Atlantic Credit Union
Cybersecurity Policy Framework

DATE LAST MODIFIED:	23 June 2021
VERSION NO:	2.1
PREPARED BY:	CGI

Document Acceptance and Sign-off

Name and Position	Signature and Date
Completed By (CGI):	
Amandeep (v1.0) **Tim Feeley and Laura Ferguson (v2.0)**	**12 February 2020** **10 June 2021**
Reviewed By (CGI):	
Jason MacDonald and Krishna Raj Kumar (v1.0) **Allan Zinck and Krishna Raj Kumar (v2.0)**	**19 February 2020** **23 June 2021**
Approved by (League Data):	
Allan Brown (v1.0) **Allan Brown (v2.0)**	**24 June 2020** **XX June 2021**
Reviewed by (ACU Cybersecurity Governance Committee):	

Document Revision History

Description	Author	Date Modified	Version
Cybersecurity	Krishna Raj Kumar	24 June 2020	1.0
Updates to version 1.0	Tim Feeley Laura Ferguson	09 June 2021	2.0
Reviewed and QA	Allan Zinck Krishna Raj Kumar	23 June 2021	2.1
Updates to version 2.1	Hannah Noftall	26 October 2021	2.2

Table of Contents

Article I. Overview

The Atlantic Credit Union Cybersecurity Program is committed to protecting employees, partners, and clients of CU's from damaging acts that are intentional or unintentional. By extension, management of all CUs have an obligation to provide appropriate protection against internal and external threats which could adversely affect the security of the overall CU system or the data contained within.

The Atlantic Credit Union Cybersecurity Policy Framework is a subset of the Atlantic Credit Union Cybersecurity Program and will outline the set of baseline, cybersecurity policy requirements that must be met by Credit Unions (CUs) to improve and maintain their cybersecurity posture in accordance with industry best practices, compliance regulations, and standards (NIST 800-53 and ISO 27001:2013).

Effective implementation of this policy framework will limit the exposure to and effect of cybersecurity threats to the assets and business of Atlantic Canada's Credit Unions.

Article II. Purpose

The purpose of the document is to describe a comprehensive Cybersecurity policy framework for:

- Creating a NIST-based Cybersecurity policy set that covers the NIST control areas outlined in the Atlantic Credit Union Cybersecurity Program;
- Protecting the confidentiality, integrity, and availability of CU assets (data and Information and Communication Technology (ICT) systems);
- Protecting the CU, its employees, and its customers from the unauthorized use of CU data and ICT systems;
- Ensuring the effectiveness of security controls over data and ICT systems that support CU operations;
- Providing effective, system-wide management and oversight of cybersecurity risks; and,
- Providing for the development, review, and maintenance of minimum security controls required to protect CU data and ICT systems.

These policies set the ground rules under which League Data and Atlantic Canadian Credit Unions operate and the safeguards which protect data and ICT systems. These policies are necessary to support the management of information risk across the Atlantic Credit Union system. The development of policies provides due care to ensure CU employees understand their day-to-day security responsibilities. Implementing consistent security policies across the "Atlantic CU Community" aims to help all stakeholders to meet any regulations, legal obligations and ensure long-term due diligence in protecting the confidentiality, integrity, and availability of CU assets.

Article III. Scope & Applicability

These policies shall be applicable to all CU data, ICT systems, activities, and assets owned, leased, controlled, or used by CUs, contractors, or other business partners on behalf of CUs. These policies shall be applicable to all CU employees, contractors, and their respective facilities supporting CU business operations, wherever CU data is stored, or processed, including any third party contracted by a CU to handle, process, transmit, store or dispose of CU data.

These policies do not supersede any other applicable law or higher-level company directive.

Article IV. Policies, Standards, Procedures and Guideline Structure

Cybersecurity policy sets are comprised of five main parts: a core policy; a control objective that identifies desired conditions; measurable standards used to quantify the requirements; procedures that must be followed; and guidelines that are recommended, but not mandatory.

Cybersecurity Policies

Cybersecurity policies are the highest level of cybersecurity policy sets. Policies are approved and issued by senior management of the organization as their expectation for the overall security program, system controls, and user behavior. Policies provide the "why" of the security program. Cybersecurity policies are mandatory in that all information systems and users are expected to conform to the policy statements. The policies in the ACU policy set are aligned with and based on the NIST 800-53 Framework.

Cybersecurity Standards

Cybersecurity standards are a refinement of mandatory security requirements in the cybersecurity policies that address selected methods, techniques, and devices. Standards provide the "what" of the security program. The standards in the ACU policy set are based on the NIST 800-53 frameworks and align with industries best practices.

Cybersecurity Guidelines

Cybersecurity guidelines are a further refinement of security requirements in the cybersecurity policies that address selected methods, techniques and devices. Guidelines are not mandatory as they specify suggested refinements of the cybersecurity policies. Guidelines are typically issued and approved by either senior management or their delegates such as a CISO or a security manager.

Cybersecurity Procedures

Cybersecurity procedures are step-by-step instructions for the implementation of security controls or processes dictated in the cybersecurity policies and standards. They are also a refinement of security requirements in the cybersecurity policy but they provide the "how" and the "who".

Cybersecurity Baselines

Cybersecurity baselines are mandatory minimum-security controls for a selected area or application. They are also a refinement of security requirements in the cybersecurity policies but they are used for devices, applications or other areas where a number of settings, parameters, and activities are related to the effectiveness of a security control.

Article V. Governance of the Cybersecurity Policy Framework

The policies within this framework have been developed by the Atlantic Credit Union Cybersecurity Program and will be governed as follows:

- This policy framework can only be updated with approval from League Data in collaboration with the Atlantic Credit Union Cybersecurity Governance Committee.
- This policy framework will be reviewed annually.
- The Atlantic Credit Union Managed Cybersecurity Service (MCS) will identify needs to update Policies and will make recommendations to League Data.
- CUs will establish their own cybersecurity standards and procedures that align with and support the cybersecurity policies.
- Where necessary, the MCS will assist CUs in identifying cybersecurity standards, procedures and guidelines required to align with the cybersecurity policies.

DISTRIBUTION

Updates to the approved policies or new policies shall be released to CUs via email. Changes to policies will be noted in the record of changes.

LANGUAGE

Throughout this policy document, the words Must, Must Not, Shall, Shall Not, Should and Should Not are used. Their respective definitions for the purpose of this policy set are:

- MUST – An absolute requirement of this policy document.
- MUST NOT – An absolute prohibition of the policy.
- SHALL – An absolute requirement of this policy document.
- SHALL NOT – An absolute prohibition of this policy.
- SHOULD - A best practice and a recommendation of this policy.
- SHOULD NOT- Not a best practice nor a recommendation of this policy.

Article VI. Format of a Cybersecurity Policy

Each policy in this policy set contains the following elements:

References

This section will provide relevant references that this policy refers where more detailed information might be found.

NIST Controls

This section will provide the specific CSF NIST controls that are covered by this policy.

Purpose

This section describes the purpose of the policy. Typically, the purpose is to establish a set of minimum security controls for ICT systems within the organization.

Policy Statement

This section includes the direct policy statements, including directives, requirements and references to standards, procedures and guidelines, where applicable.

Scope & Applicability

This section describes the reach of the policy in terms of who and what ICT systems are affected or governed by the policy. Scope statements typically cover application to departments, personnel, information systems, data, and devices.

Role and Responsibilities

This section lists the various roles involved with the policy and policy enforcement and each of their responsibilities for implementing, adhering to, or enforcing the policy statements. To eliminate confusion the same titles and roles should be used throughout the cybersecurity policy set, e.g. CEO, CISO, CIO, Cybersecurity Manager, System Owner, and User.

