NETWORK AND INFORMATION SECURITY POLICY

Approval Date	October 2024
Policy Owner	Director of Operations
Adopted by Trust Board	Ratified by the Trust Board November 2024
Review Date	October 2025

CONTENTS

Section Page No.

1. INTRODUCTION ..... **Error! Bookmark not defined.**
2. PURPOSE ..... **Error! Bookmark not defined.**
3. SCOPE ..... **Error! Bookmark not defined.**
4. NETWORK SECURITY ..... **Error! Bookmark not defined.**
   - 4.1 Access Controls: 3
   - 4.2 Firewalls and Intrusion Detection/Prevention Systems: 3
   - 4.3 Network Segmentation: 3
   - 4.4 Wireless Network Security: 4
   - 4.5 Endpoint Security: 4
   - 4.6 Patch Management: 4
   - 4.7 Data Encryption: 4
   - 4.8 Device Management: 4
5. USER SECURITY ..... **Error! Bookmark not defined.**
   - 5.1 User Authentication: 4
   - 5.2 User Training and Awareness: 4
   - 5.3 Account Management: 5
6. INCIDENT RESPONSE & REPORTING ..... **Error! Bookmark not defined.**
   - 6.1 Incident Response Plan: 5
   - 6.2 Reporting: 5
7. MONITORING AND LOGGING ..... **Error! Bookmark not defined.**
   - 7.1 Network Monitoring: 5
   - 7.2 Log Management: 5
8. PHYSICAL SECURITY ..... **Error! Bookmark not defined.**
   - 8.1 Data Centre Security: 6
   - 8.2 Device Physical Security: 6
9. COMPLIANCE & REGULAR AUDITS ..... **Error! Bookmark not defined.**
   - 9.1 Compliance Monitoring: 6
   - 9.2 Security Audits: 6
10. POLICY REVIEW UPDATES ..... **Error! Bookmark not defined.**
    - 10.1 Policy Review: 6
    - 10.2 Policy Communication: 6
11. RESPONSIBILITIES & ACCOUNTABILITY ..... **Error! Bookmark not defined.**
    - 11.1 Responsibilities: 7
    - 11.2 Accountability: 7

POLICY HISTORY ..... **Error! Bookmark not defined.**

1. INTRODUCTION

This Network and Information Systems Security Policy, with a focus on attribute-based access control, least privilege principles, and physical restrictions, is integral to Reach South Academy Trust's overall security strategy. Regular training, monitoring, and updates will maintain a secure and resilient network and information systems environment.

This policy reflects the design and usage principles of the IT systems and related systems within Reach South Academy Trust.

2. PURPOSE

This Network and Information Systems Security Policy is designed to provide comprehensive guidelines and procedures to ensure the confidentiality, integrity, and availability of Reach South Academy Trust's network and information systems.

3. SCOPE

This policy applies to all personnel, systems, and devices connected to Reach South Academy Trust's network and information systems.

4. NETWORK SECURITY

4.1 Access Controls:

The Trust’s approach is to have attribute-based access control (ABAC) to define and manage access permissions based on job responsibilities, ensuring that each user has the minimum access necessary for their role. Additional access permissions will require justification and be time limited.

4.2 Firewalls and Intrusion Detection/Prevention Systems:

The Trust deploys robust firewalls and intrusion detection/prevention systems to monitor and control network traffic. These systems play a crucial role in identifying and preventing unauthorized access and malicious activities. These are deployed at each internet facing point.

4.3 Network Segmentation:

The Trust employs network segmentation to compartmentalise different segments of the network. This not only enhances security but also mitigates the impact of potential security breaches by restricting lateral movement.

4.4 Wireless Network Security:

The Trust secures wireless networks with strong encryption protocols, strong credentials, and regularly monitor for any unauthorised access points. Access to the primary wireless will be restricted to managed devices. Segmented guest wireless will be provided for authorised use on unmanaged devices.

4.5 Endpoint Security:

The Trust implements attribute-based endpoint security measures, including antivirus software, endpoint detection and response (EDR) tools, and regular software updates to protect against malware and other security threats.

