Governance Policy: System Access Logging & Auditability

Healthcare Manufacturing Division

1. Purpose

This policy ensures that all system access within the Healthcare Manufacturing Division is logged, auditable, and reviewable to support regulatory compliance, security monitoring, and incident response.

2. Scope

This policy applies to all internally developed software systems, third-party platforms, users, and system-to-system interactions involved in manufacturing, quality, or supply chain workflows.

3. Policy Requirements – Authentication and Authorization Logging

All authentication and authorization decisions must be logged, including successful and failed authentication attempts, authorization decisions, and system-to-system credential usage. Each log entry must include a timestamp, identity, action, decision outcome, and correlation identifier.

4. Log Integrity

Access logs must be tamper-resistant, written in near real-time, and protected from unauthorized modification or deletion. Logs must not contain sensitive secrets or regulated data.

5. Log Retention

Access logs must be retained for a minimum of 365 days and support internal audits, regulatory inspections, and security investigations.

6. Audit Access

Authorized audit personnel must be able to query, export, and review access logs by user, system, or time range.

7. Roles and Responsibilities

Platform Engineering implements logging mechanisms. Product Owners ensure compliance is in scope. Compliance and Audit validate adherence.

8. Compliance and Enforcement

Failure to comply may result in audit findings, system approval delays, and increased regulatory risk.

9. Review and Updates

This policy will be reviewed annually or upon significant regulatory or system changes.

10. Effective Date

Effective Date: January 1, 2026
Policy Owner: Director of Compliance, Healthcare Manufacturing