   - Establishes the overall responsibilities for information security;
   - Sets out the Commission's policy for the protection of its information assets;
   - Provides reference to the Information Security Management System (ISMS) documentation.

Purpose

3. The purpose of the Policy is to protect the FC's information assets from all threats, whether internal or external, deliberate or accidental, based on a risk assessment approach.

Scope

4. This policy applies to all FC employees; contractors, volunteers, work placement students and any other category of employee that has access to the FC's information.

5. The ISMS applies to all business functions and covers the information, information systems, networks, physical environment and people who support those business functions. This policy covers all Security Policies and Procedures.

Requirements

6. It is Commission policy that information is:

   - Available as and when required to conduct the Commission's business;
   - Protected from unauthorised or accidental modification thus ensuring the accuracy and completeness of the Commission's information;
   - Protected against unauthorised disclosure.

7. To fulfil these requirements the FC will:

   - Protect information based on an assessment of the risks;
   - Meet regulatory and legislative requirements;

- Ensure that its key business systems are compliant with central Government guidance and appropriate standards including the Security Policy Framework;
- Request a statement of compliance against the relevant Security Policy Framework requirements as part of its Invitation To Tender. Successful suppliers must provide evidence of an acceptable level of compliance and, if necessary, agree a Security Plan in the Security Schedule of the contract;
- Produce, test and maintain Business Continuity Plans;
- Train members of staff to the levels required for their responsibilities;
- Create procedures to support the policy;
- Treat breaches or attempted breaches of this policy as a disciplinary matter.

Overall Responsibilities

8. This policy is endorsed by the Information Security Management Forum (ISMF) on behalf of the Executive Board and is promulgated, monitored and periodically reviewed for them by the Departmental Security Officer (DSO).

9. The ISMF is responsible to the FC Executive Board for co-ordinating and controlling the implementation of information security. Each part of the FC has a Senior Information Risk Owner (SIRO) responsible to the Accounting Officers for implementation of information security in their respective business areas with the assistance/support of the DSO/ITSO.

10. The ISMF is responsible for:

- Ensuring that the Forestry Commission has effective policies and management arrangements covering all aspects of information handling in line with the Commission's overarching Security Policy;
- Ensuring that the Forestry Commission's approach to information handling is communicated to all staff and made available where appropriate to the public;
- Co-ordinating Forestry Commission information security activities including the specific security requirements arising from data protection, confidentiality, information quality, records management and freedom of information;
- Ensuring that appropriate training is made available and taken up by staff as necessary to support their role;
- Monitoring the Forestry Commission's information handling activities to ensure compliance with the law and guidance;
- Reviewing major incidents - and any other events that have serious security implications - and the proposed measures to prevent recurrence;
- Assisting SIROs in their reports to their respective Audit and Risk Committees;
- Assisting SIROs in their annual assessment of information risk and written advice to their respective Accounting/Accountable Officer;
- Providing an Annual Report to the Executive Board. This will constitute the GB SIRO's Annual Report to the Accounting Officers.

11. Accounting Officers are responsible for:

- Leading and fostering a culture that values, protects and uses information for the public good;
- Discussing information risk in the delivery chain regularly with their board;
- Covering information risk explicitly in the statement on internal control.

12. Senior Information Risk Owners (SIRO) are responsible for:

- Leading and fostering a culture that values, protects and uses information for the public good;
- Owning the overall information risk policy and risk assessment process, testing its outcome and ensuring that it is used;
- Advising the Accounting Officers on the information risk aspects of their statements on internal control.

13. Information Asset Owners are responsible for:

- Leading and fostering a culture that values, protects and uses information for the public good;
- Knowing what information the asset holds, what enters and leaves it and why;
- Knowing who has access to the asset and why and that their access is monitored;
- Understanding and addressing risks to the asset, and providing assurance to the SIRO;
- Ensuring that the asset is fully used for the public good, including responding to requests for access from others.

14. The DSO is responsible for:

- Acting as a central point of contact on information security within the Commission, for both staff and external departments;
- Implementing an effective framework for the management of security;
- Advising on the content and implementation of an Information Security Programme;
- Producing departmental standards, procedures and guidance on information security matters for approval by the Information Security Management Forum;
- Co-ordinating information security activities throughout the Commission;
- Liaising with external organisations on information security matters, including representing the Commission on cross-community committees e.g. Departmental Security Officers' Forum.

15. The IT Security Officer is responsible for:

- Reporting to the Information Security Management Forum on matters relating to IT security as required.;
- Creating, maintaining, giving guidance on and overseeing the implementation of IT Security;
- Representing the Commission on external committees that relate to IT security, e.g. IT Security Officers' Forum;
- Ensuring that risks to information systems are reduced to an acceptable level by applying security countermeasures identified following a risk assessment;
- Ensuring the application and/or development of required policy standards and procedures in accordance with the ISMS;
- Ensuring that access to the Commission's information assets is limited to those who have the necessary authority, clearance and 'need-to-know.';
- Providing advice and guidance to systems development teams to ensure compliance with Commission policy;
- Approving System Security Policies for information systems;
- Advising the DSO on the accreditation of information systems;
- Providing a central point of contact on IT security issues.;
- Passing on the advice of external sources/authorities on IT security matters;
- Providing advice and guidance on the terms of this policy.

16. The Director of Information Services is responsible for the operational security of the installations.

17. Heads of Business Areas are responsible for ensuring that each information system for which they are responsible:

- incorporates a level of security commensurate with the degree of risk and the impact involved in loss, corruption or disclosure of information,
- has an up to date business continuity plan that is periodically tested;
- meets the requirements of the FC Information Assurance Policies

18. All managers are directly responsible for implementing the policy and supporting procedures within their business areas, and for adherence by their staff.

19. Each member of staff is personally responsible for ensuring that they familiarise themselves with the procedures within their own area.

Breaches

20. Breaches of this policy will be dealt with as defined in the Staff Handbook – Discipline section..

Post Holders at Nov 2014 Annex 1

Senior Information Risk Owners:–

FC GB	Wilma Harper (Lead SIRO)
FC England	PK Khaira-Creswell (Richard Barker (Nov 14 – Apr 2015))
FC Scotland	Ann Robertson
Forest Research	Hugh Williams

Information Asset Owners:-

Central Services	Wilma Harper – C&FS systems
(Full details on	Steve Atkins - FAS systems
the Intranet)	David Felstead – IS systems (including Outlook)
	Jean Lindsay – HR systems

FC England & FC Scotland:-
Costs centre managers are responsible for ensuring the IAO role is fulfilled.

Forest Research:-
Hugh Williams – all FR data.

Departmental Security Officer – Stuart fletcher
IT Security Officer – Stuart Fletcher

Document History

Reviewed By

Organisation	Person
Corporate and Forestry Support	Wilma Harper (SIRO)
Information Services	Stuart Fletcher (DSO)
ISMF	Current Forum Members
Internal Audit	Chris Watling (internal Audit)

Revision Record

Number	Date and Sections	Notes
0.1	25/8/04	Initial draft for comment
0.2	19/10/04	Second draft
0.3	09/01/06	Final form
1.0	March 2006	Publication
1.6	13 August 2009	Updated to reflect change of responsibilities
1.7	10 September 2009	Updated to reflect ISMF comments
2.0	27 October 2009	Published
3.0	16 December 2009	Updated to incorporate third party requirements
3.1	19 November 2014	Amended Terms of Reference and brought up to date