### Management of Policies Procedure control sheet

<table>
<thead>
<tr>
<th>Name of document to be loaded</th>
<th>ICT Information Security Incident Management Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area to be added to</td>
<td>Information Governance</td>
</tr>
<tr>
<td>Type of document</td>
<td>Policy</td>
</tr>
<tr>
<td>Immediate</td>
<td></td>
</tr>
<tr>
<td>Priority</td>
<td></td>
</tr>
<tr>
<td>Questions</td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td></td>
</tr>
<tr>
<td>Where to be published</td>
<td>External and Internal</td>
</tr>
<tr>
<td>Target audience</td>
<td>NHSFV wide</td>
</tr>
</tbody>
</table>
Consultation and Change Record

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Change</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>20/08/12</td>
<td>LALLEN</td>
<td>Draft produced</td>
<td>0.1</td>
</tr>
<tr>
<td>19/08/13</td>
<td>LALLEN</td>
<td>Comments from IG group applied</td>
<td>1.0</td>
</tr>
</tbody>
</table>

Contributing Authors: Information Governance

Consultation Process: Information Governance, ICT Department, Security of Information Working Group

Distribution:

Date | Author | Change                                      | Version |
---|-------|---------------------------------------------|---------|
20/08/12 | LALLEN | Draft produced                              | 0.1     |
19/08/13  | LALLEN | Comments from IG group applied              | 1.0     |
1 INTRODUCTION

1.1 Overview
This procedure describes NHS Forth Valleys’ (NHSFV) approach to reporting and managing an Information/IT security (ITS) related incident.

A ITS security incident is defined as a breach, threat, weakness, or malfunction that impacts on the confidentiality, integrity, and availability of one or more of NHSFVs’ information assets (electronic or manual).

This procedure is aligned closely with ISO 27002 (ISO/IEC 17799:2005) best practice and is a requirement of the NHS Scotland Information Governance Standards.

1.2 Purpose
The objectives of the process are:
a) To establish whether a suspected ITS event is in fact an incident;
b) To analyse the incident;
c) To contain the incident, to eradicate the cause(s), and to recover from the incident;
d) To learn from the incident, with a view to avoiding a recurrence and of its ill effects;
e) To minimise any necessary business disruption.

2 PROCESS

2.1 Recognising a ITS Security Incident
The following are examples of common symptoms that can occur to suggest a ITS security incident within the organisation. This is not intended to be an exhaustive list and is simply to provide guidance. If in doubt, advice and further guidance should be sought from the NHSFV IT Security Officer or a member of NHSFV’s ICT Support Team.

2.1.1 Unauthorised Access / Modification
Examples:-

- Files that should be accessible to a user are suddenly unavailable.
- A user’s account suddenly becomes active, but the user is not there to use it and is known not to be using it remotely (computer hacking).
- System logs record numerous unsuccessful logon attempts to a given user’s account, but the user denies multiple logons.
- Files have been edited, though no changes in them should have occurred.
- Application software has been modified, but changes have not been approved through the Change Control process.
Output of a sensitive nature that would normally be handled carefully is found in printer trays or left uncontrolled in the work area.

Unauthorized personnel are discovered in the work area.

Files (manual/electronic) appear, disappear, or undergo significant and unexpected changes in size.

User accounts appear or disappear from the system without the knowledge or consent of the system administrator.

Parts or all of the system logs are missing, or logs appear altered.

A user’s password has been changed without the user’s knowledge or involvement.

### 2.1.2 Malicious Software Outbreaks (Including Spyware and Adware)

Examples:

- Similar symptoms (error messages, system or application failure) reported by several users, and not obviously explainable by another cause.
- Sudden degradation or failure of service on several NHSFV servers.
- Any purported error messages or other system messages using profanity, apparent jargon, poor English or a foreign language.
- Unexpected graphics on screen.
- Desktop PCs become unstable/unusable/slow for no obvious reason.
- Numerous pop-ups encountered while browsing.
- NHSFVs’ anti-virus reports virus infections at several points.
- Sudden very high volume of outbound emails.
- Denial of service attacks - Internet-facing servers, and possibly other servers, degrade due to very heavy inbound traffic. Connections may be lost.

