Version number:	2.0
Consultation Groups	Information Governance Steering Group, Digital Board and Key Leads
Approved by (Sponsor Group)	Information Governance Steering Group, Digital Board and Key Leads
Ratified by:	Quality Committee
Date ratified:	30th August 2023
Name of originator/author:	Michael Loughlin
Executive Director lead:	Phillipa Graves
Implementation Date:	September 2023
Last Review Date	September 2024
Next Review date:	September 2025

Services	**Applicable**
Trust wide	X
Mental Health and LD	
Community Health Services	

East London
NHS Foundation Trust

Version Control Summary

Version	Date	Author	Status	Comment
1.0	30/08/2023	Octavius Max-Lino	DRAFT	Initial Draft
2.0	28/08/2024	Octavius Max-Lino	Final	Reviewed & Updated

Purpose

This policy establishes the framework for conducting regular audits and ensuring compliance with internal policies, regulatory requirements, and industry standards within the EFLT. This policy aims to protect sensitive patient data, maintain the integrity of healthcare services, and ensure the organisation adheres to legal and regulatory obligations.

Scope

This policy applies to all EFLT staff, contractors, and third-party service providers who manage or use EFLT information systems and assets.

Policy Statement

The EFLT is committed to maintaining a robust audit and compliance program to ensure that all information systems, processes, and practices adhere to established security policies, regulatory requirements, and industry standards. Periodic audits and reviews will be conducted to verify compliance and identify areas for improvement.

Key Components

1. Audit Planning and Scheduling

- Annual Audit Plan: Develop an annual audit plan based on risk assessments, regulatory requirements, and organizational priorities.

- Audit Frequency: Determine the frequency of audits for different systems and processes based on their criticality and risk level.

2. Compliance Reviews

- Regular Audits: Conduct regular audits to verify compliance with EFLT policies, regulatory requirements (e.g., GDPR, Data Protection Act), and industry standards (e.g., ISO 27001).

- Standard Build Compliance: Include periodic standard build compliance reviews to ensure all systems adhere to approved configurations and security baselines.

3. Documentation and Reporting

- Audit Findings: Document the findings of all audits, including any deviations from policies and corrective actions taken.

- Compliance Reports: Prepare comprehensive compliance reports and distribute them to relevant stakeholders, including IT management, the Information Security Officer (ISO), and senior leadership.

4. Remediation and Follow-up

- Corrective Actions: Implement corrective actions to address any non-compliance issues identified during audits.

- Follow-up Audits: Conduct follow-up audits to verify the effectiveness of remediation efforts and ensure sustained compliance.

5. Continuous Improvement

- Feedback Loop: Use insights from audit findings to improve policies, procedures, and standard configurations.

- Policy Updates: Regularly review and update audit and compliance policies to reflect changes in regulatory requirements, industry standards, and organizational needs.

6. Training and Awareness

- Staff Training: Provide regular training to staff on audit and compliance policies, procedures, and best practices.

- Awareness Programs: Conduct awareness programs to promote a culture of compliance within the organization.

7. Third-Party Audits

- Vendor Compliance: Ensure that third-party service providers comply with EFLT policies and regulatory requirements.

- Contractual Obligations: Include audit and compliance requirements in contracts with third-party service providers.

Responsibilities

- Digital Team: Develop and execute the annual audit plan, conduct audits, document findings, and report results.

- Chief Information Security Officer (CISO): Oversee the audit process, ensure alignment with security policies, and address compliance issues.

- Network/Infrastructure/Desktop Team: Support audit activities, remediate identified issues, and ensure systems meet compliance requirements.

- Department Heads and Managers: Ensure their teams comply with audit findings and implement necessary changes.

- Third-Party Providers: Comply with EFLT audit and compliance requirements and support audit activities as needed.

Compliance

Compliance with this policy is essential to maintain the security and integrity of EFLT information systems and protect sensitive patient data.

Review and Updates

This policy will be reviewed annually or as needed to ensure it remains effective and aligned with the EFLT's needs and regulatory landscape.