**Appendix 1: Incident Identification Guide**

# Definition of an Information Security Incident

The potential loss of Confidentiality, Integrity or Availability affecting an information asset. The following are examples of security incidents:

# Unauthorised access to computer files/secure locations:

* Complaints from users about other unauthorised users accessing confidential files;
* Inappropriate access to mailboxes/folders;
* Third party access without change control authorisation;

# Unauthorised disclosure of information, confidential data:

* Confidential information left in network printers/faxes;
* Confidential information sent to wrong printers/locations/email recipients;

# Password/Credentials sharing:

* Users sharing access to individual accounts i.e. login account, clinical systems, email;
* Passwords written down in i.e. post-it notes;
* Concerns about shoulder surfing or inadvertent disclosure of passwords;

# Backup Failure:

* SNMPC alerts for system backups;
* Calls logged by staff;

# Data Loss:

* Information being stored locally in a PC without being backed up;
* Inadvertent deletion of data ;
* Corrupt backups;
* Loss of hard copy information/paper;
* Loss of IT equipment, USB sticks, other devices that could contain data i.e. tablet, iPad;

# Theft:

* Theft of IT equipment i.e. computers, iPads, memory sticks, monitors etc;

# Unplanned downtime for important services

* Unavailability of critical systems: i.e. Oasis/PACS/Labs/Opera;
* Unavailability of other clinical systems;
* Network unavailability/connection problems i.e. Internet, file stores etc.;

# Significant Network issues:

* Network kit hardware failure;
* Firmware issues;
* External internet faults;
* Non NHS Fife equipment connecting to the network;

# Vandalism:

* Cable/wire theft;
* Destruction of equipment/infrastructure;

# Virus outbreaks:

* Alerts from ePO Server (McAfee);
* Users reporting virus infection or suspicious behavior;
* Malware alerts/reports by users;

# Inappropriate access rights for user accounts:

* Movers still having access to a system/area not longer required for the new job;
* Users/third parties having more privileges than required for the position;

# Fraud:

* Misuse of financial systems;
* Forgery of documentation/signatures;

# Loss of power (unplanned):

* UPS failures;
* Unplanned mains cut;
* Generator failure;

# Policy/regulation breaches:

* Breach of acceptable use policy;
* Breach of confidentiality agreement;
* Breach of Data protection act/Computer misuse act;
* Caldicott permission not granted for data use;

# Misuse of IT equipment/facilities (unacceptable use):

* Excessive personal use within work time;
* Running another business;
* Installation of unauthorised software;
* Breeching dignity at work principles;
* Inappropriate use of Internet;

# Attempted or successful social engineering attacks:

* Bogus calls;
* Spear Phishing;
* Impersonating;
* Actual or penetrating of logical access controls;

# Misuse of NHS Mail:

* Spam;
* unsolicited emails;
* chain emails;

# Web filtering issues:

* Inappropriate/Unauthorised websites not being blocked as they should;
* Inappropriate configuration of the Web filtering system for certain machines i.e. Internet Café;