### 2.1.3 Misuse

Examples:

- High incidence of misaddressed incoming emails,
- Inappropriate or illegal material found on user’s PC or network storage,
- Unauthorised software found on user’s PC (possible malicious software, or breach of policy).

### 2.2 Reporting of a Security Incident (See Appendix F)

A security incident may be reported in a number of ways:

- Identified as part of a ICT Helpdesk call (for example a virus),
- Identified as part of an incident report (IR1) (Safeguard system),
- An anomaly may be reported by a member of staff;
• A line manager may raise a concern over a member of staff;
• An item may be reported as stolen,
• Excessive or inappropriate use may be identified as part of routine monitoring of web and e-mail communications,
• Whistle blowing.

(Once again, these are examples and are not intended to be an exhaustive list).

Once a potential security incident has been identified all relevant details should be made available when reporting the incident, so that a complete investigation can be conducted.

For computer related incidents, any messages that appear on the screen and any other facts that might be relevant (e.g. the sequence of events that led to the problem, any recent changes, the time and date, etc.) should be recorded. These details should be reported in the first instance through the ICT Service desk or by telephone 01324 566556 (if emergency). Information relating to breaches and threats should be given to the NHSFV IT Security Officer (01786 433283) fv-uhr.informationgovernance@nhs.net as well as being logged on the Incident Report system (IR1) available on the NHS FV Intranet as soon as practically possible.

For non-computer related incidents, details about the event (e.g. name of person involved, activity, place, time and date, etc.) should be recorded using the IR1 system.

Hoax virus warnings should also be reported to the ICT Service desk.

2.3 Incident Validation

An incident, having been reported, will involve a set of symptoms. Those symptoms will be compared, formally or informally, against current known exploits, and/or some other authoritative source of information. A member of the ICT Support team will perform this validation in conjunction with the NHSFV IT Security Officer if required.

If the incident is not validated as being a security incident, then this process is terminated and the call dealt with as a normal through the ICT Service desk.

2.4 Incident Analysis

Once a suspected security incident has been identified as such by the ICT Service desk, the NHSFV IT Security Officer will be informed and in conjunction with other expert/informed opinion(s) will decide:-

• Is this incident of sufficient magnitude to keep an Incident Log (see Appendix D)?
• Is this incident likely to escalate into such?

The NHSFV Risk Assessment model will be used to establish the magnitude of the security incident and categorise it accordingly. See Appendix H.
The Incident Log, if warranted, should contain:-
- Incident details as reported (See Section 2.1).
- A detailed explanation of the incident.
- The operational urgency of incident.
- Planned actions and findings.
- The current status of the incident
- Escalation points

The following practices should be followed in maintaining the Incident Log:-
- The log should be restricted only to staff involved in the investigation.
- All entries must be timed/dated, and signed (in whatever fashion) by the creator of the entry.
- Entries should never be expressions of opinion, but of fact.

It is vital that the NHSFV IT Security Officer and the relevant departmental head agree the planned corrective action required and that all relevant parties affected e.g. application owners, system administrators are contacted and the required action is communicated to them.

If the incident is deemed serious enough to warrant an incident log then the Information Security Incident Management team must be notified (see Appendix E).

2.5 Resolution Timescale and Escalation for Corrective and Preventative Action

Target times for resolution are dependant on the nature and severity of incident. During the Incident Validation (see section 2.3), an agreed timescale should be agreed between those involved. Where relevant, this should be noted in the Incident Log (ISF04D) and / or the Service desk system.

Target times have been documented and are dependant on the nature of incident:-

<table>
<thead>
<tr>
<th>Operational Impact</th>
<th>Target Time to Fix / Escalate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severe</td>
<td>3 Hours</td>
</tr>
<tr>
<td>Urgent</td>
<td>1 Day</td>
</tr>
<tr>
<td>High</td>
<td>1 Week</td>
</tr>
<tr>
<td>Important</td>
<td>1 Month</td>
</tr>
<tr>
<td>Low</td>
<td>3 Months</td>
</tr>
</tbody>
</table>

For example, an incident which would lead to severe operational impact within NHS Forth Valley should be set at a maximum of 3 hours following notification to the NHSFV IT Security Officer. However, if investment is required a timeline of up to 3 months is more appropriate.
If after expiry of the target time there is no resolution of the incident, the incident must be escalated to the full Information Security Forum for formal review.

