NHS
Mersey Care
NHS Foundation Trust

Community and Mental Health Services

TRUST-WIDE NON-CLINICAL DOCUMENT

User Account Investigation Security Standard

Standard Number:	**SS04**
Scope of this Document:	**All Staff**
Recommending Committee:	**Joint Information Governance & Caldicott Committee**
Approving Committee:	**Joint Information Governance & Caldicott Committee**
Date Ratified:	**February 2020**
Next Review Date (by):	**December 2021**
Version Number:	**Version 2**
Lead Executive Director:	**Executive Director of Finance**
Lead Author(s):	**IM&T Security Manager**

TRUST-WIDE NON-CLINICAL DOCUMENT

2018 – Version 2

Striving for perfect care and a just culture

TRUST-WIDE NON-CLINICAL DOCUMENT

USER ACCOUNT INVESTIGATION SECURITY STANDARD

Further information about this document:

Document name	**User Account Investigation Security Standard SS04**
Document summary	**Trust Standard On the use of Internet and email**
Author(s) Contact(s) for further information about this document	**Mark Williams** **IM&T Security Manager** **Telephone: 0151 472 4031** **mark.williams@imerseyside.nhs.uk**
Published by Copies of this document are available from the Author(s) and via the trust's website	**Mersey Care NHS Foundation Trust** **Trust Headquarters** **V7 Building** **Kings Business Park** **Prescot** **L34 1PJ** **Trust's Website www.merseycare.nhs.uk**
To be read in conjunction with	**IM&T Security Standard IT02**
This document can be made available in a range of alternative formats including various languages, large print and braille etc	

Version Control:

		Version History:
Draft	Executive Director of Finance / Deputy Chief Executive / Senior Information Risk Owner (SIRO) / Medical Director / Cadicott Guardian	December 2015
Review	Informatics Merseyside ITSecurity	December 2017
Version 2		February 2020

SUPPORTING STATEMENTS –

Failure to adhere to the acceptable usage outlined in this Policy will be deemed as misconduct, any required deviation from these guidelines must be reviewed on an individual basis at the trusts discretion.

This document should be read in conjunction with the following statements:

SAFEGUARDING IS EVERYBODY'S BUSINESS

All Mersey Care NHS Foundation Trust employees have a statutory duty to safeguard and promote the welfare of children and adults, including:

- being alert to the possibility of child/adult abuse and neglect through their observation of abuse, or by professional judgement made as a result of information gathered about the child/ adult;
- knowing how to deal with a disclosure or allegation of child/adult abuse;
- undertaking training as appropriate for their role and keeping themselves updated;
- being aware of and following the local policies and procedures they need to follow if they have a child/ adult concern;
- ensuring appropriate advice and support is accessed either from managers, *Safeguarding Ambassadors* or the trust's safeguarding team;
- participating in multi-agency working to safeguard the child or adult (if appropriate to your role);
- ensuring contemporaneous records are kept at all times and record keeping is in strict adherence to Mersey Care NHS Foundation Trust Standard and procedures and professional guidelines. Roles, responsibilities and accountabilities, will differ depending on the post you hold within the organisation;
- ensuring that all staff and their managers discuss and record any safeguarding issues that arise at each supervision session

EQUALITY AND HUMAN RIGHTS

Mersey Care NHS Foundation Trust recognises that some sections of society experience prejudice and discrimination. The Equality Act 2010 specifically recognises the *protected characteristics* of age, disability, gender, race, religion or belief, sexual orientation and transgender. The Equality Act also requires regard to socio-economic factors including pregnancy /maternity and marriage/civil partnership.

The trust is committed to equality of opportunity and anti-discriminatory practice both in the provision of services and in our role as a major employer. The trust believes that all people have the right to be treated with dignity and respect and is committed to the elimination of unfair and unlawful discriminatory practices.

Mersey Care NHS Foundation Trust also is aware of its legal duties under the Human Rights Act 1998. Section 6 of the Human Rights Act requires all public authorities to uphold and promote Human Rights in everything they do. It is unlawful for a public authority to perform any act which contravenes the Human Rights Act.

Mersey Care NHS Foundation Trust is committed to carrying out its functions and service delivery in line the with a Human Rights based approach and the FREDA principles of **F**airness, **R**espect, **E**quality **D**ignity, and **A**utonomy

Contents

1 PURPOSE AND RATIONALE

1.1 **Purpose** –The purpose of this Standard is to both control and record access to user account information when supporting Human Resources department with investigations. This standard describes how control will be applied by the Investigation process and completion of the Chain of Custody document.

1.2 This Standard forms a key component of Mersey Care NHS Foundation Trust's overall information security management framework and should be considered alongside the Trust's IM&T Security Policy IT02 and more detailed information security documentation including, system level security policies, security guidance and procedures.

1.3 This Standard is based on the principles identified within the NHS Code of Practice for Information Security and other related NHS policy and may be periodically updated as standards and guidance changes.

1.4 This Standard applies all staff including contractors and voluntary personnel

1.5 **Rationale** –In order to help maintain the security and integrity of investigative access to staff systems.

1.6 It is imperative that user data – whether stored on a home drives, within a personal mailbox or as notes on a clinical systems, are available to support Human Resource disciplinary procedures.

