April 2020

Contents

1 Overview

Organisationsare increasing reliant on IT systems to deliver a wide range of business functions and services and typically have an extensive IT estate. This heavy reliance on IT, coupled with the ever-increasing and evolving threat landscape, places them at significant risk of major compromise from cyber-attack. IL7 processes and stores significant quantities of sensitive information, and in the event of a compromise this could have significant reputational, public safety and national security implications.

In light of this, it essential that IL7 defines and implements a robust organisational and governance structure for cyber security, and further, ensure that cyber security is seen as a strategic priority. It is essential that the structure and governance in place for cyber security is integrated and aligned with wider organisational structures and governance. This will ensure that cyber security is appropriately managed and considered across all levels of the department, with a clear escalation path up to and including the Departmental Board (including PRC, ARAC and ExCo).

1.1 Purpose

1.2 This policy sets out the requirements by which IL7 shall design and deliver a a robust Cyber Security organisation and governance chain, in order to drive the mitigations of Cyber Security Risk.

1.3 Scope

The scope of this policy covers the necessary Cyber Security organisation and governance from ExCo down through the Directorates.

1.4 Applicability

This policy applies to all IL7 staff at all levels.

2 Cyber Organisation and Governance Policy

2.1 Policy and Controls

This policy is written to ensure that the outcomes of the following Cyber Security Principles are met;

- SP01 Governance and Risk Management (Ref [1])
- SP05 Security Incident Management (Ref [2])
- SP06 Operational Security (Ref [3])
- SP08 Validation, Confidence and Assurance (Ref [4])

This policy is one of several that are required to support principles above.

This policy implements the following NIST controls, which are detailed in NIST Special Publication 800-53 [5]:

PL-1	Security Planning Policy and Procedures
PM-2	Senior Information Security Officer
PM-3	Information Security Resources
PM-5	Information System Inventory
PM-6	Information Security Measures of Performance
PM-7	Enterprise Architecture
PM-9	Risk Management Strategy
PM-10	Security Authorisation Process
PM-11	Mission/Business Process Definition
PM-14	Training, Testing and Monitoring
PM-15	Contacts with Security Groups and Associations
SI-5	Security Alerts, Advisories and Directives

3 ExCo Requirements

Exco shall ensure that:

Policy ID	Policy Requirement
1.1.1	A framework, with the relevant strategy, policy and process, is established for the management of Information and Cyber Security Risk, aligned with the Departmental Risk Policy.
1.1.2	Information and IT systems are secured throughout the organisation, and that Cyber Security is embedded as a priority in the department's business and culture.
1.1.3	A comprehensive set of cyber and information security policies is defined, implemented and maintained, consistent with HMG Policy, legal requirements, NCSC guidance and relevant internationally recognised Cyber and Information Security Standards [NIST PL-1].
1.1.4	Adequate resources are in place to meet the department's information and cyber security objectives and obligations, ensure compliance with its policies and ensure risk is managed in line with the departmental risk appetite. [NIST PM-3].
1.1.5	Business owners are accountable for the secure design and operation of business processes and supporting information systems, in accordance with departmental information and cyber security policy [NIST PM-11].
1.1.6	An accountable security assurance process is conducted prior to information systems providing live services or storing or processing sensitive information. [NIST PM-10]
1.1.7	A Chief Information Security Officer (CISO) is appointed as a single, accountable owner of information security and cyber security functions across the department and is provided with appropriate resources to discharge these functions [NIST PM-2].
1.1.8	A central management function is established and operated to support the CISO and ensure the successful implementation of the departmental information and cyber security policy [NIST PL-9].