In the worst case scenario the incident will be classed as a disaster and NHSFVs’ formal disaster recovery (DR) plan will be invoked.

2.6 Incident Management

The key tasks involved in dealing with the incident are:

a) Containment
b) Eradication
c) Recovery/Invocation Of Formal NHSFV DR plan – leading to full recovery
d) Post-incident tasks
e) Incident Closure

The next step is to create a containment strategy, based on the type of incident.

3 TYPES OF SECURITY INCIDENTS

3.1 Breaches of Confidentiality

Disclosure

In April 2010, statutory powers were provided to the Information Commissioner to facilitate the enforcement of monetary penalties against organisations that failed in the provision of adequate security to Personal information as defined by the Data Protection Act 1998 (DPA). Any accidental or deliberate disclosures should be notified urgently to the NHSFV Data Protection Lead (01786 433285) fv-uhb.informationgovernance@nhs.net and will be dealt with in accordance with the NHSFV’s Disciplinary and Employee Conduct policies.

Unauthorised Access

One of the key elements of the Computer Misuse Act 1990 (CMA) is that of “unauthorised access”. In order to prosecute a Section 1 of the CMA, it is imperative that logs and system files are preserved prior to remedial action being taken.

Sharing Passwords

Individuals within NHSFV are under strict instructions not to share passwords with anyone. This type of incident will be dealt with in line with established policies e.g. NHSFV IT Security policy and through the NHSFV disciplinary process in conjunction with Human Resources.
3.2 Breaches of Integrity

Fraud
Where an incident is a deliberate and serious action to defraud the organisation, an authorised law enforcement agency must be involved and those involved take advice from them and / or specialist staff to ensure evidential continuity and integrity.

Unauthorized Modification
Another of the key elements of the CMA is that of “unauthorised modification”. In order to prosecute a Section 3 of the CMA, it is imperative that logs and system files are preserved prior to remedial action being taken.

Power Failure
This can be in the form of any component within NHSFV infrastructure caused by electrical fault or anomaly requires investigation and timely restitution. This containment may require the intervention of NHSFVs’ utility company provider.

Procedural Errors
Individuals who systematically fail to follow the documented procedures then containment should take the form of guidance and or training to minimise the likelihood of these occurring again in the future.

Misuse
This category covers a wide range of incidents from email and Internet abuse to the more offensive issues such as pornography or racial discrimination.

Where there is an intention to prosecute, it is advisable to seek specialist advice to secure the chain of evidence. Further, Human Resources should be involved with such incidents in case of the possible damage to corporate reputation.

3.3 Breaches of Availability

Theft
With an increasing range of mobile devices (e.g. laptops, PDAs, removable storage) the loss of business information through theft of such devices could seriously compromise the organisation. The containment strategy is likely to depend on the type and protective marking of the information held on the device.

It is likely that an authorised law enforcement agency will be involved.

Malicious Software
If malicious software is self-replicating, then the pathways must be removed as part of the containment strategy. The authorisation for this may be required from senior management whether it is shutting down internal or external e-mail, or isolating relevant traffic at a port level on a firewall.
All infected computers must be identified, and disconnected from the network by authorised ICT personnel for maintenance.

**Denial of Service**

During a Denial of Service (DoS) attack, the containment strategy would be to remove the attack vector(s). For example, if the DoS attack is coming from an easily identifiable source, it may be possible to deny a specific class of traffic, or even all traffic until the attack has ceased. Alternatively, where the attack is exploiting vulnerability, then the containment strategy would be to patch it.

**Wilful Damage**

In the rare cases where computer equipment or devices are deliberately damaged then the containment strategy should be dealt with under the Disciplinary Policy.

**System Failure**

This can be in the form of hardware or software failure caused by unforeseen circumstances that requires investigation and timely resolution. This containment may require the intervention of ICT personnel and or system vendors.

### 4 ERADICATION/RECOVERY AND GUIDANCE

Having contained the incident and made any required management decisions concerning preservation of evidence etc., the next step is to address the cause of the incident.