Article VII. Key Terminology

Key terminology used in the policy set includes:

- **Applicability:** The scope in which a control or standard is relevant and applicable.
- **Asset Custodian:** A person or entity with the responsibility to assure that:
  - assets are properly maintained;
  - assets are used for the purposes intended;
  - Information regarding the equipment is properly documented.
- **Classification:** 2 levels of classification have been implemented:
  1. Classified – files and/or devices contain personal information and/or business information that needs to be guarded against release to unauthorized persons.
  2. Public – Information that contains no personal information or is of no value to the Credit Union or any of its partners.
- **Criticality**: 3 levels of criticality have been implemented in this document:
  1. High – Critical to business (Even a minor interruption would cause significant disruption of the business. Major effect on delivering the service to the client.)
  2. Medium – Somewhat essential to business. (Would cause significant issues, however for short durations it would not greatly affect business processes. Minor disruption to the client)
  3. Low – Not essential to business. (Can operate for days or weeks without affecting the business. No disruption to the client)
- **Control:** Any management, operational, or technical method that is used to manage risk.
- **Control Objective:** Targets or desired conditions; Control objectives ensure that policy intents are met. Where applicable, Control Objectives are directly linked to an industry-recognized best practice to align with accepted due care requirements.
- **Cybersecurity:** The protection of information and ICT assets against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional; or, the assurance that Confidentiality, Integrity, and Availability (CIA) of information and ICT assets is maintained.
- **Data:** An information resource that is maintained in electronic or digital format. Data may be accessed, searched, or retrieved via electronic networks or other electronic data processing technologies.
- **Encryption:** The conversion of data from its original form to a form that can only be read by someone that can reverse the encryption process. The purpose of encryption is to prevent unauthorized disclosure of data.
- **Employee:** A person employed in a position below the executive level.
- **Guidelines:** Recommended steps/actions that are based on industry-recognized best practices. Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation, or use.
- **ICT:** Information and Communication Technology (ICT).
- **IT Manager (Manager - Technology):** The person accountable for managing the IT systems and assets either through a third party contract or directly themselves. This position is either the primary role as listed in the job title or a secondary position as assigned by the Manager/Team Leader and/or the Board of Directors.

- **IT Officer (IT Administrator):** Responsible for the physical security along with the safety of employee's assets and the protection of data. This position is either the primary role as listed in the job title or a secondary position as assigned by the Manager/Team Leader and/or the Board of Directors.
- **Least Privilege:** The theory of restricting access by only allowing users or processes the least set of privileges necessary to complete a specific job or function.
- **Manager/Team Leader:** A person by title or role has been assigned the duties of manager to the employees. This position is either the primary role as listed in the job title or a secondary position as assigned by the Manager/Team Leader and/or the Board of Directors.
- **Policy:** A formally established requirement to guide decisions and achieve rational outcomes. Essentially, a policy is a statement of expectation that is enforced by standards and further implemented by procedures.
- **Procedure:** An established or official way of doing something based on a series of actions conducted in a certain order or manner. Procedures are the responsibility of an asset custodian to build and maintain, in support of standards and policies.
- **Risk Manager (Manager, Risk and Compliance):** The position accountable for risk management operations. This position is either the primary role as listed in the job title or a secondary position as assigned by the Manager/Team Leader and/or the Board of Directors.
- **Sensitive:** A descriptor of data whose loss, misuse, or unauthorized access or modification could adversely affect security. Examples of sensitive data include Personally Identifiable Information (PII), Electronic Protected Health Information (PHI), passwords, account balances, withdrawal limits, etc.
- **Standard:** Formally established requirements in regard to processes, actions, and configurations.
- **System:** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Includes, but is not limited to, computers, workstations, laptops, servers, routers, switches, firewalls, and mobile devices.
- **Target Audience:** The intended group for which a control or standard is directed.

VIOLATIONS

Any user found to have violated any cybersecurity policy, standard or procedure may be subject to disciplinary action, up to and including termination of employment. Violators of local, provincial, federal, and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

EXCEPTION

While every exception to a policy potentially weakens protection offered by the policy to information systems and data, occasionally exceptions will be required. Policy exception request procedures shall be maintained and exceptions shall be monitored to avoid abuse.

Any exceptions to these policies must be approved by management.

COMPLIANCE

The CRO, Regulators or Auditors appointed by the Security Governance body will verify compliance with this policy through various methods, including but not limited to, periodic audits and compliance monitoring.

1. Cybersecurity Program Management Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.GV-1, ID.GV-2, ID.RA-3, ID.SC-1, ID.SC-2, ID.SC-4

Purpose

The purpose of the Cybersecurity Program Management policy is for CUs to specify the development, implementation, assessment, authorization, and monitoring of the Cybersecurity program. The successful implementation of security controls for organizational Information systems depends on the successful implementation of the organization's program management controls.

Policy Statement

To establish a Cybersecurity Program Management System to protect and maintain the confidentiality, integrity, and availability of the CU's information system.

Scope & Applicability

This policy shall apply to the CU's data, information systems, activities and assets, owned, leased, controlled, or used by the CU, its agents, contractors, or other business partners on behalf of the CU.

Role & Responsibilities

The **Board of Directors and Chief Executive Officer (CEO)** are ultimately responsible for the cybersecurity program and thus also for the implementation of this policy.

The management of the cybersecurity program is **shared between the Chief Administrative Officer (CAO) and the Manager - Technology.**

The **Manager – Technology** is responsible for:

- Publishing and promoting (internally) the Cybersecurity Policy;
- Formulating the business requirement for information systems;
- Defining responsibility for information systems including documentation requirements;
- Subjecting the business and third parties to recurring audits and managing cybersecurity risk.
- IT department guidelines, procedures and system-specific documentation;
- Ensuring that all documentation within their own domain of responsibility is updated and relevant;
- Daily operations of the information systems, infrastructure and strategic assets within their own domain;
- Implementing risk mitigating actions in line with budgets and organizational risk appetite; and
- Balancing spending on threat prevention, threat detection and threat remediation in cooperation with the Chief Information IT Security Officer and Chief Risk Officer (or equivalent roles).

The **CAO** is responsible for:

- Defining the risk appetite and acceptable risk levels;
- Budgeting so that risk can be managed according to the risk appetite;
- Creating a framework and procedures for risk and consequence/impact analysis and performing the analysis;
- Risk assessment of third-party contractors including new and existing vendors; and,

- Creating and maintaining the Risk Register.

The **manager/team leader** is responsible for compliance with the cybersecurity policies, procedures, and guidelines within his/her own group of personnel.

The **employee** is responsible for carrying out daily tasks within the framework of this cybersecurity program policy.

2. Awareness and Training Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.RA-2, PR.AT-1, PR.IP-8

Purpose

The purpose of the Awareness and Training Policy is to provide accessible education for CU employees and third-party vendors to minimize the risk associated with employee's actions and behavior.

Policy Statement

All employees and third-party vendors who access a CU's information system must understand how to protect the confidentiality, integrity and availability of CU information.

The CU shall ensure that all employees and contractors are given security and awareness training during the new hire process and before accessing any CU information system. This training reflects common security and privacy awareness specific to the environment including, but not limited to physical access, restricted areas, potential incidents, incident reporting, best practices, social engineering and how to spot a phishing scam.

The CU shall also conduct refresher training annually or anytime there are significant changes to the system/ environment.

Scope & Applicability

This policy shall apply to all CU employees, agents, contractors, or other business partners on behalf of CUs.

Role & Responsibilities

Senior Management shall commit to the development of a security and awareness training program and allocation of staff and resources to implement the program.

