Creating Tomorrow Trust

Information Risk Management Policy 2023

About this document:

Purpose

Information that is collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption.

Information may be put at risk by poor education and training, and the breach of security controls.

Information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation as well as possible judgements being made against the Trust.

This high-level Information Risk Management Policy sits alongside the Information Security Policy and Data Protection Policy to provide the high-level outline of and justification for the Trust's risk-based information security controls.

Complied by: Ali Jones	**Date: 10th January 2023**
Committee:	**Date agreed by Trustees:**
Review Cycle: (annually, 2 years, 3 years) **2 Years**	**Review Date:** **Jan 2025**

Wellbeing in our Trust

The responsibility for managing an information risk assessment can be challenging and so this document aims to set out procedures to be followed to minimize what can be difficult process.

We are all affected by poor physical and mental health at times during our lives and it is important the appropriate support is available in a timely manner.

Health and wellbeing is everyone's responsibility and we encourage an open and honest culture whereby anyone can discuss any issues they may have.

The Trustees of Creating Tomorrow take the health and wellbeing of all employees seriously and are committed to supporting our staff. The Trustees ensure that support for staff is available through:

- Effective line management
- Commitment to reducing workload
- Supportive and professional working environments
- Employee support programs
    - Health Assure (confidential counselling support available through Perkbox account).
    - Education Support: telephone number 08000 562561 or website www.educationsupport.org.uk

1. OBJECTIVES

The Trust's information risk management objectives are that:

- Our information risks are identified, managed and treated according to an agreed risk tolerance
- Our physical, procedural and technical controls are agreed by the information asset owner
- Our physical, procedural and technical controls balance user experience and security
- Our physical, procedural and technical controls are cost-effective and proportionate.

2. SCOPE

The Information Risk Management Policy and its supporting controls, processes and procedures apply to all information used at the Trust, in all formats.

This includes information processed by other organisations in their dealings with the Trust.

The Information Risk Management Policy and its supporting controls, processes and procedures apply to all individuals who have access to Trust information and technologies, including external parties that provide information processing services to the Trust.

3. COMPLIANCE

Failure to comply with this procedure could result in action in line with the Trust's Disciplinary Procedure or Capability Procedure.

Any prohibited use which is deemed to be in contravention of the law and/or which involves the intentional access, creation, storage or transmission of material which may be considered indecent or obscene will be regarded as an act of gross misconduct on the part of staff. This would also qualify as an act for which students may be expelled under the student disciplinary procedure.

Compliance checks will be undertaken by the Trust's Information Governance functions. The results of compliance checks, their risk assessment and their remediation will be managed by the Information Security Board.

4. REVIEW

A review of this policy will be undertaken by the information security team annually or more frequently as required and will be approved by the Information Governance Board.

There are other Trust policies which will apply when you access Trust systems, including the Trust's Data Protection Policy (and users should complete the Trust's mandatory UK GDPR training).

5. POLICY STATEMENT

Information Risk Assessment is a formal and repeatable method for identifying the risks facing an information asset. It is used to determine their impact and identify and apply controls that are appropriate and justified by the risks.

It is the Trust's policy to ensure that information is protected from a loss of:

- Confidentiality – information will be accessible only to authorised individuals
- Integrity – the accuracy and completeness of information will be maintained
- Availability – information will be accessible to authorised users and processes when required
- Risk assessment
- Threats
- Vulnerabilities
- Risk Register
- Risk Treatment
- Roles and Responsibilities
- Risk Appetite and Tolerance

5a. RISK ASSESSMENT

Risk assessments must be completed with access to and an understanding of:

- The Trust's business processes
- The impact to the Trust of risks to business assets
- The technical systems in place supporting the business

The legislation to which the Trust is subject

- Up-to-date threat and vulnerability assessments

A risk assessment exercise must be completed at least:

- For every new information-processing system
- Following modification to systems or processes which could change the threats or vulnerabilities
- Following the introduction of a new information asset
- When there has been no review in the previous three years
- A risk score is calculated from Likelihood x Impact Level, consistent with the Trust's high level Risk Management Policy.

5b. THREATS

The Trust will consider all potential threats applicable to a particular system, whether natural or human, accidental or malicious.

The Trust will reference Annex C of the ISO 27005 standard to aid with threat identification.

Threat information will be obtained from specialist security consultancies, local and national law enforcement agencies and security services, and contacts across the sector and region.

It is the responsibility of the information manager to maintain channels of communication with appropriate specialist organisations.

5c. VULNERABILITIES

The Trust will consider all potential vulnerabilities applicable to a particular system, whether intrinsic or extrinsic.

The Trust will reference Annex D of the ISO 27005 standard to aid with vulnerability identification.

Vulnerability information will be obtained from specialist security consultancies, local and national law enforcement agencies and security services, technology providers and contacts across the sector and region.

It is the responsibility of the Information Manager to maintain channels of communication with appropriate specialist organisations.

5d. RISK REGISTER

The calculations listed in the risk assessment process will form the basis of a risk register.

All risks will be assigned an owner and a review date.

The risk register is held, with access controlled by the Information Security team.

5e. RISK TREATMENT

The risk register will include a risk treatment decision. The action will fall into at least one of the following categories:

Tolerate the risk – where the risk is already below the Trust's risk appetite and further treatment is not proportionate

Treat the risk – where the risk is above the Trust's risk appetite but treatment is proportionate; or where the treatment is so simple and cost effective that it is proportionate to treat the risk even though it falls below the Trust's risk appetite

Transfer the risk – where the risk cannot be brought below the Trust's risk appetite with proportionate treatment but a cost-effective option is available to transfer the risk to a third party

Terminate the risk – where the risk cannot be brought below the Trust's risk appetite with proportionate effort/resource and no cost-effective transfer is available

The Information Security team in collaboration with the Information Asset Owner will review Medium and Low risks and recommend suitable action.

The Information Governance Board in collaboration with the Information Asset Owner will review High risks and recommend suitable action.

In the event that the decision is to treat, then additional activities or controls will be implemented via a Risk Treatment Plan.

5f. ROLES AND RESPONSIBILITIES

The Chair of the Information Governance Board has accountability to the CEO for managing information risk.

They will direct the information risk appetite for the Trust and review the information risk register. They will be involved in assessing and reviewing High risks via the Information Governance Board.

The information manager is responsible to the Chair of the Information Governance Board for managing the risk assessment process and maintaining an up-to-date risk register. The Information Security team will conduct risk assessments and recommend action for Medium and Low risks, where these can be clearly defined in terms of the Trust's risk appetite.

The Information Governance Board is responsible for assessing and reviewing High risks, and will have visibility of the risk register.

Information Asset Owners and Information Asset Managers must be responsible for agreeing and implementing appropriate treatments to risks under their control. They must also take an active role in identifying and reporting new risks.

5g. RISK APPETITE AND TOLERANCE

The Trust has agreed a series of risk appetite statements.

While not exhaustive, these give a good overview of the Trust's desire to pursue or tolerate risk in pursuit of its business objectives.

The risk appetite statements give the Information Security team, and the Information Governance Board, a framework within which to conduct risk assessments and make recommendations for appropriate treatments.