Eradication and recovery are primarily technical issues, whose details depend very largely on the precise details of the incident, and of the damage it may have caused. Guidance relates to the ‘Human’ errors or acts that require training and or disciplinary action.

This section does not attempt to cover all types of incidents but provide a few examples related to technical and non-technical (human) incidents.

#### 4.1 Examples of Technical Incidents:

**Denial of Service**

In the case of a denial of service attack, there is little or no action required immediately following the containment phase. Assuming that the removal of vulnerabilities has been done as part of containment, it should be found that recovery of the service is automatic.

Any question of inappropriate usage (insider rather than outsider attack) will best be handled under that heading. Assuming, therefore, that the individual is external, there will be no opportunity to control his/her actions directly as part of eradication. The next step to contemplate for this category, therefore, will be that of post-incident activity.

**Malicious Software**

There may be competing priorities here: firstly, the need to salvage as much service data as possible, and secondly, the need to restore service as soon as possible.
What must never be contemplated, however, is the restoration to normal operations before the malicious software has been completely eradicated. There is a risk here of re-infection, with consequent additional costs and loss of service.

Prior to restoring service, it is vital to ensure that the configuration of anti-virus software, browser security settings etc. are up-to-date. In addition, if it has been possible to identify the attack vector, it may be necessary to take management action (e.g. training of staff, removal of remote access privileges) to discourage or prevent further opportunities for infection to occur.

4.2 Examples of Non Technical Incidents:

Unauthorized Access

The removal of access rights etc. has the effect of removing the immediate problem. Any further hardening against comparable incidents will be undertaken as part of post-incident activity.

Recovery from an attack will involve correcting any loss of integrity or availability resulting from the incident. This may involve e.g. identifying and restoring corrupted or deleted files, correcting any malicious configuration (e.g. Windows registry items, executables).

Loss and breach of confidentiality is not recoverable.

Inappropriate Usage

Once any requirements for collection of evidence have been fulfilled, eradication of the cause of the problem will normally involve management action to discourage or prevent the individual from continuing or repeating his/her actions.

Recovery from the incident is likely to involve removing results of the inappropriate usage, e.g. erasing illegal material from equipment.

Note: compromised equipment must never be returned to service without all trace of such material being removed. This requirement is to protect any future users of the equipment against unjustified accusations. It may also be advisable in such cases to have disks physically destroyed; alternatively they can be forensically cleansed.

5 POST INCIDENT ACTIVITY – REPORTING SECURITY INCIDENTS

5.1 Process

Post-incident activity should be completed by the relevant Team Leader and NHSFV IT Security Officer and cover the following areas:-

- Produce a final report for the next management review meeting.
- Review of the incident to confirm, if possible, the validity of the analysis and the effectiveness of the actions taken;
- Assessment of any service, process or procedure changes which may be
necessary to prevent or discourage a recurrence of the incident including updating all relevant documentation; (Preventative Action)

- Consideration of any training or awareness initiatives arising from the incident.
- Close off any ISF10D Incident Logs in use. These should be collated and passed to the NHSFV IT Security Officer for permanent retention.
- Update any NHSFV Service desk system entries accordingly.

Ensure that ISF01A is created for each incident, taking detail from ISF04D as required. The classification of an incident is as follows:

Information/IT Security incidents will be summarised on the detailed ITS incident reporting form – ISF02B to provide an organisation wide summary – see Appendix B. This report can be broken down by Department to assist learning and help to minimise their future occurrence.

The relevant department in which the breach occurred should complete ISF03C which the NHSFV IT Security Lead will present to the Security of Information Group (see Appendix C) as part of the Management Review.