The **Manager – Risk and Compliance** shall be responsible for:

- Maintaining ongoing activities related to security training and awareness;
- Updating annual security training materials;
- Conducting new hire cybersecurity training;
- Ensuring all employees understand and follow security-related policies and procedures.
- Cybersecurity information will be shared between known partners as required.

The **manager/team leader** is responsible for ensuring all employees complete required security training.

The **employee** is responsible for understanding and following all security-related policies and procedures, and asking their manager or IT Security Officer for clarification if needed. The **employee** is responsible for completing all training as assigned.

3. Security and Privacy Planning Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.GV-1, ID.GV-2, ID.GV-3, PR.AC-1

Purpose

The purpose of the Security and Privacy Planning policy is to develop security and privacy measures and procedures for the information systems to meet the CU's objectives and address the changes in the system and the environment of operations. Security planning helps maintain the confidentiality, integrity, and availability of the CU's data and information systems. This policy shall provide an overview of the security requirement of a CU's information system and describe the controls that shall be in place to meet these requirements.

Policy Statement

To establish a high-level security and privacy plan or program that protects the CU's data and information systems. The CU shall define the plan or program under which the CU protects and controls access to its information systems. This policy shall satisfy all the procedures of NIST 800-53 control categories.

Scope & Applicability

This policy shall apply to all the CUs data, systems, activities, and assets owned, leased, controlled, or used by the CU, its agents, contractors, or other business partners on behalf of the CU.

Role & Responsibilities

The Board of Directors and CEO are ultimately responsible for the cybersecurity policy and thus for the implementation of this policy.

Senior Management shall commit to the development of a security and privacy plan and allocation of staff and resources to implement the plan. Senior management shall ensure distribution of and accessibility to the security and privacy plan.

The **IT Administrator or equivalent** role will draft a security and privacy plan that reflects the selected security controls, and applicable laws, directives, and regulations. This includes the responsibility to:

- Develop, document, and maintain cybersecurity and privacy plans for each CU system and network;
- Develop, document, and maintain a cybersecurity architecture;
- Develop, document, and maintain privacy plans that address the requirements for collection, use and disclosure of personal information via the CU's information systems.

The Manager – Technology or equivalent role is responsible to implement the selected approved controls.

4. Personnel Security Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.AM-6, ID.GV-1, ID.GV-2, ID.SC-3, PR.AC-1, PR.AT-3, PR.AT-4, DE.CM-3

Purpose

The purpose of this policy is to minimize the chances of abuse, misuse, or destruction of the CU's information systems by verifying the integrity of personnel who are provided access to the CU's information systems.

Policy Statement

The CU shall:

- Screen individuals holding positions designated as sensitive prior to hiring or contracting.
- Define cybersecurity responsibilities for all personnel;
- Conduct exit interviews and revoke access to information, upon termination of personnel.
- Review logical and physical access upon change of duties;
- Establish personnel security requirements including security roles and responsibilities for third-party vendors.

Scope & Applicability

This policy shall apply to all CU employees, agents, contractors, or other business partners on behalf of the CU.

Role & Responsibilities

The **Board of Directors and CEO** are responsible for the cybersecurity program and for the implementation of this policy.

Senior Management shall commit to providing resources and budget for the assessment of personnel security.

The **Manager - Technology or equivalent** role shall draft standards that reflect the procedures and guidelines to provide personnel security.

5. Risk Assessment Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.AM-5, ID.GV-1, ID.GV-2, ID.GV-3, ID.GV-4, ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6, ID.RM-1, ID.RM-2, ID.RM-3, ID.SC-1, ID.SC-2, ID.SC-4, PR.IP-7, PR.IP-12, DE.AE-2, DE.AE-4, DE.CM-1, DE.CM-2, DE.CM-8, DE.DP-1, RS.AN-1, RS.AN-3, RS.MI-2, RS.MI-3

Purpose

The purpose of this policy is to ensure that the CU identifies cybersecurity risks to its information systems considering the relevant threats and vulnerabilities and corresponding business impact; and that the CU plans appropriate risk mitigation initiatives to address the identified cybersecurity risks.

Policy Statement

The CU shall manage risk appropriately. Risk management includes the identification, analysis, and management of risks associated with a CU's business, information technology infrastructure, processes, and physical security.

The CU shall:

- Conduct risk assessments, including the assessment of likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, or destruction of the information system;
- Document risk assessment results, review open risk assessment results bi-annually and update the risk assessment annually or when there are significant changes in the system; and,
- Assess supply chain risks associated with the CU's information system.
- Scan for vulnerabilities in the information systems and hosted applications;
- Conduct vulnerability scanning and reporting;
- Analyze vulnerability scan reports and remediate findings;
- Respond to findings from security and privacy assessments, monitoring, and audits;
- Conduct privacy impact assessment for systems, programs or other activities that potentially pose a privacy risk; and,
- Identify critical system components and functions by performing a criticality analysis.

Scope & Applicability

This policy shall apply to all the CU's data, systems, activities, and assets owned, leased, controlled, or used by the CU, its agents, contractors, or other business partners on behalf of CUs.

Role & Responsibilities

The **Board of Directors and CEO** are responsible for the cybersecurity program and for the implementation of this policy.

Senior Management shall commit to providing resources and budget for conducting risk assessments and mitigating identified risks.

The **Manager, Risk and Compliance** shall approve third party assessment engagements and have oversight of the risk assessment process. They will be responsible to treat identified risks in coordination with the system/data/asset owners. The **Manager, Risk and Compliance** shall work with third-party risk assessors to conduct risk assessments.

The **Manager - Technology** role is responsible to provide adequate information about the information systems and processes in place.

6. System and Service Acquisition Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.BE-1, ID.SC-1, ID.SC-3

Purpose

The purpose of this policy is to ensure that security is integrated through the whole lifecycle of information systems acquisitions and development. This policy establishes requirements that address system and services acquisition controls for CU information systems.

Policy Statement

The CU systems and service acquisition process requires that:

- All identified systems and services for procurement should be reviewed against best practices and standards for the technology type or service being acquired;
- Capital planning activities, which include the acquisition of products/services should include an assessment capable of identifying potential cybersecurity risks;
- CUs procuring technology for use in their computing environment shall be provided documentation which states the security configuration of the technology;
- Supply chain procedures shall be documented; and,
- Providers of external system services comply with the CU's security and privacy requirements.

Scope & Applicability

This policy shall apply to all the CUs data, systems, activities, and assets owned, leased, controlled, or used by CUs, its agents, contractors, or other business partners on behalf of the CU.

Role & Responsibilities

The **Board of Directors and CEO** are responsible for the cybersecurity program and for the implementation of this policy.

Senior Management shall commit to provide resources and budget to incorporate/assess the secure lifecycle in the development/ acquisition of information systems.

The **Manager, Risk and Compliance** role shall identify key activities to be carried out to ensure that security is an integral part of the information system and service acquisition lifecycle. They shall make requests to 3rd party vendors to understand integral security practices during the development and acquisition of information systems.

The **Manager - Technology** shall assess third-party vendor practices adopted in the development and acquisition of CU information systems.

7. System and Information System Ownership Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.AM-1, ID.AM-2, ID.GV-4, ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6, PR.AC-1, PR.DS-8, PR.IP-11, DE.CM-4, DE.CM-5, DE.CM-7, DE.DP-1, RS.AN-1, RS.MI-3

Purpose

The purpose of this policy is to identify the owners of the information systems, data, information, and processes and to outline the responsibilities of the owners.

Policy Statement

The CU shall define the owners and their roles in relation to each and every subsystem and part of the information system including data owner, process owner, and solution owner.

Scope & Applicability

This policy shall apply to all the CU's data, systems, activities, and assets owned, leased, controlled, or used by the CU, its agents, contractors, or other business partners on behalf of CUs.

