<System Name>

System Security Policy (SSP)

**Document control**

|  |  |
| --- | --- |
| **Title** | <System Name> System Security Policy (SSP) |
| **Author** |  |
| **Creation date** |  |
| **Date of version** |  |

**Version history**

|  |  |
| --- | --- |
| **Version** | **Comments** |
|  |  |
|  |  |

Table of contents

[1 <System Name> overview 2](#_Toc359688)

[2 System description 3](#_Toc359689)

[3 Assets and services 5](#_Toc359690)

[4 People 8](#_Toc359691)

[5 Security controls 9](#_Toc359692)

[6 Risk analysis and recommendations 13](#_Toc359693)

[7 Annex A – NHS Scotland risk matrices 14](#_Toc359694)

# <System Name> overview

## Introduction

(Name of the system, background high level overview)

## Business goals/benefits of the system

(Purpose of the system, ownership, funding – any risk that might be accepted is accepted to enable the delivery of the business benefits)

## System status and timescales

(Current status of system/project, e.g. “outline business case”, “requirements”, “user acceptance testing”, associated timescales)

## Privacy impact assessment

(Any solution that processes personally identifiable data or other sensitive data must have a corresponding completed Privacy Impact Assessment. Provide summary of key points and cross reference here)

## Responsible parties

(Identify individual holders of key roles: system owner, system manager, senior information risk owner (SIRO), Information security officer (ISO), information governance officer, cross reference Appendix B if necessary)

The following individuals are responsible:

System owner: (who is paying for the system)

System manager: (who is responsible for implementing/managing the system)

Senior information risk owner (SIRO): (the person ultimately responsible for signing off the risk assessment)

Information security officer/Accreditor: (a security practitioner assisting in the development of the risk assessment)

Information governance officer: (an information governance practitioner assisting, most likely cross referenced to PIA)

# System description

## Context

(Describe key information like hosting locations, suppliers, functions, information processed, interdependencies – key points, high level)

## Operation

(Brief step by step description of key use cases)

## Hardware

(Architecture, summary of hardware, versions, configuration)

## Software

(Server OS/platforms, versions of server and client software, thick or thin client, underlying/enabling technologies where appropriate (such as Java, .NET, php, etc.)

## Interfaces

(List interfaces with other networks/systems/applications/organisations, describe how each communication and interface works e.g. SMTP email, web based access using SSL over HTTP, Internet facing web services based on WSDL, etc. Where possible capture specific technologies and versions of protocols in use)

## Accreditation scope

(Summarise what is in scope and any scope exclusions)

Figure 1 shows an overview diagram of the system.

**(Diagram is essential** – logical diagram based on physical locations – initially identify locations as boxes, put system components in each location, describe architecture and connectivity, add interfaces to other systems/networks/applications, place data storage and user groups)

<Insert diagram here>

Figure 1: diagram of proposed architecture

# Assets and services

## Introduction

At the heart of a risk assessment are assets that are valuable to the business and need to be protected – these assets include:

**Information assets** e.g. NHS data sets that must be protected from risks such as unauthorised access and loss

**Physical assets** e.g. mobile devices or data centre equipment that must be protected from threats such as theft and fire damage

**Services** e.g. clinical applications or infrastructure services like AD and DNS that must be protected from threats such as loss of service

This section captures the assets that are to be protected in the case of this information system.

## Information assets

Table 1 lists the information assets.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Name | Description | NHS sensitivity |
| A1 |  |  |  |
| A2 |  |  |  |
| A3 |  |  |  |

Table 1: information assets

The “NHS sensitivity” is the label applied to the information according to the NHS Scotland traffic light system as set out in Table 2.

