System Acquisition, Development and Maintenance

Table of Contents

1. Purpose 2
2. Scope 2
3. Objectives 2
4. Governing Laws and Regulations 2
5. Policy Statement 3
   - 14.1 Security requirements of information systems 3
     - 14.1.1 Security Requirements Analysis and Specification 3
     - 14.1.2 Secure System Engineering Principles 3
     - 14.1.3 Secure Development of Applications 3
   - 14.2 Protection of information systems against malware 3
     - 14.2.1 Malware Prevention 3
     - 14.2.2 Malware detection and removal 3
   - 14.3 Backup of information systems 4
     - 14.3.1 Back-up procedures 4
     - 14.3.2 Retrieval of information from back-up 4
   - 14.4 Cryptographic Controls 4
     - 14.4.1 Policy on the use of cryptographic controls 4
     - 14.4.2 Key management 4
6. Non-Compliance 5
7. Exceptions 5
8. Revision History 5

1.0 Purpose

The purpose of this cybersecurity policy is to establish the necessary controls and guidelines for the acquisition, development, and maintenance of information systems and data by HealthCare Credit Union and Mednow. The policy is designed to protect the confidentiality, integrity, and availability of sensitive data and ensure that these organizations comply with applicable legal and regulatory requirements.

2.0 Scope

This policy applies to all employees, contractors, and third-party service providers who have access to HealthCare Credit Union and Mednow's information systems, data, and networks. The policy covers all information systems and data, including but not limited to databases, software applications, network devices, and hardware. The policy applies to all phases of the information system lifecycle, including the acquisition, development, implementation, operation, maintenance, and disposal.

3.0 Objectives

The objectives of this policy are to:

- Define the roles and responsibilities of employees, contractors, and third-party service providers in the acquisition, development, and maintenance of information systems and data.
- Ensure that information systems and data are acquired, developed, and maintained according to industry best practices and standards, including the ISO 27001 framework, HIPAA, and PCI-DSS regulations.
- Establish guidelines for the assessment, mitigation, and management of cybersecurity risks and vulnerabilities.
- Ensure that all employees, contractors, and third-party service providers are trained on cybersecurity policies, procedures, and best practices.
- Establish incident response procedures to detect, respond to, and recover from cybersecurity incidents.
- Ensure that the policy is reviewed and updated regularly to reflect changes in the threat landscape, legal and regulatory requirements, and industry best practices.

4.0 Governing Laws and Regulations

Guidance	Section
ISO27001:2013	A.14 (A14.1, A14.2, A14.3, A14.4)

5.0 Policy Statement

HealthCare Credit Union and Mednow are committed to implementing and maintaining secure systems, applications, and networks to support their business objectives and protect their information assets. The following policies apply to all employees, contractors, and third-party service providers involved in the acquisition, development, and maintenance of the companies' systems, applications, and networks.

Security requirements of information systems

1.1 Security requirements analysis and specification

Both HealthCare Credit Union and Mednow shall carry out security requirements analysis and specification for all information systems. The analysis and specification shall cover the identification of threats, vulnerabilities, and potential impacts. Security requirements shall be documented, and they shall be integrated into the system development life cycle.

1.2 Secure system engineering principles

Both HealthCare Credit Union and Mednow shall ensure that security is integrated into their systems from the outset. Secure system engineering principles shall be used in the design and development of all systems, applications, and networks. The principles shall include secure coding, secure configuration management, and the use of secure design patterns.

1.3 Secure development of applications

HealthCare Credit Union and Mednow shall ensure that all applications are developed securely. The development process shall include threat modeling, code reviews, and testing for vulnerabilities. The development process shall also follow secure coding standards and practices.

Protection of information systems against malware

2.1 Malware prevention

Both HealthCare Credit Union and Mednow shall implement measures to prevent malware from infecting their systems, applications, and networks. The measures shall include antivirus software, intrusion prevention systems, and firewalls. The antivirus software shall be updated regularly to ensure that it can detect and remove the latest malware.

2.2 Malware detection and removal

Both companies shall implement measures to detect and remove malware that may infect their systems, applications, and networks. The measures shall include regular scanning of systems, applications, and networks for malware. Detected malware shall be removed immediately to prevent it from spreading to other systems, applications, and networks.

Back-up of information systems

3.1 Back-up procedures
Both HealthCare Credit Union and Mednow shall implement back-up procedures for their systems, applications, and networks. The procedures shall include regular back-ups of critical data and storage of back-up data in secure locations. Back-up data shall be tested regularly to ensure that it can be restored in the event of a disaster.

3.2 Retrieval of information from back-up
Both companies shall ensure that data can be retrieved from back-up in the event of a disaster. The retrieval process shall be tested regularly to ensure that it is effective and efficient. In the event of a disaster, data shall be restored as quickly as possible to minimize the impact on business operations.

Cryptographic controls

4.1 Policy on the use of cryptographic controls
Both HealthCare Credit Union and Mednow shall implement a policy on the use of cryptographic controls. The policy shall cover the selection, implementation, and use of cryptographic controls to protect their information assets. Cryptographic controls shall be used to ensure the confidentiality, integrity, and authenticity of information.

4.2 Key management
Both companies shall ensure that cryptographic keys are managed securely. The management process shall include the generation, distribution, storage, and destruction of cryptographic keys. The management process shall also include procedures for revoking and replacing compromised keys.

6. Non-Compliance:

Non-compliance with this cybersecurity policy can result in disciplinary action, up to and including termination of employment or contract. Non-compliance can also lead to legal and financial liabilities for HealthCare Credit Union and Mednow, including fines, lawsuits, and reputational damage. All employees, contractors, and third-party service providers are responsible for complying with this policy and reporting any suspected or actual breaches of this policy.

7. Exceptions:

Any exception to this cybersecurity policy must be approved by the Chief Information Security Officer (CISO) or designated representative. Exceptions will be considered on a case-by-case basis, and only where there is a compelling business reason for the exception. Any exception must be documented and reviewed regularly to ensure that it remains valid. The CISO or designated representative will assess the potential risks and ensure that appropriate controls are in place to mitigate those risks. The CISO or designated representative will also ensure that any exception is consistent with legal and regulatory requirements.

8. Revision History

Version ID	Date of Change	Author	Rationale