Role & Responsibilities

The **Board of Directors and CEO** are ultimately responsible for the cybersecurity program and thus also for the implementation of this policy.

The **Manager -Technology** role shall assess the separation of duties in regards to system ownership. They shall communicate the responsibilities of the ownership to the owner of each information system / subsystem.

The **Manager, Risk and Compliance** shall communicate the risks listed in the assessment of the system with the system/subsystem owner and shall communicate the process of treating the risk in alignment with the CU's risk mitigation strategy.

The **Owner of the system/subsystem** is responsible to:

- Maintain the confidentiality, integrity and availability of the owned system;
- Treat the risks identified in risk assessments of the owned information system/subsystem; and,
- Authorization, monitoring and quarterly review of access to owned information system/subsystem.

8. Access Control Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.GV-1, PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.AT-2, PR.IP-11, PR.MA-2, PR.PT-3, DE.CM-5, DE.CM-6, DE.CM-7

Purpose

The purpose of this policy is to establish the access controls for the protection of the CU's information systems. This policy establishes the requirements for managing risks related to user account management, access enforcement, monitoring, separation of duties, and remote access.

Policy

The CU will develop, adopt or adhere to a formal, documented access control program that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance. The access control program will:

- Identify user account types and establish roles and permissions for user groups.
- Maintain a list of authorized users of each information system including their access privileges.
- Require appropriate approvals for requests to establish user accounts.
- Maintain a user provisioning (onboard, off-board) process.
- Monitor the use of guest/anonymous and temporary accounts.
- Notify managers and administrators when temporary user accounts are no longer required and when a user is terminated, transferred, or requires changes to access permissions.
- Grant access to information systems based on a validated and authorized need-to-know.
- Review user accounts on a periodic basis (at least once annually).
- Separate the duties of individuals as necessary, e.g. an individual who approves access should not also be responsible for implementing (setting up) user accounts. Separation of duties shall be documented.
- Employ the concept of least privilege, i.e. limiting authorized access necessary only to accomplish assigned tasks in accordance with business functions/responsibilities.
- Display system use notifications or banners before granting access to the system, that provide privacy and security notices consistent with policies, standards and regulations.
- Initiate session locking after an established period of inactivity (e.g. 15 minutes) or upon receiving a locking request from a user.

Remote Access:

- Document allowed methods and requirements for remote access to information systems.
- Technical controls shall be implemented to monitor for unauthorized remote access to information systems.

Wireless Access:

- Establish usage restriction and implementation guidance for wireless access.
- Monitor for unauthorized wireless access to information systems.
- Authorize wireless access prior to connection.

- Guest wireless access shall be separated from the corporate network.

MOBILE DEVICES:

- Establish usage restrictions and implementation guidance for organization-controlled mobile devices.
- Restrict the connection of mobile devices to only devices that meet organizational technical criteria.
- Monitor for unauthorized connections of mobile devices to organizational information systems.
- Disable mobile functions that provide the capacity for automatic execution of code without user direction.

USE OF EXTERNAL INFORMATION SYSTEM:

- Establish terms and conditions, consistent with any trusted relationships established with other organizations owning, operating, and maintaining external information assets.
- Only allow authorized access to information CU information systems from trusted external information systems.

PUBLICLY ACCESSIBLE CONTENT:

- Designate individuals authorized to post information to organizational information systems that are publicly accessible.
- Train authorized individuals to ensure that publicly accessible information does not contain private, internal, or other kinds of sensitive information.
- Review proposed public content for non-public information prior to posting onto publicly accessible information systems.

SCOPE & APPLICABILITY

This policy shall apply to all the CU's data, systems, activities, and assets owned, leased, controlled, or used by the CU, its agents, contractors, or other business partners on behalf of CUs.

ROLE & RESPONSIBILITY

The **Board of Directors and CEO** are ultimately responsible for the cybersecurity program and thus also for the implementation of this policy.

The **CAO** shall be responsible for the effectiveness of the selected access controls to protect the confidentiality, integrity, and availability of CU information systems.

The **Owner of the system/subsystem** is responsible to ensure that:

- Access controls and authorization processes are approved by the CISO.
- Every new method of access or authorization is assessed for security risk.
- Access control and authorization procedures and controls are reviewed quarterly.

The **Manager -Technology** shall develop access control procedures that are approved by the **CAO**.

9. Audit and Accountability Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.GV-3, PR.PT-1, PR.PT-4, DE.AE-3, DE.CM-7

Purpose

Maintaining detailed audit logs is critical to managing and tracking the chronological flow of data from sources to destinations. In instances of security and compliance, audit logs offer an official record that can provide valuable insights that are beneficial to CU interests.

The purpose of this policy is to ensure proper audit logs are maintained.

Policy Statement

The CU Shall:

- Record all users' actions in system audit logs.
- Retain system audit logs and records for the purpose of monitoring, analysing, investigating, and reporting unlawful or unauthorized system activity.
- Integrate automated systems/solutions to centrally collect, review and correlate logs to identify suspicious activities.
- Synchronize internal system clocks with an authoritative source to generate accurate timestamping for audit records.
- Configure audit logging to balance the size of log files with the required retention period for audit logs.
- Retain audit logs for periods aligned with the useful business purpose and legal and regulatory requirements.

Scope & Applicability

This policy shall apply to all CU information systems, employees, agents, contractors, or other business partners on behalf of the CU.

Role & Responsibilities

The **Board of Directors and CEO** are ultimately responsible for the cybersecurity program and thus also for the implementation of this policy.

The **Manager, Risk and Compliance** role shall draft an audit and accountability plan that reflects the procedure and guidelines to collect, store and correlate audit logs.

The **Manager -Technology** is responsible to draft configuration procedures that reflect the requirement of each event to be logged and audited and is responsible to list the auditable events and content of audit records.

Managers and team leaders shall ensure that all employees are aware that they are responsible for their actions which are recorded in audit logs.

10. Configuration/Change Management Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.AM-3, ID.AM-4, ID.RA-3, PR.DA-7, PR.IP-1, PR.IP-2, PR.IP-3, PR.PT-2, DE.AE-1, DE.CM-7

Purpose

Change management is the process of communicating, coordinating, scheduling, recording and monitoring changes to infrastructure and the technical environment.

The purpose of this policy is to preserve the integrity and stability of the CU's information systems by establishing requirements that will govern the system change management process.

Policy Statement

Information systems are typically dynamic, causing the system state to change frequently as a result of upgrades to hardware, software, firmware or modification to the environment in which a system resides.

Changes to information systems shall be planned, documented and assessed for potential impact on the operational processes and security posture of the CU.

The CU shall:

- Develop or adopt and adhere to a formal, documented program that ensures the implementation of appropriate and effective system configuration management controls.
- Establish a configuration management plan / process that outlines how configuration management will be conducted throughout the lifecycle of information systems.
- Develop, document, and maintain a record of baseline configurations for information systems.
- Review baseline configurations at least annually.
- Document all configuration changes and conduct assessments of potential impacts before approving implementation of the changes.
- Configure information systems to provide only essential services/functions.
- Disable/restrict all non-essential services, functions, ports, and protocols.

Scope & Applicability

This policy shall apply to all CU employees, agents, contractors, or other business partners on behalf of CUs who have responsibility for configuration, management and oversight of the CU's hardware, software, and applicable documentation.

Role & Responsibilities

The **Board of Directors and CEO** are ultimately responsible for the cybersecurity program and thus also for the implementation of this policy.

The **CAO** is responsible for approving and issuing policies, procedures and guidelines for implementing and coordinating the CU's configuration management program.