Policy ID	Policy Requirement
1.1.9	Processes are in place to monitor and assess the effectiveness of the cyber and information security policy set and implement change where required [NIST PM-14].
1.1.10	Processes are in place to monitor and assess the effectiveness of the cyber and information security controls and implement change where required. [NIST PM-14]
1.1.11	A Risk Executive function is in place to own information and cyber security risk across the department and provide a robust risk management process, with a clear route for escalating risks to ExCo. [NIST PM-2]
1.1.12	The Risk Executive is supported by a dedicated cyber board structure to enable it to successfully discharge its responsibilities [NIST PM-2].
1.1.13	The department's cyber risk appetite is defined, documented and published across a range of risk and information categories.
1.1.14	Processes are in place to monitor the department's IT systems to detect, respond to and recover from cyber security attacks [NIST PM-14].
1.1.15	A fair, robust and impartial process is operated for reporting and managing cyber and information security violations and policy non-compliances.
1.1.16	Incidents and breaches are investigated should they occur, and the findings of the investigation are acted upon and remediated. Exercises should be carried out to ensure lessons are learned to ensure that improvements are made to IL7's Cyber Security posture.
1.1.17	The department will stay up to date with current threat intelligence and work to continuously improve its information and cyber security posture in line with this.

4 CISO Requirements

The CISO shall:

Policy ID	Policy Requirement
1.1.18	Set the enterprise-wide information and cyber security strategy, principles, policy, process, and vision.
1.1.19	Establish a Cyber Security Strategy and framework that meets IL7's Information and Cyber Security objectives and obligations.
1.1.20	Ensure compliance with security strategy, standards, and policy requirements from the UK National Cyber Security Centre and wider HMG [NIST SI-5].
1.1.21	Support the establishment of a IL7 organisational risk appetite.
1.1.22	Design, implement and operate a portfolio management function to manage and monitor the delivery of new information and cyber security capabilities to the department.
1.1.23	Develops and maintain an inventory of information assets, systems and services that are owned, managed and/or used by the department.
1.1.24	Establish a central governance, risk and assurance function that, at minimum: • Performs the security assurance of all IL7 information systems and services; • Implement the cyber risk management process and monitor the associated cyber risks and assurance status of all entries on the information systems and services register; • Monitor and assess the effectiveness of the security controls that have been implemented to address the information and cyber security risks; • Monitor and assess the effectiveness of information and cyber security activities undertaken across the department. [NIST PM-5, 6]

Policy ID	Policy Requirement
1.1.25	Develop, maintain and ensure the implementation of an enterprise security architecture, consistent with the department's risk appetite, and integrated into the wider departmental enterprise architecture. [NIST PM-7].
1.1.26	Design and enforce a 'secure by design' process such that security is driven in to all Directorates, programmes and projects at the outset and through life.
1.1.27	Establish, monitor and maintain a strong security training and awareness campaign in line with the latest Cyber Threats and Risks, that drives a deep culture of security into IL7.
1.1.28	Establish security requirements for IL7 supply chain and assess, assure and monitor suppliers for conformance.
1.1.29	Establish and maintain regular contact with selected external organisations within the cyber security community, including NCSC and the HMG security Clusters, to maintain currency with recommended security practices, techniques and technologies; share cyber security threats, vulnerabilities and incidents; and facilitate cyber security training [NIST PM-15].
1.1.30	Receive, process and act on security alerts, advisories and guidance from reputable UK and international cyber security bodies [NIST SI-5].

5 Directorate Requirements

Directorates shall ensure that:

Policy ID	Policy Requirement
1.1.31	Business processes, products, systems and services within their portfolio are demonstrably secure, protected, and resilient to cyber-attack throughout their lifecycle.
1.1.32	Business processes, products, systems and services within their portfolio are compliant with IL7 information and cyber security policy.
1.1.33	All products, systems and services are delivered and assured in line with the GRA Secure By Design Process (Ref [6]) and Cyber Assurance Policy (Ref [7]) prior to providing live services or storing or processing sensitive information and throughout the product, system or service lifecycle.
1.1.34	A directorate level risk appetite is set, communicated and regularly reviewed, aligned to the departmental risk appetite.
1.1.35	Information and cyber risk management processes are aligned to departmental risk management policy (Ref [8])
1.1.36	The information and cyber security risks associated with all products, systems and services are assessed by the CISO function throughout their lifecycle, in accordance with the departmental risk appetite.
1.1.37	Identify and empower Information Asset Owners to ensure the secure handling, storage and processing of directorate information assets.
1.1.38	Ensure that all information assets are identified and documented in line with Departmental Policy.
1.1.39	They help to lead and foster a culture that values and continually improves the information and cyber security posture.

IL7
SECURITY