|  |  |
| --- | --- |
| Label | Description |
| Green | This is information which is unlikely to cause distress to individuals, breach confidence or cause any financial or other harm to the organisation if lost or disclosed to unintended recipients. This can include information which mentions only a person’s name (e.g. routine appointment confirmation letter) as long as it does not contain anything that is judged to describe a person’s physical or mental state. |
| Amber | In most boards the largest proportion of patient information can be said to require extra protection because it constitutes sensitive personal data as defined by the Data Protection Act. In particular:   * any information about an individual (i.e. anything clinical or non-clinical) that would cause short-term distress, inconvenience or significant embarrassment if lost. * any information which if lost or disclosed to unintended recipients would lead to a low risk to a person’s safety (e.g. loss of an address but no evidence to suggest direct harm would result). * any information if lost that would be likely to negatively affect the efficiency of that service (e.g. cancellation of appointments). |
| Red | Most boards also hold some information which is highly sensitive. Particularly:   * Any information which if lost could directly lead to actual harm (e.g. to mental health or put the person at physical risk from themselves or others in any way). * Any information that would in the opinion of a qualified person cause substantial distress and/or constitute a substantial breach in privacy (e.g. identity theft, loss of professional standing) to the subject. This is likely to include for example information on a person’s sexual health. * Information that affects the privacy or could cause distress to more than one individual (e.g. several family members or several linked persons contained in a file). * Information relating to vulnerable persons’ health (e.g. child protection cases) * Information governed by legislation that requires additional layers of security and recognises the substantial distress that would be caused by loss (e.g. embryology, human fertilisation and gender re-assignment). * Information if lost that is likely to result in undermining confidence in the service or would cause significant financial loss to the organisation, prejudice investigation of crime etc. |

Table 2: NHS Scotland traffic light sensitivity descriptions

## Physical assets

Table 3 lists the *major* physical assets comprising the system. (If it is a managed service and the supplier owns all the major physical assets this section can be omitted)

|  |  |  |
| --- | --- | --- |
| ID | Description (model, type, configuration for all of these) | Cost to replace |
| PA1 |  |  |
| PA2 |  |  |
| PA3 |  |  |

Table 3: physical assets

## Services

Table 4 lists the services provided by the solution.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Name | Description | Max. tolerable downtime |
| S1 |  |  |  |
| S2 |  |  |  |
| S3 |  |  |  |

Table 4: services

# People

## User groups

Table 5 lists the user groups with access to the system.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Name | Description | Type of access | Number[[1]](#footnote-1) |
| U1 |  |  |  |  |
| U2 |  |  |  |  |
| U3 |  |  |  |  |
| U4 |  |  |  |  |

Table 5: User groups

In addition to people based sources of threat the following non-people based sources of threat should be considered in the risk assessment:

## Other sources of threat

In addition to people based sources of threat the following non-people based sources of threat shall be considered in the risk assessment:

Environmental threats such as fire, flood

Technical threats such as technical failure of equipment

Automated threats such as worms that propagate mostly without human interaction

# Security controls

## Supplier arrangements

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)

What contracts are in place? Summarise the information security/information governance/data protection contract terms, or other arrangements.

Do information security requirements that apply to the named contractor also apply to any subcontractors? Name any sub contractors.

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

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

## Access control

How are new users provisioned? How is it ensured that users get the correct permissions?

How do users log onto the solution? Are there different options for different interfaces?

How is it ensured that users can only access the information and functions for which they are authorised?

How are the user accounts managed? For example who removes accounts of staff that leave the organisation, resets forgotten passwords, updates a users permissions, changes to permissions, etc?

How can users recover their account if they forget their credentials?

How are user credentials, such as passwords, stored within the system?

Are any individuals/groups, who are **not** authorised users of the system, able to access any part of the system e.g. the hardware or shared infrastructure components? (For example cleaners or patients that may be able to access physical terminals in shared areas; or users of other applications that may be able to access a shared database or hosting environment)

## Personnel controls

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

How are users made aware of their security responsibilities with respect to the system? (e.g. to keep their password secret, or to report a security breach?)

What training is provided to system administrators or managers on how to properly run the system?

What information security and governance training is provided to users of the system?

## Network security controls

Are the system’s network interfaces hardened? For example have all unnecessary services been disabled and ports closed?

How does the solution protect access to network traffic on shared networks?

How is the hosting environment separated/protected from connected networks (e.g. firewall(s), models, config, etc.)?

Have all network components been deployed in a hardened configuration, for example all default passwords changed, and unneeded services blocked?

Is the solution remotely accessible? If so, how is the remote access provided and controlled?

## Data protection

Who are the data controllers and data processors for this solution?