The **Asset Custodian** shall be responsible to assure that all changes are approved by an authorized CU representative.

The **Manager -Technology** shall ensure that all change control activity is appropriately documented and acts as the gatekeeper to ensure that only authorized changes are documented. Responsible for change approval/denial/closure and ensuring that each change has:

- Appropriate priority/schedule;
- Implementation plan approval;
- Test/validation sign-off;
- Rollback plan/criteria; and,
- Post-implementation lessons learned discussions.

System users are responsible for testing changes before change implementation and also perform post-implementation review.

11. Identification and Authentication Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.GV-1, PR.AC-1, PR.AC-4, PR.AC-6, PR.AT-2, PR.PT-3

Purpose

This policy establishes the enterprise identification and authentication program in relation to information systems access.

This policy provides requirements for the management of user identification and authentication to safeguard access to agency information and information systems and critical business processes.

Policy Statement

The CU shall:

- Ensure the CU's information systems uniquely identify and authenticate CU users or processes acting on behalf of organizational users.
- Assign to each CU and non-organizational user a unique identifier.
- Authenticate each CU and non-organizational user prior to each instance of access to CU assets.
- Not allow the use of shared user accounts.
- Implement multifactor authentication for network access from privileged user accounts, e.g. system administrator accounts.
- Ensure that all devices are uniquely identified and authenticated before establishing a network connection.

Scope & Applicability

This policy shall apply to all the CU data, systems, activities, and assets owned, leased, controlled, or used by CUs, its agents, contractors, or other business partners on behalf of the CU.

Role & Responsibilities

The **Board of Directors and CEO** are ultimately responsible for the cybersecurity program and thus also for the implementation of this policy.

The **CAO** shall draft an identification and authentication plan that includes mechanisms, technologies, procedures and guidelines to identify and authenticate users, employees, and system processes.

The **Manager - Technology** is responsible to implement the technology approved by the CAO to identify and authenticate employees, users and processes prior to providing access to CU information systems.

The **individual manager/team leader** is responsible for ensuring all employees are trained to securely use their access credentials and follow all CU access, authorization, and authentication procedures.

The **Individual employee** shall not share their identity and authentication credentials with anyone.

12. System and Communication Protection Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.GV-1, ID.RA-3, ID.RA-5, ID.RA-6, PR.DS-1, PR.DS-2, PR.DS-4, PR.DS-5, PR.DS-6, PR.IP-7, PR.PT-3, DE.AE-2, DE.AE-4

Purpose

The purpose of this policy is to establish appropriate controls to protect the confidentiality, integrity, and availability of the CU information systems and communication channels.

Policy Statement

The CU shall:

- Separate user functionality, including user interface services, from system management functionality.
- Prevent the presentation of system management functionality at an interface for non-privileged users.
- Deploy an intrusion detection system or service to detect suspicious activities.
- Isolate security functions from non-security functions.
- Prevent unauthorized and unintended information transfer via shared system resources.
- Protect against or limit the effect of denial of service events by employing best practice safeguards.
- Protect the availability of resources by allocating priority and quota of services.
- Deploy best practice safeguards to protect the system boundaries.
- Protect the confidentiality and integrity of transmitted information.
- Protect the CU information at rest, in transit and in use by using encryption technologies.
- Laptops may only be connected to a secure internet connection and a VPN is needed to access sensitive CU business and client information.

Scope & Applicability

This policy shall apply to all the CU data, systems, activities, and assets owned, leased, controlled, or used by the CU, its agents, contractors, or other business partners on behalf of the CU.

Role & Responsibilities

The **Board of Directors and CEO** are ultimately responsible for the cybersecurity program and thus also for the implementation of this policy.

The **CAO** shall approve a list of controls to secure the CU system and communications.

The **Manager – Technology** is responsible to deploy the controls and processes approved by the IT Security Officer to increase the security posture of the CU system and communications. The **Manager - Technology** shall assess the effectiveness of these controls and recommend changes to the **CAO**.

13. Asset Management Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.AM-1, ID.AM-2, ID.AM-5, ID.BE-2, ID.BE-3, ID.BE-4, ID.BE-5, ID.RA-4, ID.SC-2, PR.MA-1

Purpose

The purpose of this policy is to ensure that all of the CU ICT systems are identified, assigned to specific owners and appropriately classified considering their relevant business purpose and sensitivity. The recording, documenting, classifying, and maintenance of information assets is critical for appropriately protecting information assets and helps to determine the appropriate security controls for each ICT system.

Policy Statement

The CU shall appropriately manage the information processing systems to reduce risks of data leakages, and loss of the tangible asset.

The CU Shall:

- Define procedures to uniquely identify its ICT assets.
- Maintain an inventory of all ICT assets, including but not limited to, all network components, network interfaces, servers, desktops, laptops, software and mobile devices owned or leased by the CU.
- Classify all information assets based on the criticality and importance (classification) of the assets to the business.
- Monitor all changes to CU's assets and update the asset inventory accordingly.
- Assign an owner to each asset or group of assets.
- Securely dispose information assets.
- Conduct as a minimum, an annual physical audit to verify ICT assets.

League Data Shall:

- Maintain an inventory of all ICT assets, including but not limited to, all network components, servers, network interfaces, desktops, laptops, software and mobile devices owned or leased by League Data.
- Ensure (through contract) that all third-party providers maintain a similar inventory of all ICT assets required to provide services to CUs.

Scope & Applicability

This policy shall apply to all CU data, systems, activities, and assets owned, leased, controlled, or used by the CU, its agents, contractors, or other business partners on behalf of the CU.

Role & Responsibilities

The **Board of Directors and CEO** are ultimately responsible for the cybersecurity program and thus also for the implementation of this policy.

Senior Management shall commit to provide resources and budget for deploying solutions (e.g. IT Asset Management (ITAM) system) and processes to manage CU information assets. Senior Management shall be responsible to assign the ownership of the information asset.

The **CAO** role shall approve a list of controls and define procedures for asset management, asset classification and ownership of the CU information systems. The CAO shall be responsible to classify the asset in alignment with defined categories. The CAO will document the risks associated with classified asset and maintain the risk register. The CAO will communicate the risks with the asset's owner.

The **Manager- Technology** is responsible to deploy any approved automated controls/mechanisms (ITAM system) to inventory CU information systems.

The **System Owner** is responsible to manage the asset and responsible for physical and cyber risk related to the asset.

The **Manager, Risk and Compliance** shall assess the effectiveness of asset inventory controls every quarter.

14. Application Security Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.RA-1, PR.DS-7, PR.IP-2, PR.PT-1, PR.PT-4, DE.AE-3, DE.CM-8, DE.DP-1

Purpose

The purpose of this policy is to ensure that the CU manages cybersecurity risks associated with the software applications used by the CU.

Policy Statement

- Applications in use by the CU shall meet application security standards (e.g. OWASP).
- A secure development life cycle shall be adopted for the development of applications.
- Secure code review shall be performed before implementing applications into production (go-live / launch).
- Vulnerability testing and penetration testing shall be performed on applications before go-live and after any change is made to an application.
- Applications shall be configured in alignment with industry best practices.
- Applications shall utilize robust authentication and authorization controls in alignment with the CU's Identification and Authentication policy and standards.
- Applications shall be configured to generate audit logs in alignment with the CU's Audit and Accountability policy and standards.

Scope & Applicability

This policy shall apply to all the applications used by the CU, its agents, contractors, or other business partners on behalf of the CU.

Role & Responsibilities

The **Board of Directors and CEO** are ultimately responsible for the cybersecurity program and thus also for the implementation of this policy.

The **CAO** role shall have oversight of application secure code reviews and vulnerability and penetration testing.