6 INCIDENT TEAM CONTACT DETAILS

ICT Helpdesk:  fv-uhb.servicedesk@nhs.net  01324 566556
IT Security Officer:  fv-uhb.informationgovernance@nhs.net  01786 433283
Data Protection Lead:  fv-uhb.informationgovernance@nhs.net  01786 433285
IG Team:  fv-uhb.informationgovernance@nhs.net  01786 433282
# APPENDIX A – DETAILED INCIDENT REPORTING FORM (ISF01A)

<table>
<thead>
<tr>
<th>Date of Incident</th>
<th>Time of Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name of Individual</th>
<th>Username</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Full Details of Incident

## Proposed Action Recommended

| Investment / Training / Counselling / Disciplinary / Refer to Line Manager |

## Logged by

## Escalation Process

<table>
<thead>
<tr>
<th>1. Breach</th>
<th>3. Weakness</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Threat</td>
<td>4. Failure</td>
</tr>
</tbody>
</table>

## Remedial Timeline

<table>
<thead>
<tr>
<th>3 Hours / 1 Day / 1 Week / 1 Month / 3 Months</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

## Confidentiality

<table>
<thead>
<tr>
<th>Disclosure</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Theft</td>
</tr>
</tbody>
</table>

## Unauthorised Access

<table>
<thead>
<tr>
<th>Malicious Software (4)</th>
</tr>
</thead>
</table>

## Sharing Passwords

<table>
<thead>
<tr>
<th>Systems Failure (1)</th>
</tr>
</thead>
</table>

## Integrity

<table>
<thead>
<tr>
<th>Wilful Damage</th>
</tr>
</thead>
</table>

## Fraud

## Unauthorised Modification

## Procedural Errors (2)

## Power Failure (3)

## Misuse (5)

## Key

<table>
<thead>
<tr>
<th>1 – Systems Failure</th>
<th>2 – Procedural Errors</th>
<th>3 – Power Failure</th>
<th>4 – Malicious Software</th>
<th>5 – Misuse</th>
</tr>
</thead>
<tbody>
<tr>
<td>A – Hardware</td>
<td>A – Unlicensed Software</td>
<td>A – Server</td>
<td>A – Spoofing</td>
<td>A – Private Work</td>
</tr>
<tr>
<td>B – Software</td>
<td>B – Other</td>
<td>B – Desktop</td>
<td>B – Email Spam</td>
<td>B – Internet</td>
</tr>
</tbody>
</table>

Version 1.0 13/09/2013 Page 14 of 23

UNCONTROLLED WHEN PRINTED
**APPENDIX B – SUMMARISED INCIDENT REPORTING FORM (ISF02B)**

<table>
<thead>
<tr>
<th>Date</th>
<th>Summary of the Security Incident</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
<th>Intent</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Key**

1 – Systems Failure  2 – Procedural Errors  3 – Power Failure  4 – Malicious Software  5 – Misuse

A – Hardware       A – Unlicensed Software       A – Server       A – Spoofing       A - Private Work
B – Software       B – Other        B – Desktop       B – Email Spam       B – Internet
C – Laptop        C – Viruses & Worms        C – Offensive
## APPENDIX C – MONTHLY INCIDENT REPORTING FORM (ISF03C)

<table>
<thead>
<tr>
<th>Type of Incident</th>
<th>Number of Incidents</th>
<th>Intent</th>
<th>Business Consequence*</th>
<th>Remedial Action Required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Accidental</td>
<td>Deliberate</td>
<td>Investment</td>
</tr>
<tr>
<td><strong>Confidentiality</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Disclosure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Unauthorised access</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Sharing passwords</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Fraud</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Unauthorised modification</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Power failure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Procedural errors</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Misuse</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Theft</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Malicious software</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Wilful damage</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Systems failure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Qualitative and / or quantitative - Criticality of system, no. of people involved, length of downtime, impact, hours affected × average salary
APPENDIX D – PERSONAL INCIDENT LOG (ISF04D)

<table>
<thead>
<tr>
<th>Date / Time</th>
<th>Item Number</th>
<th>Detailed Description</th>
<th>Witness Verification (If used)</th>
</tr>
</thead>
</table>

Incident as Reported:-

Incident Log of:

Reference | Date |
APPENDIX E – INFORMATION/IT SECURITY INCIDENT MANAGEMENT TEAM

Members

- Head of ICT
- Senior ICT Service Managers
- Head of Information Management
- Head of Information Governance
- IT Security Officer
- Data Protection Lead
- HR manager

Purpose

To conduct an investigation when a serious breach, as defined in the Security Reporting and Incident Management Procedure, has been identified.

Depending on the nature of the incident, not all members may be required to participate. It may also be necessary to call upon the services of additional resources for specific actions.

