POLICY

The Clatterbridge Cancer Centre NHS Foundation Trust

IM&T POLICY

Information Security Incident Response and Management

Policy reference	**PTWSISIRM**
Version	**1.4**
Summary	The purpose of this document is to ensure that all departments within CCC are fully aware of the reporting responsibilities within the organisation and also by 3rd Parties
Name and designation of policy author(s)	Richard Pilkington – IT Security Manager
Approved by (committee, group, manager)	James Crowther – Head of IT Operations
Approval evidence received (minutes of meeting, electronic approval)	Electronic approval received
Date approved	12th May 2021
Review date	May 2022
Review type (annual, three yearly)	Annual
Target audience	All Staff
Links to other strategies, policies, procedures	Information Security Policy
Protective Marking Classification	Internal
This document supersedes	V1.3

Consultation

	Authorised by	Date authorised	Comments
Equality Impact Assessment	Michelle Pennington- Document Control Manager & FOI Lead	17th March 2017	No requirement for full assessment
Fraud department	Claire Smallman, Anti-Fraud Manager, MIAA	3rd July 2018	Assessment no longer needed

Circulation/Dissemination

Date added into Q-Pulse	14th May 2021
Date document posted on the Intranet	14th May 2021

Version History

Date	Version	Author name and designation	Summary of main changes
Jan 2017	1.0	Richard Pilkington- ICT Manager/Information Security Manager	New Policy.
June 2018	1.1	Richard Pilkington- ICT Manager/Information Security Manager	Annual review and GDPR update
June 2019	1.2	Richard Pilkington – IT Security Manager	Annual Review – minor changes
May 2020	1.3	Richard Pilkington – IT Security Manager	Annual Review – minor changes
May 2021	1.4	Richard Pilkington – IT Security Manager	Annual Review – minor changes

1.0 Introduction

Information and information systems are important corporate assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support the operation and continued success of The Clatterbridge Cancer Centre NHS Foundation Trust (CCC).

The CCC Digital Team acknowledges that we must demonstrate to third parties our expertise in security technology and implementing it. To achieve this, it is recognised that we must protect our own assets as well as the environment.

The aim of the CCC Digital Team Security Policy and Security Standards is to maintain the confidentiality, integrity and availability of information stored, processed and communicated by and within CCC. These standards, procedures and policies are used as part of the Information Security Management System (ISMS).

This section covers arrangements for reporting and management of incidents or potential incidents, which breach these policies and associated procedures.

This document covers two separate but closely related areas: incident reporting, and incident investigation.

Incident reporting can be sub-divided into two main areas of interest:

- Reporting incidents as part of the incident management process.
- Reporting incidents as part of an ongoing process of collecting data on security incidents in order to extract statistical data and trend analysis, with a view to improving CCC's defensive position and countermeasures.

CCC operates a 'fair blame' culture in terms of incident management, but investigations of serious incidents can lead to disciplinary action, dismissal, or even legal action.

2.0 Purpose

The purpose of this document is to ensure that all departments within CCC are fully aware of the reporting responsibilities within the organisation and also by 3rd Parties. It will also aim to define the definitions associated with Information Security Management

3.0 Scope

The scope of this document includes the processes involved in reporting Cyber security incidents to NHS Digital and their role in the management of such incidents. It clarifies the roles of all those responsible in the reporting of these incidents. It also outlines the procedures for incident investigation.

4.0 Definitions

In principle, an information security incident is any breach or potential breach of information/data security, either involving physical records or computer-related. Incidents may be internal, external or both, depending on the origin of the perpetrator. Incidents that concern the NHS WAN (N3 and HSCN) are generally computer-related.

4.1 Classification of Incidents

Information security breaches may be classified in terms of the impact they have in terms of:

- **Confidentiality** – that is, incidents related to accidental or intentional leakage of confidential data, passwords and the like to unauthorised persons and organisations.

- **Integrity** – that is, accidental or intentional damage to data, sensitive or otherwise.

- **Availability** – that is, partial or complete disruption of legitimate services such as the processing of data, access to network and Internet resources, reduced service due to inappropriate or malicious network traffic, inappropriate use of network, hardware and software resources, and so on, albeit either purposefully or accidentally generated.

- **Accountability** – this basically refers to responsibility for the welfare of the organisation held by all individuals, to a greater or lesser degree. It includes, for example, breaches of local policies and codes of conduct by personnel at all levels in the organisation which can disrupt business processes.

6.2 Types of Incidents

What constitutes an incident worthy of reporting can vary considerably and it is difficult to include in this document every possible event that should be considered. However, Appendix 2 contains some types of events, which must be reported and investigated.

Further information can be obtained by contacting the IT Security Manager.

5.0 Responsibilities

5.1 Responsibilities of Connected Organisations

Organisations that are connected to The NHS WAN network (N3 or HSCN) are expected to report a range of security incidents to NHS Digital, The National Cyber Security Centre (NCSC) and the C&M STP. For example, where another site is the source of virus, Ransomware, Malware, mailstorms, unauthorised connection attempts, or Denial of Service (DoS) attacks. This enables NHS Digital to take appropriate action to reduce the impact of such incidents on N3 and HSCN, for instance by liaison with or disconnection of organisations that are responsible for security breaches.