Are all information assets held in the system allocated to a responsible owner?

Are any technical controls employed within the solution to protect information assets? For example encryption at rest, de-identification or data obfuscation.

What controls are in place to 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.

How is data imported/exported from the solution? What controls are employed to protect any data on removable media?

What information transfers does the solution permit/enable? How are these controlled?

## Physical and environmental security

What physical or environmental controls apply at any locations where the solution is hosted?

What physical security controls apply at any locations from where the solution is used/accessed?

## Operational security

Who is responsible for Information Backup controls? Describe the data backup and recovery process.

Who is responsible for solution Change Management? Describe the change management process.

What anti-malware controls apply within the solution?

How are information security incidents (or potential information security incidents) reported, managed and communicated?

What controls have been employed to ensure continuity of service?

Has a business continuity plan and a disaster recovery plan been produced for the solution? Have these plans been tested?

## Audit controls

Describe the audit controls employed by the solution. What events are recorded? For how long are audit logs retained? What tools are available to analyse audit logs?

Who is responsible for auditing system access?

How are audit logs protected from unauthorised access or modification?

## Solution development, testing and maintenance

Who is responsible for deploying patches and updates?

In what timescales will patches and updates be deployed?

Are any components of the solution **excluded** from the above patching policy?

Describe the patch deployment process.

What testing controls are in place to understand any potential unintended impacts of updates?

What agreements are in place to ensure the solution keeps pace with information security developments? For example migrating onto new information technologies when previous versions become obsolete/unsupported.

What security or vulnerability tests have been performed on the solution? What was the outcome of the test? What commitment has been made to ongoing security testing?

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?

## Assumptions

What assumptions have been made about security controls that are out of scope of this SSP? For example assumptions about controls that are believed to be the responsibility of the health boards or suppliers such as end user device security, behaviours or responsibilities, physical/environmental security at operating locations, etc.

# Risk analysis and recommendations

## This section to be completed in collaboration with

## Residual risk statement

Table 6 provides a summary of the key residual risks identified.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk | Threat actor | Risk examples | Residual risk | Recommendation |
| <Risk ID> (e.g. R1 from table in annex A) Denial of service – Internet services | Internet user | Denial of service on main business website causing damage to reputation and customer confidence | 4 | Accept |
|  |  |  |  |  |

Table 6: Summary of key risks

## Risk treatment recommendations

Significant residual risks

[Accreditor completes]

Risk treatment

[Accreditor completes]

Accreditation recommendation

[Accreditor completes]