The **Manager – Technology** is responsible to ensure that application configuration is secured and aligned to industry best practices approved by the IT Security Officer.

15. Antivirus, Patch Management and Vulnerability Management Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.GV-1, ID.GV-4, ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6, PR.DS-8, PR.IP-8, PR.IP-12, DE.CM-4, DE.CM-5, DE.CM-7, DE.CM-8, DE.DP-1, DE.DP-2, RS.MI-2, RS.MI-3

Purpose

The purpose of this policy to ensure that the CU adopts a vulnerability management process to identify and manage security weaknesses such as flaws/vulnerabilities, malicious code, unauthorized code changes, and inadequate error handling on CU systems and accordingly take appropriate actions to resolve such weaknesses.

Policy Statement

The CU Shall:

Flaw Remediation:

- Implement centralized vulnerability scanning tools or service.
- Regularly assess critical information systems for flaws and address identified issues in a timely manner by conducting periodic vulnerability assessments of all information systems.
- Patch/update all the CU information systems including hardware and firmware with the latest up to date patches from the approved source (e.g. hardware / software vendor).
- Incorporate flaw remediation into the organizational configuration management process.
- Not conduct intrusive scans of systems that are not under the CU's direct authority, e.g. systems provided by League Data.
- Not permit vendors or third-parties to conduct scans of CU information systems without the express permission of the IT Security Officer/equivalent role.
- Share identified vulnerabilities and any suspected and/or known suspicious activity with League Data, MCS and peers.

Malicious Code Protection:

Each CU shall:

- Employ malicious code protection mechanisms to detect, block, quarantine, or eradicate malicious code and alert administrative staff.
- Ensure malicious code protection mechanisms are current and updated.
- Periodically scan critical information systems for malicious code.
- Deploy a centralized Anti-Virus solution to scan the CU systems.
- Maintain and implement application whitelisting and blacklisting through automated tools.

Information System Monitoring:

Each CU shall:

- Monitor critical systems and networks for indicators of attacks, and unauthorized connections to critical information systems.
- Assess identified indicators and report unauthorized activity to the IT Security Officer and information system owner.

- Ensure the integrity of monitoring tools and the information obtained from those tools.
- Employ and maintain spam protection mechanisms.

Scope & Applicability

This policy shall apply to all the CU's data, systems, activities, and assets owned, leased, controlled, or used by the CU, its agents, contractors, or other business partners on behalf of the CU.

Role & Responsibilities

The **Board of Directors and CEO** are ultimately responsible for the cybersecurity program and thus also for the implementation of this policy.

The **CAO** shall approve the selection of tools for vulnerability and penetration testing in compliance with industry best practice and approve a mitigation strategy to treat the risks associated with identified vulnerabilities.

The **Manager – Technology** is responsible to implement and appropriately configure approved vulnerability scanning tools to avoid disturbance to system functions and quality of service offered. The **Manager -Technology** shall run vulnerability scan, generate vulnerability reports and share them with the CAO. For instances where vulnerability scans are provided by third party vendors, the **Manager - Technology** shall review the vulnerability reports and take appropriate actions where necessary. The **Manager - Technology** shall assess the effectiveness of these controls and recommend changes to the IT Security Officer.

The **system owner** will be responsible to ensure that the information system is updated and patched.

16. Assessment, Authorization and Monitoring Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.GV-1, ID.GV-3, ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6, PR.AC-5, DE.AE-3, DE.CM-1, DE.CM-7, DE.DP-3, RS.AN-1, RS.AN-2

Purpose

The purpose of this policy is to establish assessment, authorization and monitoring procedures for managing security and privacy risks.

Policy Statement

Information Risk Assessments are important to determine the extent to which controls are implemented correctly, operating as indented, and producing the desired outcome with respect to meeting established security and privacy requirements.

Assessment:

The CU shall:

- Develop a security and privacy risk assessment plan.
- Ensure that the assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment.
- Assess the security and privacy controls in the system and its environment of operations to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome in alignment with security and privacy requirements.
- Produce a security and privacy assessment report that includes recommendations for mitigating risks identified in the assessment.

Information System Connections:

The CU must:

- Ensure that connections are authorized from the information system to other information systems outside of the authorization boundary through the use of an interconnection security agreement.
- Document, for each connection, the interface characteristics, security requirements, and the nature of the information communicated.
- Monitor the information system's connections on an ongoing basis, verifying enforcement of security requirements.

Security Authorization:

The CU must:

- Assign a senior-level executive or manager to the role of authorizing official for the information system.
- Ensure that the authorizing official authorizes the information asset for processing before commencing operations.
- Document and update security authorizations on an annual basis.

Scope & Applicability

This policy shall apply to all the CU's IT resources owned by or operated on behalf of the CU by employees, agents, contractors, or other business partners.

ROLE & RESPONSIBILITIES

The **Board of Directors and CEO** are ultimately responsible for the cybersecurity program and thus also for the implementation of this policy.

The **Manager, Risk and Compliance** shall develop a plan of action and milestones for mitigating risks identified in assessments and incorporate the controls in alignment with the CU policies and best practices.

The **Manager - Technology** shall review the effectiveness of the controls in place and assess the risks related to the CU information systems.

17. Incident Response Policy

Cybersecurity Policy Handbook (NIST Controls)

PR.AT-1, PR.IP-9, PR.IP-10, PR.PT-5, DE.AE-2, DE.AE-4, DE.AE-5, DE.CM-1, DE.CM-7, DE.DP-4, DE.DP-5, RS.RP-1, RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4, RS.CO-5, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.MI-3, RS.IM-1, RS.IM-2

Purpose

The purpose of this policy is to define requirements, controls and response procedures for security incident/event management.

Policy Statement

The CU shall protect information systems against events that may jeopardize cybersecurity by contaminating, damaging, or destroying information assets.

Reportable incident:

The CU shall:

- Ensure that CU employees, vendors, and contractors are trained to identify and report suspicious activities.
- Conduct phishing simulation tests to check the behavior and knowledge of the CU employees, vendors, and contractors.

Incident Team:

- An incident management and response team shall be defined and communicated. The team should manage and respond to information system incidents.
- The incident management and response team shall be responsible for processing all incident reports and conducting all follow-up activities.

Incident Reporting:

- Cybersecurity incidents or events shall be reported in a timely manner to enable proper review of vulnerable controls and the establishment of appropriate corrective measures to reduce the likelihood of recurrence.

Response:

- The CU shall establish procedures to respond to reported incidents in a timely manner to protect the information resource(s) at risk.
- The incident response team shall initiate incident response procedures in the event of a security incident to contain the incident and protect the CU's information and information systems.
- Business risk and other criteria shall be defined to aid the escalation of incidents up the management chain based on the defined criteria.

Scope & Applicability

This policy shall apply to all the CU's data, systems, activities, and assets owned, leased, controlled, or used by the CU, its agents, contractors, or other business partners on behalf of the CU.

Role & Responsibilities

The **Board of Directors and CEO** are ultimately responsible for the cybersecurity program and thus also for the implementation of this policy.

Senior Management shall commit to provide resources and budget for incident management and response.

The **Manager, Risk and Compliance** role shall draft an incident management procedure and establish the incident management and response team.

The **Manager - Technology** is responsible to deploy best practices and tools to identify incidents and shall be responsible to assess the effectiveness of incident management procedures and tools in place.

The **manager/team leader** is responsible for ensuring all employees are trained to identify suspicious activities and report incidents to the incident management team.

The **employee** shall know the initial channel of communication to report incidents and suspicious activities.

18. Media Protection Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.GV-1, PR.DS-3, PR.IP-6, PR.PT-2

Purpose

The purpose of this policy is to define requirements for proper data sanitation and disposal of electronic storage media; and to establish device and media protection controls for the CU to reduce risk related to the storage, transport, and disposal of information.

