System Security Policy - Lite

**Completing this form**

This form and the report carried out through the “Information Security Risk Assessment Tool” are integrating part of NSS information security management system (ISMS). The completion of this form is required when the score of the risk assessment tool is medium.

It is a data owner’s responsibility to ensure that risk to information assets is managed and this “SSP Lite” asks minimum questions to determine that baseline security controls are in place for your solution.

These are mandatory baseline requirements for protecting NHS Scotland systems and information. The information / service owner is responsible for the completion of this SSP liaising with IT SBU / other service provider for technical completion.

|  |  |
| --- | --- |
| Title | <System Name> System Security Policy (SSP) |
| Info Sec Risk Assessment Tool | <Report number> |
| Author |  |
| Creation date |  |
| Date of version |  |

* 1. **Secure Configurations for Hardware and Software**

As delivered by manufacturers and resellers, the default configurations for operating systems and applications are focused on ease of deployment and ease of use but not security. (For example: default passwords are sometimes not changed).

1.1.1 Describe how the servers and desktops have been securely configured (if unsure ask your IT team or supplier about “security hardening” or “standard builds”).

1.1.2 Describe the processes and timescales for releasing patches to the IT system. (Critical and security updates shall be applied to systems not more than 4 weeks after they have been released).

1.1.3 Has the system been penetration tested and all medium or high criticality findings been resolved? If the solution is accessible through the Internet, a penetration test must be carried out and scheduled annually. The penetration test is like annual medical check-up where the doctor runs a series of tests (some old and some new) to detect dangers that have not yet developed.

**2. 1 Data Recovery Capability**

It is important that the solution includes a process and tool to back up the data. For example, if attackers compromise the system, the backup should provide the ability to restore the data. Tests should be carried out to make sure that the backup works and recover what is required and expected.

2.1.1 Describe the data backup and disaster recovery plan. The latter is defined as a “coordinated activity to enable the recovery of the system and network due to a disruption”

2.1.2 Describe the frequency of the back-up and disaster recovers tests.

* 1. **Data Protection**

Protecting sensitive data is pivotal in order to avoid identity theft and to protect privacy. The solution should facilitate the provision of encrypting sensitive data in transfer and at rest. In addition, it should protect the data if it is transferred to external media like usb storage devices.

3.1.1 Describe the technical controls employed within the solution to protect information assets. For example encryption at rest, de-identification or data obfuscation; encryption for data transfer.

* + 1. Describe the process that ensure secure disposal of hardware and information assets? For example to prevent unauthorised recovery of data on recycled hard disks, or secure shredding of printed output. Detail if such destruction/disposal is undertaken on site or off site by a contracted third party.
    2. How is data imported/exported from the solution? What controls are employed to protect any data on removable media (For example usb stick)?

4.1 **Account Monitoring and Control**

The system should provide tools for registering; managing and removing users’ accounts and access to sensitive data should be part of an audit trail.

4.1.1 Describe how are users accounts provisioned, managed and removed? (Please, include a full description of the process)

4.1.2 Describe how privileged accounts for system administrators are restricted to authorised individuals and how they are approved.

4.1.3 Explain whether access to sensitive information is monitored and audited and what information are included?

**5.1 Malware prevention**

Malicious software is a dangerous threat that can attack the system from different access points: emails’ attachments, infected web sites, user actions and removable media. Malware defences need to operate in this dynamic environment and be able to be updated across the infrastructure.

5.1.1 Describe the malware protection software adopted and how the protection is kept up to date on all computers that are connected to the Internet?

5.1.2 Does the malware protection prevent connections to malicious websites on the Internet?

**6.1 Supply chain**

The solution must guarantee that the protection of the NHS Scotland information assets is safe throughout the full service cycle.

6.1.1 What suppliers are involved in provision of any aspect of the solution? (Identify all supplier groups including internal/health board teams, and external commercial third parties)

6.1.2 Who is responsible for reviewing supplier performance and ensuring conformance with security requirements?

6.1.3 What independent assurance/audits/certifications are applicable to any part of the solution? Describe the scope of any applicable certifications.

6.1.4 What personnel pre-employment screening checks are applied for personnel involved in provision of the service?

7.1 **Testing and development**

The solution must ensure that industry practice information security controls are applied throughout the development lifecycle and it follows the Information Commissioner guidance on Privacy by Design. (Source: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/)

7.1.1 Is there a separate test and development environment? Is any live data utilised in this environment? How is access to the test and development environment controlled? Do developers have access to the live system?