# Annex A – NHS Scotland risk matrices

## Impact/consequence definitions

| **Descriptor** | **1 Very low (VL)** | **2 Low (L)** | **3 Medium (M)** | **4 High (H)** | **5 Very high (VH)** |
| --- | --- | --- | --- | --- | --- |
| Patient  Experience | Reduced quality of patient experience/clinical outcome not directly related to delivery of clinical care. | Unsatisfactory patient experience/ clinical outcome directly related to care provision – readily resolvable | Unsatisfactory patient experience/ clinical outcome; short term effects – expect recovery <1wk. | Unsatisfactory patient experience/ clinical outcome; long term effects – expect recovery >1wk. | Unsatisfactory patient experience/ clinical outcome; continued ongoing long term effects |
| Objectives / Project | Barely noticeable reduction in scope, quality or schedule. | Minor reduction in scope, quality or schedule. | Reduction in scope or quality of project; project objectives or schedule. | Significant project over-run. | Inability to meet project objectives; reputation of the organisation seriously damaged. |
| Injury (physical and  psychological) to patient/visitor/staff. | Adverse event leading to minor injury not requiring first aid. | Minor injury or illness, first aid treatment required. | Agency reportable, e.g. Police (violent and aggressive acts).  Significant injury requiring medical treatment and/or counselling. | Major injuries/long term incapacity or disability (loss of limb) requiring medical treatment and/or counselling. | Incident leading to death or major permanent incapacity |
| Complaints / Claims | Locally resolved verbal  complaint. | Justified written complaint peripheral to clinical care. | Below excess claim.  Justified complaint involving lack of appropriate care. | Claim above excess level.  Multiple justified complaints. | Multiple claims or single major claim  Complex justified complaint. |
| Service / Business  Interruption | Interruption in a service which does not impact on the delivery  of patient care or the ability to continue to provide service. | Short term disruption to service with minor impact on patient care. | Some disruption in service with unacceptable impact on patient care.  Temporary loss of ability to provide service. | Sustained loss of service which has serious impact on delivery of patient  care resulting in major contingency plans being invoked. | Permanent loss of core service or facility.  Disruption to facility leading to significant “knock on” effect |
| Staffing and Competence | Short term low staffing level temporarily reduces service  quality (< 1 day).  Short term low staffing level (>1 day), where there is no disruption to patient care. | Ongoing low staffing level reduces service quality  Minor error due to ineffective training/implementation of training. | Late delivery of key objective / service due to lack of staff.  Moderate error due to ineffective training/implementation of training.  Ongoing problems with staffing levels. | Uncertain delivery of key objective/ service due to lack of staff.  Major error due to ineffective training/implementation of training. | Non-delivery of key objective/service  due to lack of staff.  Loss of key staff.  Critical error due to ineffectivetraining/ implementation of training. |
| Financial (including  damage / loss / fraud) | Negligible organisational/personal financial loss. (£<1k).  (NB. please adjust for context) | Minor organisational/personal financial loss (£1-10k). | Significant organisational/personal financial loss (£10-100k) | Major organisational/personal financial loss (£100k-1m). | Severe organisational/personal financial loss (£>1m). |
| Inspection / Audit | Small number of recommendations which focus on minor quality improvement issues. | Recommendations made which can be addressed by low level of management action. | Challenging recommendations that can be addressed with appropriate action plan. | Enforcement action.  Low rating.  Critical report. | Prosecution.  Zero rating.  Severely critical report |
| Adverse Publicity / Reputation | Rumours, no media coverage.  Little effect on staff morale. | Local media coverage – short term.  Some public embarrassment.  Minor effect on staff morale/public attitudes. | Local media – long-term adverse publicity.  Significant effect on staff morale and public perception of the organisation | National media/adverse publicity, less than 3 days.  Public confidence in the organisation undermined.  Use of services affected. | National/international media/adverse publicity, more than 3 days.  MSP/MP concern (Questions in Parliament).  Court Enforcement.  Public Inquiry/ FAI. |

Table 7: Impact/consequence definitions

## Likelihood definitions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Descriptor** | **1 Very low (VL)** | **2 Low (L)** | **3 Medium (M)** | **4 High (H)** | **5 Very high (VH)** |
| Probability | Rare - can’t believe this event would happen – will only happen in exceptional circumstances | Unlikely - not expected to happen but definite potential exists – unlikely to occur. | Possible - may occur occasionally, has happened before on occasions – reasonably chance of occurring | Likely - strong possibility that this could occur – likely to occur | Almost certain - this is expected to occur frequently / in most circumstances – more likely to occur than not |

Table 8: Likelihood definitions

## Risk matrix

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Impact | | | | |
| Likelihood | **Very low (1)** | **Low (2)** | **Medium (3)** | **High (4)** | **Very high (5)** |
| **Very low (1)** | Low1 | Low 2 | Low 3 | Medium | Medium |
| **Low (2)** | Low | Medium | Medium | Medium | High |
| **Medium (3)** | Low | Medium | High | High | High |
| **High (4)** | Medium | Medium | High | High | Very High |
| **Very high (5)** | Medium | High | High | Very High | Very High |

Table 9: Risk evaluation matrix

## NHS Scotland risk appetite statement

NHS Scotland risk appetite is broadly defined as “cautious”: Preference for safe delivery options that have a low degree of residual risk and may only have limited potential for reward. Further guidance on the acceptance of risk is defined based on residual risk values:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Residual risk value | 1-3 | 4-8 | 9-19 | 20+ |
|  | Risk acceptable | Risk may be acceptable if all methods for further mitigating or avoiding the risk have been considered | Further reduction of risk strongly recommended | Risk unacceptable |

Table 10: Residual risk statement options

1. Approximate number band: 1-9, 10-99, 100-999, etc. [↑](#footnote-ref-1)