CCC is also expected to co-operate with NHS Digital personnel in providing follow-up information, where necessary, to assure NHS Digital that incidents are satisfactorily resolved and that the NHS in general is able to discharge its mandatory responsibilities.

In addition, CCC is required to ensure that all personnel, including temporary workers and consultants, are aware of their responsibilities as individual members of a connected organisation.

5.2 Responsibilities of 3rd Party Organisations

The responsibility for the management of any information security incidents remains with the IT Security Manager and the relevant Trusts Risk Management department. Third Party organisations are required to provide all guidance and assistance to the Trusts Risk Management in investigating incidents involving their systems on Trust premises, and for taking appropriate actions in relation to incidents within their organisation which may impact upon the security of Trust information.

The Service Level Agreement with the third party organisation (NHS Digital) specifies that incidents within the third party organisation which impact the Trust must be notified to the Trust so that they can be entered into the relevant Trust incident reporting system. Details of any investigations and outcomes from those investigations will be provided to the Trust Risk Management department and IT Security Manager.

5.3 Responsibilities of NHS Digital

The NHS Digital Statement of Compliance (SoC) requires the reporting of security incidents to allow for learning and improvement. The new process will allow NHS Digital to:

- Follow the progress of local countermeasures, offer advice and help where requested or appropriate
- Make further investigations where necessary.

Reports are also logged for statistical analysis, in order to improve the Service's defenses and response to security breaches of all kinds.

CCC is further required to ensure compliance with all relevant legislation, mandated policies and standards such as ISO 27001/2 and to this end may need to make further investigations into particular incidents.

5.4 Responsibilities of the Trust

CCC is responsible for implementing and maintaining an incident management system which is capable of:

- Receiving and managing incident reports, carrying out investigations on reports, and notifying of incidents where appropriate.
- Analysing incidents to determine risk trends and to identify where actions to manage risks are required.

CCC are required to train staff in general on reporting of incidents

5.5 Responsibilities of end users

End users are required to:

- Abide by relevant legislation in relation to their work
- Meet the requirements imposed upon any individual member of a connected organisation to meet the collective requirements of that organisation under the NHS Digital Statement of Compliance
- Co-operate with those personnel charged with ensuring that CCC meets its responsibilities. In particular, they are expected to report security incidents through their Trusts Incident Reporting Procedure

6.0 Laws & Regulations

- Access to Health Records Act 1990
- Electronic Communications Act 2000
- Copyright, Designs & Patents Act 1988
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Health & Social Care Act 2001
- Regulation of Investigatory Powers Act 2000
- Data Protection Act 2018
- GDPR 2018

- The Human Rights Act 1998
- Information Security Policy
- Access and Authentication (Application) Policy

7.0 Main Body of Policy

Incidents will be actioned in accordance with the relevant Trusts incident reporting system, and for information-related incidents

- CCC IM&T will ensure that IT incidents are rapidly brought to the attention of the relevant Systems Manager via Datix. This person will ensure that incidents are investigated as appropriate, and that actions required to mitigate any risks are put in place.
- The IT Security Manager is informed, and involved as appropriate in investigation of incidents.
- Where allegations of misconduct by staff are implied, senior management are required to authorise any subsequent investigation, which will be carried out in conjunction with the HR department.

7.1 Documentation of Incidents

The Risk Manager is responsible for maintaining the incident report. Subsequent reports relating to investigations will be filed and appropriately cross referenced to incidents. Actions resulting from investigations will be documented and carried out as specified by the action plan.

The IT Security Manager will bring all security incidents to the attention of the IG Board and will advise on investigations and action plans.

7.2 Collection of Evidence

Where it is necessary, information on an incident will be collected in line with regulations and guidance governing the collection of information, and in a manner, which will ensure the reliability of that information.

7.3 Audit data

Sources of evidential information can be obtained from audit data which is required to be collected for all systems and processes which handle personal or Patient Identifiable Data (PID).

The audit data will reside in approved data silos which comply with the ISMS security standards relating to physical security and access authentication.

Audit data will be kept for the length of time specified with the current NHS Record Retention Policy (Part 2).

Access to the audit data will be available to authorised personnel only.

8.0 Training

None

9.0 Audit

None

10.0 References

None

11.0 Appendices

Appendix 1 - Categories of Incidents

- **Confidentiality** – that is, incidents related to accidental or Intentional leakage of confidential data, passwords and the like to unauthorised persons and organisations. In this context, The Trust is particularly but by no means exclusively concerned to ensure the security and confidentiality of sensitive data such as patient records and personnel records. This type of breach can include attempts to elicit confidential information (or the means of accessing confidential information) by means of network and backdoor Trojans; viruses; theft; social engineering (gaining information by deception) and trespass. It can also include poor practice such as the inappropriate storing of passwords.

- **Integrity** – that is, accidental or intentional damage to data, sensitive or otherwise.