Individual duties

Information Governance team

- Perform investigation and collate evidence for presenting to Incident Management team. Provide specialist advice regarding any legal aspect. Act as “expert witness” in any resultant disciplinary action, as necessary.

Head of ICT and Senior ICT Services Managers

- Provide technical resource, where necessary, for any incident involving a breach of the IT Security policy. To liaise with the Head of IG and Director of IM&T/eHealth Lead.

Head of Information Management

- Liaise with Head of IG, Head of ICT and/or Director of IM&T/eHealth Lead.

HR Manager

- Provide advice regarding employment law and discipline procedures as they apply to the incident. Will notify the relevant line manager as necessary. Where necessary will be involved in any disciplinary action that results.

ICT Service desk

- Take details of initial call from member of staff. Ascertain whether incident form has been completed and note response in call. Pass call on to Information Governance team.
APPENDIX G – DEFINITION OF SECURITY BREACH

The table below lists the types of events that may be classified as Incidents. The seriousness of each incident, and hence the resulting action, will be determined on a case by case basis.

| Malware | Intentionally, or accidentally through reckless conduct, introducing malware (malicious software) onto NHSFVs’ infrastructure and/or storage of virus material on NHSFV hardware. The term malware includes, but is not restricted to, viruses, worms, Trojan horses, spyware and adware.  
Examples:  
- Downloading and installing toolbars or animated cursors;  
- Downloading “Smileys”, etc.  
- Downloading unauthorised software |
| --- | --- |
| Unauthorised Access | Intentional entry to NHSFV Information Systems via hacking, misappropriation of Administrator rights, usage of login and passwords other than those allocated to user.  
Example:  
- Logging on to the network or a specific system using a colleague’s credentials with or without their knowledge. |
| Unauthorised Software | Software stored on file servers, desktop or mobile computers, including laptops, notebooks, PDAs and Blackberries, that is not authorised by NHSFV ICT Services; unlicensed software, pirated software, inappropriate software including, but not restricted to, non work related image, video, audio or executable files, etc.  
Examples:  
- Installing personally owned copies of applications;  
- Storing non work related photographs;  
- Storing music files. |
| Theft | Physical theft of NHSFVs’ owned Hardware or Software. Theft of NHSFV information.  
Examples:  
- Failing to return assets upon completion of project;  
- Taking copies of information with NHSFVs’ IPR (Intellectual Property Rights) for personal gain. |
| Misuse of Company Assets | Use of NHSFV Property including ICT assets for excessive personal use, for personal gain, for business use other than that of NHSFV.  
Examples:  
- Running a personal business;  
- Unreasonable amount of time on Internet for personal use. |
| **Unauthorised Equipment** | Connection of equipment to NHSFVs’ computers or network that is not owned by NHSFV, or has not been approved by NHSFV ICT Services. This includes, but is not restricted to, desktop and laptop computers, USB storage devices including MP3 players, modems, routers/switches, cameras, mobile phones, etc.  
Examples: Using unauthorised USB memory stick; Connecting unauthorised wireless router. |
|---------------------------|--------------------------------------------------------------------------------------------------|
| **Breach Of Confidentiality** | Disclosure of confidential NHSFV Information/Documentation/Data to external sources.  
Examples: Emailing patient information out from NHSFV NHSmail to non NHSmail accounts such as Hotmail; Leaving patient records unattended in a public place. Discussing patients on Social Media |
| **Breach Of Procedure** | Use/Installation/Removal/Relocation/Extension of NHSFV ICT systems contrary to NHSFV Processes and Procedures.  
Example: Installation of a desktop computer in a location where confidential information can be viewed by unauthorised persons. |
## APPENDIX H – RISK ANALYSIS TABLE – IMPACT/CONSEQUENCE DEFINITIONS