Policy Statement

All electronic storage media used by the CU must be properly sanitized before being transferred, replaced, repaired or removed from service, and disposed of in an appropriate manner to prevent unauthorized access to CU data.

Scope & Applicability

This policy shall apply to all electronic storage media containing information owned or used by the CU.

Role & Responsibilities

Senior Management shall commit to provide resources and budget for incorporating media sanitation practices.

The **CAO** role shall draft media disposal standards, procedures and guidelines to securely dispose of, remove, repair or update storage media.

The **Manager - Technology** is responsible to ensure that CU data is properly destroyed or removed from media before the media leaves the controlled CU environment.

19. Contingency Planning Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.BA-2, ID.BE-3, ID.BE-4, ID.BE-5, ID.GV-3, ID.SC-5, PR.IP-9, PR.IP-10, PR.IP-12, PR.PT-5, DE.AE-2, DE.AE-4, DE.AE-5, RS.RP-1, RS.AN-2, RS.AN-4, RS.IM-1, RS.IM-2, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3

Purpose

Contingency planning minimizes the impact of a potentially damaging event on the information technology environment and organization. Contingency planning enables the CU to resume daily operations as soon as possible after an unforeseen event.

The purpose of this policy is to ensure that adequate planning and contingency is established to allow the CU to efficiently recover from unforeseen service disruption in a manner that maintains the confidentiality, integrity, and availability of the CU information assets during recovery activity.

Policy Statement

All information resource owners shall ensure contingency plans are documented for those information systems that are business- critical or subject to regulatory requirements.

The CU contingency plan should include:

- Identification of the key functional areas essential to business operations.
- Determination of how each potentially disruptive event (e.g. fire, flood, hurricane, etc.) would affect these key areas; what actions would be taken; and the resources needed to conduct each action.
- Procedures for restoring the CU's information systems, including the acquisition and maintenance of resources needed to facilitate the recovery and continuity of essential system functions;
- Processes for acquiring and maintaining the resources necessary to ensure the viability of the restoration procedures;
- Training for personnel to execute contingency procedures; and,
- Readiness and preparedness procedures for annual review and testing of the contingency plan.

Scope & Applicability

This policy applies to all information systems and information resources owned or operated by or on behalf of the CU.

Role & Responsibilities

Senior Management shall commit to provide resources and budget for contingency planning.

The **information/data/system owner** shall be responsible for data backup, configuration backup, and the contingency plan for the information system owned by them.

The **Manager, Risk and Compliance** will be responsible to align the contingency plan with risk tolerance capabilities of the organization.

The Individual employee is responsible for understanding and following contingency plans, related policies and procedures.

20. Acceptable Use Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.GV-3, PR.AC-1, PR.AC-2, PR.AC-4, PR.AC-6, PR.AT-2, PR.IP-6, PR.IP-11, PR.PT-2, PR.PT-3,

Purpose

The purpose of this policy is to outline the acceptable use of organization information system assets to reduce risks due to disclosure or modification of information, or service disruption, whether intentional or accidental as well as protecting electronic data and information systems including all confidential, personal and proprietary information.

Policy Statement

The CU's information and information system shall be used in an approved, ethical, and lawful manner to avoid loss or damage to corporate operations, financial interests or reputation.

- The CU shall ensure that individuals requiring access to organizational information and organization information systems acknowledge and accept appropriate access agreements.
- Managers shall provide the Acceptable Use Policy to all employees, contractors and 3rd party vendors.
- Management shall assign responsibility to a department, role or named individual to keep records of acknowledgement and acceptance (by signature) of the Acceptable Use Policy by employees and contractors.

Expected Behavior:

Those accessing CU information systems, shall use caution and exercise good security practices to ensure the protection of organizational information systems and data, including but not limited to:

- Using caution when opening email attachments or following hypertext links received from unknown senders.
- Selecting strong passwords; not writing them down; changing them frequently; and not sharing them with anyone.
- Complying with the Access Control Policy.
- Using available operating system functions to lock workstations when away from their desk.
- Assisting in enforcing physical access controls by challenging unauthorized personnel who may not be following procedures for visitor sign-in, appropriate badge use, escort control, and entry.
- Reporting any weaknesses in computer security or data privacy, suspicious behavior of others, and any incidents of possible misuse or violation of this policy to the proper authorities.
- Protecting confidential information.
- Labelling documents and information assets in alignment with the Data Classification Policy. Unlabeled data is assumed to be public.
- Encrypting confidential information that is transported or transmitted outside of the organization (via email, electronic messaging or any other medium) with an encryption standard established by the Security Officer or equivalent role.
- Store data in containers (Folders, Databases) in Credit Union network locations only.
- Access to these containers is based on security groups.
- Accessing Credit Union data remotely should be through VPN when possible.
- Privileged access is to be distributed in accordance of least privilege of the user role within the organization.
- Managers are responsible for the approval of data access roles for employees.

- Email must be encrypted when sending confidential information. Refer to the Privacy Policy.
- Personal email is not to be used when sending Credit Union data.
- Data cannot be stored or saved on computers not belonging to the Credit Union.
- Credit Union supplied encrypted USB drives are to be used if temporary data must be copied off of the network.
- Data in transit and at rest is to be encrypted with the minimum industry standards (AES 256 for example).
- Data that cannot be accessed by employees needs to be followed up with management to obtain access.
- Data will be retained in accordance with the Credit Union records management policy.
- Take appropriate precautions before deletion of data.
- Follow Credit Union privacy policies at all times.
- Storing information in accordance with the Media Protection Policy.

Prohibited behavior:

The following activities are strictly prohibited with no exceptions:

- Unauthorized access, interception, modification or destruction of any computer, computer system, organizational information system or computer programs.
- Installation of any computing device or software not authorized by management on CU information systems.
- Installation or use of any unauthorized software, including but not limited to security testing, monitoring, encryption or hacking software on CU information systems.
- Knowingly introducing a compute contaminant into any computer, computer system, or CU information system.
- Disabling software, modifying configurations or otherwise circumventing security controls.
- Tampering with physical security controls.

Scope & Applicability

This policy shall apply to all CU employees, agents, contractors, or other business partners on behalf of the CU.

Role & Responsibilities

Senior Management shall commit to provide and communicate the Acceptable Use Policy to all employees.

The **CAO** role shall draft acceptable use standards, procedure and guidelines.

The **Manager - Technology** shall be responsible to work with managers to identify the effectiveness of the Acceptable Use Policy.

21. Email Policy

Cybersecurity Policy Handbook (NIST Controls)

PR.AT-1

Purpose

The purpose of this policy is to ensure proper use of the CU's email system and make users aware of what the CU deems as acceptable and unacceptable use of the email system. This policy outlines the minimum requirements for use of the CU's email service.

Policy Statement

- Use of the CU's email service must be consistent with CU policies, applicable laws and proper business practices.
- CU email accounts shall be used primarily for CU business purposes; personal communication is permitted on a limited basis, but commercial use is prohibited.
- CU Email accounts shall be configured to have signatures and messages that discourage the misuse and unauthorized access of the email content.
- CU email boxes shall be stored securely and shall be retained according to the Data Retention Policy.
- CU email shall not be used to create or distribute disruptive/offensive messages.
- Users shall be prohibited from automatically forwarding CU email to a third party email system.
- Public/Other email services shall not be used for official CU purposes.
- The CU email system shall be supported by security tools/functions to restrict spam and phishing.
- Employees shall be trained to identify phishing emails and avoid responding to spam emails.