This is particularly applicable to the corruption, unauthorised modification, or partial or complete loss of data, although the latter cases can also be regarded as breaches of availability. This type of breach can include such incidents as: destructive Trojans, viruses and worms; direct inappropriate and unauthorised modification of data by individuals; inducing authorised individuals to take inappropriate action by social engineering (in this context, subverting correct behavior by deception, bribery or coercion); accidental damage to or loss of data.

- **Availability** – that is, partial or complete disruption of legitimate services such as the processing of data, access to network and Internet

resources, reduced service due to inappropriate or malicious network traffic, inappropriate use of network, hardware and software resources, and so on, albeit either purposefully or accidentally generated. This type of breach can include: Denial of Service attacks such as Ransomware or packet flooding; systems failure or software failure; and inappropriate behavior such as the forwarding of chain letters and other dysfunctional content - though some of these breaches can also be seen as breaches of accountability. Lost or forgotten passwords may be seen as an example of a breach of availability and are one of the most common subjects of help desk calls. However, it is generally of limited use to report these on a case-by- case basis, though large numbers of these incidents may sometimes point to a significant shortcoming in an organisation's procedures.

- **Accountability** – this basically refers to responsibility for the welfare of the organisation held by all individuals, to a greater or lesser degree. Accountability - related threats often cause disruption of business processes by inappropriate behavior of personnel at all levels, such as breaches of local policies and codes of conduct. Breaches of this type may include: mismanagement or inappropriate use of resources; incompetence; inappropriate personal behavior. Inappropriate storing of passwords, thus subverting their use as a means of identifying the probable source of a breach of confidentiality, is also a common breach of accountability.

Appendix 2 - Examples of Types of Incidents

(a) Internet misuse & abuse

Breaches of Internet & E-mail Usage Policy, including, but not limited to:

i. Pornography or other illegal, morally unacceptable, or unethical traffic

ii. Commercial traffic inappropriate to the NHS workplace, such as advertising or operating home businesses

iii. Unauthorised exchange of software, images, documents, music and other prohibited material (software piracy, breach of copyright and license agreements, and so on).

iv. Material in breach of local or NHSnet policy, such as malicious code or programs, or activity designed to undermine the security of Internet sites.

v. Connecting to or otherwise being in contact with inappropriate newsgroups and forums.

Vi. Activity which may threaten the internet either directly or as a result of generated traffic, such as:

- Spamming (The act of distributing the electronic equivalent of junk mail to many recipients at one time, either in newsgroups, or by email).

- Denial of Service (DoS) attacks, including attempts to disrupt services with mail bombs, packet flooding, or similar activity.

vii. Use for non-NHS purposes contrary to the Trust's policy on the use of the Internet.

(b) E-mail misuse & abuse:

Breaches of email policy, including but not limited to:

i. Phishing (fraudulent mails requesting cash or services), or offensive or threatening mail, including racial remarks or comments (received or sent).

ii. Misrepresentation by the user of NHS business, or the carrying out of non–NHS business, including email usage for political activity.

iii. Offensive or threatening mail, including racial remarks or comments (received or sent).

iv. Bulk mail – including:

- Chain mail (the electronic equivalent of the chain letter)
- UCE (Unsolicited Commercial Email), UBE (Unsolicited Bulk Email) and other manifestations of what is now described as spam
- Mail bombing and subscription bombing (attacks on email account holders by bombarding them directly with unwanted mail, or indirectly by subscribing them to high volume lists).

(c) Misuse & Abuse of *(N3):*

Including:

i. Distribution of inappropriate images or text.
ii. Inappropriate messages on bulletin discussion

boards

iv. Installation or distribution of unlicensed

software

v. Social Engineering (the obtaining of restricted information i.e. Passwords, Patient Identifiable information, etc, by posing as engineers, relatives, doctors, etc.)

(d) Breaches of Security:

Including:

Breaches using information recording or transfer devices, including pagers, emails, faxes, mobile devices electronic or manual file transfers, voice messages.

Inappropriate management for the disposal of equipment. Confidential information should be removed from IT equipment, and the removal will be verified before control is passed to a third party organisation. Where this is not possible, there will be an agreement in place with that organisation to ensure confidentiality and security of the information.

Loss of, or theft of, confidential information. Such loss must be reported immediately as an incident. Where theft is suspected, then this will be reported to Derry Sinclair, LSMS, on ext 5288. If fraud is suspected, this should be reported to the Trusts anti-fraud specialist on 0151 285 4770.

(e) Virus, Worm and Ransomware Infection:

Ransomware, Worms, viruses, Trojans and other malicious software must be reported using the incident reporting forms. Instances of email worms should be reported to the Service Desk with particular urgency, since this enables CCC IM&T to take action to restrict its impact as well as logging the incident. CCC IM&T needs reports of viruses and worms detected at entry; incidents where a virus has actually infected systems without detection; may cause incidents within other organisations implicating the Trust as the source of a virus.

Virus hoax reports also need to be reported: the impact of hoax-related traffic on the network can be considerable.

Serious untoward incidents affecting information security (SUI's) will be reported to NHS Digital as a matter of urgency.