COMPLIANCE POLICY

Table of Contents

1. Purpose

The purpose of this policy is to ensure compliance with the organization's information and security policy.

2. Scope

This Policy supports the implementation of the sub-control objectives relating to Compliance, Compliance with Legal and Contractual Requirements, and Information Security.

3. Objectives

The objectives of this policy are:

- To avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security and or any security requirements.
- The Board shall conduct audits at planned intervals to ensure that information security is implemented and operated in accordance with organizational policies and procedures.

4. Governing laws and regulations

Guidance	Section
ISO27001:2013	A.18 (A18.1 & A18.2)

5. Cryptography controls

The sub-controls in this policy are designed to reduce the impact of the following threats, as defined in the **Information Security Risk Management Policy**

Threat Number	Organizations Commonly Identified Threats
T8	Communications intercepted en route
T9	Introduction of damaging or disruptive software or Malicious code (e.g. malware)
T10	Phishing/Social Engineering
T11	Breach of legislation, Privacy/Regulation issue
T12	Accidental misrouting of data, wrong recipients

T13	Inadequate or absent audit trail
T14	Network connection failures
T15	Infrastructure technical failure
T16	Environmental failure like Loss of Electricity
T17	System or network software failure
T18	Supplier withdraws a key product in the solution or end of life
T19	Key supplier becomes insolvent
T20	Supply chain cyber attack
T21	Act of Terrorism
T22	DDoS Attack for Public Facing services

6. Policy Statement

6.1 Identification of applicable legislation and contractual requirements

The Information Governance and IT Compliance Teams maintain a register of relevant legislative, statutory, and regulatory requirements. These are referenced in policy.

6.2 Intellectual Property Rights

Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements related to intellectual property rights and the use of proprietary software products.

6.3 Protection of Records

Records shall be protected from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with legislative, regulatory, contractual, or business requirements as defined by Board Procedures.

6.4 Privacy and Identification of personally identifiable information

Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

6.5 Regulation of cryptographic controls

Cryptographic controls shall be used in compliance with the Cryptographic Control Policy supporting all relevant agreements, legislation, and regulations.

7.COMPLIANCE: INFORMATION SECURITY REVIEWS

7.1 Independent review of information security

Independent review of the approach to managing information security and its implementation shall be carried out through internal and external audits and independent assurance.

7.2 Compliance with security policies and standards

Managers shall regularly review the compliance of the control areas within their area of responsibility with the appropriate security policies, standards, and any other security requirements.

7.3 Technical Compliance Review

Independent review of the approach to managing information security and its implementation shall be carried out through internal and external audits, and independent assurance.

7.4 Performance Evaluation

Security performance will be reported to the Information Governance Steering Group and the SIRO.

7.5 Assurance

There will be a regular and independent technical assurance of the security measures that are in place to protect networks and information systems. Proportionate action plans will be developed to address identified deficiencies.

8. Non-Compliance

In the event of a breach or violation of Health Care Credit Union Information Security Compliance policy, the compliance team under the direction of CISO/CSO will initiate corrective measures including restricting access to services and initiating disciplinary actions against employees, vendors, contractors, or any other related party.

9. Exceptions

Exceptions to this policy can be granted in extraordinary circumstances after the written approval of CIO.

10.Revision History

Version ID	Date of Change	Author	Rationale