1.7 Access to the data of an existing user must be requested, recorded, justified and identified. All correspondence and documentation must be included within the Chain of Custody document and will have several layers of authorisation including Service Director and HR investigating officer approval.

1.8 The IT Security team will liaise with the investigation requestor, service director and technical support teams throughout the investigation process, but will not engage with the HR disciplinary procedure.

1.9 The Trust recognises the value of information contained within their computer systems and will not tolerate unauthorised use. It is a criminal offence for an unauthorised person to attempt to access a system or information within systems or to attempt to exceed the computer facilities and privileges granted to them and the Trust will prosecute those committing any such offence as covered by the Computer Misuse Act 1990.

2 OUTCOMES AND OBJECTIVES

2.1 The aims and objectives of this Security Standard are as follows:

(a) To ensure that all staff are aware of the investigation process with regards to user account access Chain of Custody documentation.

(b) To ensure that staff use this standard as guidance when requesting access to user account data, whether stored on a home drive, personal mailbox or clinical system.

(c) To ensure the necessary parties understand their responsabilities relating to user access investigations when assisting with Human Resources with disciplinary procedures.

(d) To highlight the importance of having accurate and up to date Chain of Custody documentation as not having this available can have serious implications and consequences for the Trust.

3 SCOPE

3.1 This standard applies to everyone who owns or accesses Trust data.

3.2 All Trust employees whilst engaged in work for the Trust at any location, on any computer or internet connection should be aware that their data, correspondence with any colleagues, service users and third parties, as well as any relating clinical notes can all be subject to a review should a disciplinary request arise.

3.3 Any other use by Trust employees which identifies the person as a Trust employee or which could bring the Trust into disrepute on any computer or internet connection.

3.4 Other persons working for/with the Trust, persons engaged on Trust business or persons using Trust equipment and networks and anyone else who has been granted access to use of IT facilities over the Trust IT network.

4 RESPONSIBILITIES

4.1 Management are responsible for ensuring all staff within their department are aware of and understand the implications of this Standard.

4.2 Managers are responsible for ensuring that the Service Desk are aware of the User Account Investigation process in order to log an investigation request correctly.

4.3 Service Desk engineers are responsible for recording the initial request, accepting basic details of the request before assigning an incident to Security. Further information will be recorded by the Security team.

4.4 Service managers are responsible for registering the initial request with the Service Desk and completing the User Investigation Request form.

4.5 Human Resource investigations officers are responsible for completing the HR Investigation Officer Consent form. Once completed, the consent form authorises IT Security to carry out the data retrieval and subsequent investigation.

4.6 IT Security are responsible for liaising with all necessary parties throughout the investigation process as well as creating and maintaining the Chain of Custody document.

5 INVESTIGATION PROCESS

5.1 Where a new investigation request is submitted, IT Security have introduced a robust procedure to ensure all requests are recorded, thoroughly documented, and completed in accordance with the Chain of Custody process. This process is as follows:

a) A service manager contacts the Service Desk to initiate a new Account Investigation:

1) The Service Desk engineer records and opens new request, basic details are noted such as incident owner contact information, and adds account access investigation in job summary, before being assigned to IT Security team queue.

2) IT Security team create Chain of Custody document noting IND reference number and emails attached Investigation Criterion form to the Service Manager / Investigation Requestor.

3) After sending the Investigation Criterion form, IT Security then update Chain of Custody document noting the date, time and method document sent.

b) The Service Manager / Investigation Requestor completes the Investigation criterion form and returns to IT Security:

1) IT Security receives and reviews Investigation Criterion form updating the Chain of Custody document accordingly.

2) After reviewing form, IT Security will either return form to Investigation Requestor / Service Manager to add additional information, or if criterion form completed correctly will then Contact Service Director to authorise investigation taking place. In either scenario, IT Security will update the Chain of Custody.

3) Service Director reviews Investigation request form returned by Security then replies to Security to cancel or approve Investigation:

c) IT Security receive authorisation from Service Director and update Chain of Custody document, next:

1) IT Security updates Service Desk incident and assigns to Tech Support, detailing which data needs to be restored to Investigations area

2) Tech Support team retrieve necessary data and copy to Investigations area, informing IT security once data is available. Incident reference is then updated re-assigned back to the IT Security team.

3) IT Security compares data copied to Investigation area with information provided within Investigation Criterion Form. Chain of Custody document is again updated once this step completed.

4) After data is reviewed, IT Security then inform the Investigation Requestor as to whether any data appropriately matches investigation criterion form.

d) The requestor informs IT security of the identity of the HR Investigation Officer initiating the next phase of the process, which is as follows:-

1) IT Security send consent form to HR Investigation Officer and update Chain of Custody document.

2) HR Investigations officer completes and returns Investigation Consent form and returns to IT Security. Consent form details are added to Chain of Custody document.

3) IT Security will transfer all relevant data over to the HR Investigations officer, this will be within a secure area only accessible by the HR Investigations officer for an agreed period of time.

4) HR Investigation Requestor then reviews the data for the agreed period then informs IT Security when investigation is complete.

5) HR Investigation officer specifies whether or not data within the Investigation area is permanently deleted or retained as evidence for use in subsequent disciplinary procedures.

6) IT Security add final details to Chain of Custody document which is then saved within the investigations area. Completing the Investigation, IT Security then resolve the incident reference.