<table>
<thead>
<tr>
<th>Descriptor</th>
<th>Negligible</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Extreme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Injury (physical and psychological) to patient/visitor/staff</td>
<td>Adverse event leading to minor injury not requiring first aid.</td>
<td>Minor injury or illness, first aid treatment required.</td>
<td>Agency reportable, e.g. RIDDO, Police (violent and aggressive acts). Significant injury requiring medical treatment and/or counselling</td>
<td>Major injuries/long term incapacity or disability (loss of limb) requiring medical treatment and/or counselling. Broken bone.</td>
<td>Incident leading to death or major permanent incapacity.</td>
</tr>
<tr>
<td>Staffing and Competence</td>
<td>Short-term low staffing level temporarily reduces service quality (&lt; 1 day). Short term low staffing level (&gt;1 day), where there is no disruption to patient care.</td>
<td>Ongoing low staffing level reduces service quality. Minor error due to ineffective training/implementation of training.</td>
<td>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.</td>
<td>Uncertain delivery of key objective/service due to lack of staff. Major error due to ineffective training/implementation of training.</td>
<td>Non-delivery of key objective/service due to lack of staff. Loss of key staff. Critical error due to ineffective training/implementation of training.</td>
</tr>
<tr>
<td>Objectives / Project</td>
<td>Barely noticeable reduction in scope, quality or schedule.</td>
<td>Minor reduction in scope, quality or schedule.</td>
<td>Reduction in scope or quality of project; project objectives or schedule.</td>
<td>Significant project over-run.</td>
<td>Inability to meet project objectives; reputation of the organisation seriously damaged</td>
</tr>
<tr>
<td>Complaints / Claims</td>
<td>Locally resolved verbal complaint.</td>
<td>Justified written complaint peripheral to clinical care.</td>
<td>Below excess claim. Justified complaint-involving lack of appropriate care.</td>
<td>Claim above excess level. Multiple justified complaints.</td>
<td>Multiple claims or single major claim Complex justified complaint</td>
</tr>
<tr>
<td>Service / Business Interruption</td>
<td>Interruption in a service that does not impact on delivery of patient care or the ability to continue to provide service.</td>
<td>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.</td>
<td>Sustained loss of service which has serious impact on delivery of patient care resulting in major contingency plans being invoked.</td>
<td>Permanent loss of core service or facility. Disruption to facility leading to significant “knock on” effect</td>
<td></td>
</tr>
<tr>
<td>Inspection / Audit</td>
<td>Small number of recommendations which focus on minor quality improvement issues.</td>
<td>Recommendations made which can be addressed by low level of management action.</td>
<td>Challenging recommendations that can be addressed with appropriate action plan.</td>
<td>Enforcement action. Low rating. Critical report.</td>
<td>Prosecution. Zero rating. Severely critical report.</td>
</tr>
<tr>
<td>Emergency planning/ Region wide</td>
<td>Insignificant numbers of injuries or impact on health.</td>
<td>Small number of people affected, no fatalities, and a small number of minor injuries with first aid treatment.</td>
<td>Limited number of people affected, no fatalities, some hospitalisation and medical treatment. Localised displacement of small number of people for 6-24 hrs.</td>
<td>Significant number of people in affected area, with multiple fatalities, multiple serious or extensive injuries, significant hospitalization. Large number of people displaced 6-24 hrs or possibly beyond.</td>
<td>Very large number of people (100s) in affected area impacted, significant numbers of fatalities, large number of people requiring hospitalization with serious injuries with longer-term effects.</td>
</tr>
</tbody>
</table>
### Likelihood Definitions

<table>
<thead>
<tr>
<th>Descriptor</th>
<th>Rare</th>
<th>Unlikely</th>
<th>Possible</th>
<th>Likely</th>
<th>Almost Certain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability</td>
<td>Can’t believe this event would happen – will only happen in exceptional circumstances.</td>
<td>Not expected to happen, but definite potential exists – unlikely to occur.</td>
<td>May occur occasionally, has happened before on occasions – reasonable chance of occurring.</td>
<td>Strong possibility that this could occur – likely to occur. Not persistent.</td>
<td>This is expected to occur frequently / in most circumstances – more likely to occur than not. Persistent</td>
</tr>
</tbody>
</table>

### Risk Levels

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Consequences / Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Negligible</td>
</tr>
<tr>
<td>Almost Certain</td>
<td>Medium</td>
</tr>
<tr>
<td>Likely</td>
<td>Medium</td>
</tr>
<tr>
<td>Possible</td>
<td>Low</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Low</td>
</tr>
<tr>
<td>Rare</td>
<td>Low</td>
</tr>
</tbody>
</table>