4.6 Patch Management:

The Trust has implemented a comprehensive patch management process to ensure that operating systems, applications, and firmware are regularly updated with the latest security patches. It has also applied the principle of least privilege to limit the installation of software to authorized personnel.

4.7 Data Encryption:

The Trust enables encryption for sensitive data both in transit and at rest to protect against unauthorised access. Encryption is applied selectively based on the sensitivity of the data and the requirements of applicable regulations. Where possible this does not require user intervention, with training provided where user intervention is necessary to ensure compliance.

4.8 Device Management:

The Trust implements the principle of least privilege in device management, configuring systems and devices to grant users only the minimum level of access required to perform their duties. This includes not providing local admin accounts to staff.

5. USER SECURITY

5.1 User Authentication:

The Trust implements role-based authentication mechanisms, such as multi-factor authentication (MFA), to ensure secure access to network resources, with higher risk activities being subject to stronger controls.

5.2 User Training and Awareness:

The Trust provides regular training to users on security best practices, social engineering awareness, and the importance of safeguarding credentials, and ensure that users

understand the principle of least privilege and their responsibility to report any suspicious activity.

Users are responsible for completing all requested training to the appropriate level.

5.3 Account Management:

The Trust applies the principle of least privilege in account management, ensuring that users are granted access only to the resources necessary for their specific roles. The trust implements procedures for timely creation, modification, and removal of user accounts, based on a master source.

6. INCIDENT RESPONSE & REPORTING

6.1 Incident Response Plan:

The Trust has developed and maintains an incident response plan outlining the procedures to be followed in the event of a security incident. This defines roles and responsibilities for incident response teams based on ABAC.

6.2 Reporting:

The Trust mandates the prompt reporting of any suspected or confirmed security incidents to the designated IT security contact.

Reporting and notification of incidents to roles/individuals within the trust is defined in the incident response and cyber response plans, ensuring that the right individuals are notified and involved based on their roles.

7. MONITORING & LOGGING

7.1 Network Monitoring:

The Trust implements continuous network monitoring to detect and respond to abnormal activities and potential security threats. Monitoring alerts and reports are tailored based on ABAC to ensure relevant stakeholders are informed.

7.2 Log Management:

The Trust has established centralised log management to collect, store, and analyse logs from network devices, servers, and applications. The Trust defines access controls for log files to ensure that only authorized personnel have access to sensitive information.

8. PHYSICAL SECURITY

8.1 Data Centre Security:

The Trust ensures physical security measures, including attribute based access controls (ABAC), surveillance, and environmental controls, are in place to protect data centres and network infrastructure. The Trust has implemented ABAC for physical access to data centre facilities.

8.2 Device Physical Security:

The Trust has implemented measures to secure physical access to servers, network devices, and other critical infrastructure components. It uses ABAC to restrict access to authorized personnel only.

9. COMPLIANCE & REGULAR AUDITS

9.1 Compliance Monitoring:

The Trust regularly monitors and assesses compliance with security policies, industry standards, and relevant regulations. It has implemented ABAC in compliance monitoring, assigning responsibility for compliance checks based on job roles.

9.2 Security Audits:

The Trust conducts regular security audits and assessments to identify vulnerabilities and ensure the effectiveness of security controls. It has assigned roles based on ABAC for audit preparation, execution, and remediation.

10. POLICY REVIEW & UPDATES

10.1 Policy Review:

This Network and Information Systems Security Policy will be subject to review regularly to address emerging threats, technological advancements, and changes in the organisation's infrastructure.

10.2 Policy Communication:

The Trust will communicate updates to all relevant personnel and provide training as necessary to ensure awareness and compliance.

11. RESPONSIBILITIES AND ACCOUNTABILITY

11.1 Responsibilities:

The Trust's Director of Operations has overall responsibility for the implementation and enforcement of this policy. The Trust's Head of ICT Services and Infrastructure and ICT Services Manager is accountable for specific aspects of security and day to day implementation of this policy.

11.2 Accountability:

Failure to comply with this policy can result in disciplinary action in line with Reach South Academy Trust's policy.

POLICY HISTORY

Date	Summary of change	Contact	Policy Implementation Date	Review Date
20/09/2024	Policy creation	Nick Roe	Pending Committee Approval October 2024	October 2025