SUPPLIER RELATIONSHIPS SECURITY POLICY

Policy Date: 04/10/2023

1. Purpose

This policy ensures the protection organization's assets that are accessible by suppliers, and maintain an agreed level of security of and service delivery in line with the supplier agreements.

2. Scope

This Supplier relationships Security Policy applies to all business processes and data, information systems, as well as components, personnel, and physical areas of Health Care Credit Union which are being accessed by the supplier.

3. Governing Laws and Regulations

Guidance	Section
ISO27001:2013	A.15(A.15.1, A.15.1.1, A.15.1.2, A.15.1.3 A.15.2, A.15.2.1, A.15.2.2)

4. Policy Statement

4.1 Information security in supplier relationships

4.1.1 Information security policy for supplier relationships

· Health Care Credit Union shall ensure that a full assessment of the potential security risks with using an outsourced provider, or a supplier is carried out. This must include identification of what needs to be protected and why.

· Health Care Credit Union shall ensure that the risks associated with outsourcing are managed through the imposition of suitable controls, comprising a combination of legal, physical, technical, procedural, and managerial controls.

· Health Care Credit Union shall ensure that there is an identified service of each supplier.

· Health Care Credit Union should consider the following when selecting an outsourced provider or a supplier:

- Supplier's reputation and history.
- Quality of services provided to other customers.
- Financial stability of the company and commercial record.
- Retention rates of the company's employees.
- Quality assurance and security management standards currently followed by the company (e.g. certified compliance with ISO/IEC27001, Cyber Essentials/Cyber Essentials +).

4.1.2 Addressing Security Within Supplier agreements

· Proper information security requirements must be established with each supplier that may access, process, store, communicate or provide ICT infrastructure components for the Health Care Credit Union.

· Requirements must include specifying:

- What data is held by or accessed by the supplier.
- When data is held by the supplier the process of cleaning the stored that is applied during the contract and will be applied at contract termination.
- The supplier to Health Care Credit Union has subcontracted any services to other subcontractors or suppliers.
- Access method to the Information of Health Care Credit Union.
- Point of contact from the supplier who will be managing the cyber risks for the delivery of the contract.
- The basic staff training and awareness raising around cyber risk carried out by the supplier.

- Cyber assurance accreditation eg Cyber Essentials, ISO27001 or equivalent

These requirements must be documented in the Supplier Contract.

4.1.3 Information and Communications Technology Supplier Chain

· Access to the Organizational assets shall include assurance procedures and must be fully compliant with the Health Care Credit Union's Third-Party Access Policy.

· The contracted supplier must manage all accesses provided to it.

· Data can only be transferred by explicit agreement from Health Care Credit Union using a defined secure method written in the supplier contract.

4.2 Supplier Service Delivery Management

4.2.1 Monitoring and review of supplier services

· Supplier service delivery should be monitored, reviewed, and audited on a regular basis by Health Care Credit Union.

· Information security terms and conditions must be followed and information security incidents and problems must be effectively handled through regular monitoring and assessment of service providers. This includes a process of:

- Verification of agreement compliance through service level monitoring.

- Regularly reviewing service reports from the supplier.

- Performing audits of the supplier and following up on reported problems and, if possible, using the findings of independent auditors to help resolve the issues.

- Providing and reviewing information on safety occurrences as specified in the agreements and any applicable standards and procedures.

- Examining the audit and information security reports, operational issues, failures, fault-tracking, and service-related disturbances that other Medical or e-commerce users have reported in the past.

4.2.2 Managing Changes to Supplier Services

· Maintaining and periodically upgrading existing information security policies, procedures, and controls.

· Information Owners and Service Owners must ensure agreements with suppliers include provisions for amending agreements in response to changes in legislation, regulation, business requirements, standards, policies, or service delivery

5. Non-Compliance

In cases where it is determined that a breach or violation of Health Care Credit Union policies has occurred, the Information Security Department, under the direction of the Chief Information Officer will initiate the corrective measures including restricting access to services or initiating disciplinary including the termination of a contract or agreement with the contractor or vendor.

6. Exceptions

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

7. Revision History

Version ID	Date of Change	Author	Rationale