Scope & Applicability

This policy shall apply to all CU information systems owned by or operated on behalf of the CU. All employees, contractors and third-party vendors are responsible for adhering to this policy.

This policy does not supersede any other applicable law or higher-level company directive.

Role & Responsibilities

The **Board of Directors and CEO** are ultimately responsible for the cybersecurity program and thus also for the implementation of this policy.

The **Manager - Technology** role shall implement the tools to monitor email communication and protect from phishing and spam emails. They shall be responsible to ensure that email practices align with the Acceptable Use Policy and to restrict misuse of the email system.

Employees shall maintain their awareness to identify phishing emails and avoid responding to spam emails.

22. Physical and Environmental Protection Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.GV-1, PR.AC-2, PR.AT-5, PR.IP-5, DE.CM-2, DE.CM-3

Purpose

The purpose of this policy is to protect the CU's information systems and assets by limiting and controlling physical access and implementing controls to protect the environment in which CU information systems and assets are housed.

Policy Statement

The CU shall:

- Develop and maintain a physical access list of individuals with authorized access to controlled areas or facilities where the CU information systems reside.
- Issue authorized physical access credentials.
- Enforce physical access authorization at designated entry/exit points to CU facilities where information systems reside.
- Review and approve the physical access list and authorization credentials bi-annually.
- Remove individuals from the physical access list and revoke their access credentials when access is no longer required.
- Control ingress/egress to CU facilities using keys, locks, combinations, biometrics and/or security guards.
- Monitor physical access to CU facilities where information systems reside to detect and respond to physical security incidents.
- Ensure that visitors (not on the physical access list) to CU facilities where information systems reside are escorted at all times.
- Protect CU information systems from fire by implementing and maintaining fire suppression and detection systems in accordance with industry best practices for information system fire protection.

Scope & Applicability

This policy shall apply to all CU data, systems, activities, and assets owned, leased, controlled, or used by the CU, its agents, contractors, or other business partners on behalf of the CU.

This policy does not supersede any other applicable law or higher-level company directive.

Role & Responsibilities

The **CAO** role shall draft physical and environmental security standards and ensure that physical and environmental protection controls are aligned with NIST 800-53.

The **Manager -Technology** shall assess the physical security status of all CU information systems.

23. Backup and Recovery Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.AM-5, ID.BE-2, ID.BE-3, ID.BE-4, ID.BE-5, PR.DS-1, PR.IP-4, PR.IP-6, PR.IP-9, PR.IP-10, PR.PT-5, RC.RP-1, RC.IM-1, RC.RM-2

Purpose

The primary purpose of the policy is to protect the CU data and outline the requirements for data backup and recovery in accordance with the CU's Business Continuity Plan (BCP) and Disaster Recovery (DR) Plan.

Policy Statement

The CU shall:

- Ensure the backup and restoration of the CU electronic information is planned and executed in a timely, effective and secure manner and in alignment with the BCP and DRP plans.
- Classify all CU information systems based on criticality and classification.
- Encrypt and label/classify data at rest based on the sensitivity and value of the information.
- Store/host the backups in an environmentally protected and access controlled secure offsite location.
- Shall maintain and dispose of backups in accordance with the CU's Data Retention Policy and Media Protection Policy.
- Shall perform recovery tests quarterly.

Scope & Applicability

This policy shall apply to all the CU's data, systems, activities, and assets owned, leased, controlled, or used by the CU, its agents, contractors, or other business partners on behalf of the CU.

Role & Responsibilities

Senior Management shall commit to provide resources and budget to deploy backup and restoration procedures.

The **CAO** shall approve backup and restoration procedures and guidelines and monitor the effectiveness of the backup and restoration procedures.

The **Manager - Technology** shall assist in the development of backup and restoration procedures and is responsible for ensuring that all back ups are conducted securely and tested quarterly.

24. Privacy Authorization Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.GV-4, PR.PT-3, DE.AE-3

Purpose

The purpose of this policy is to outline the requirements for safeguards to protect the privacy of all Personally Identifiable Information (PII) collected, used or disclosed by the CU.

Policy Statement

The CU shall:

- Implement safeguards to protect PII that is collected, used or disclosed by the CU.
- Conduct Privacy Impact Assessments (PIA) to assess and document the legal authority to collect, use and disclose PII.
- Require consent to collect, use or disclose PII except where required or permitted by law.
- Communicate the purpose for collecting, using and disclosing PII in privacy notices.
- Develop guidelines for disclosing PII in compliance with the Privacy Act.
- Implement Data Loss Prevention tools to control and monitor disclosure of PII.
- Ensure that all access to PII is recorded in audit logs and that reports can be provided upon request to identify who in the CU has accessed PII.

Scope & Applicability

This policy shall apply to all CU employees and contractors working on behalf of the CU who handle, control, or access information system that contain PII.

Role & Responsibilities

The **Board of Directors and CEO** are responsible for the implementation of this policy.

The **Manager, Risk and Comnpliance** shall be responsible for PIAs and shall have an understanding of PII collection, reuse and disposal.

25. Data Classification Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.AM-5, ID.BE-2, ID.BE-3, ID.BE-4, ID.BE-5, ID.GV-3, PR.IP-6

Purpose

The purpose of this policy is to outline requirements for the classification of data. Data classification is the foundation upon which security controls, data retention, backup and disaster recovery is based. Data classification has a direct impact on budget as it requires the business to align the value of its data versus its risk appetite.

Policy Statement

All data created, stored, processed, or transmitted by the CU shall be classified according to the impact that unauthorized disclosure, modification, or loss of the data will have on the business.

Data Classification Categories:

All CU data shall be classified as one of the following categories:

Confidential data: data that shall be protected from unauthorized disclosure based on the law, regulations, or legal agreements.

Examples of confidential data include, but are not limited to:

- Personally Identifiable Information;
- Financial account data;
- System security parameters and vulnerabilities (access credentials, encryption keys, firewall tables, etc.);
- Information system configuration and network architecture details;
- Risk assessment documents;
- Audit documents.

Public Data: data that may be released to the public and requires no additional levels of protection from unauthorized disclosure.

Scope & Applicability

This policy shall apply to all data, created, stored, processed or transmitted within the CU.

Role & Responsibilities

The **Board of Directors and CEO** are ultimately responsible for the cybersecurity program and thus also for the implementation of this policy.

Senior Management shall commit to provide resources and budget for providing tools and training to deploy mechanisms for data classification.

The **Manager, Risk and Compliance** shall be responsible for defining the data classification standards and the security control standards for each classification.

The **Manager - Technology** role is responsible for deploying security controls and tools based on data classification levels.

The **Data Owner** shall

- Assign the classification of the data;
- Assign data custodians and ensure data custodians are familiar with the security requirements based on data classification levels.

The **Data Custodian** shall ensure implementation of security controls according to data classification levels.

26. Cloud Based Productivity Solution Policy

Purpose

The purpose of this policy is to regulate the usage of cloud based productivity solutions in a safe and confidential manner.

Policy Statement

This policy is for the safety and security of access and usage with cloud based productivity solutions in compliance with CU business practices in the handling of sensitive CU and client data.

Effective Storage Practices:

- Geographical Storage – data is to be stored in cloud containers in Canadian data centre(s)
- Encryption – data at rest should be strongly encrypted using AES or RSA

Effective Use Practices:

- MFA and/or VPN connection should be enabled.
- Access to cloud based productivity solutions should be done on CU approved devices only – this includes computers, laptops, mobile devices (cell phones, tablets)
- Least privilege concepts should be used when setting up individual users for all components in the cloud based productivity solution
- No usage for employees outside of CU branch unless VPN and/or MFA is established or unless an exception has been made by IT Security Officer/IT Management.
- No usage of cloud based productivity solutions outside of Canada unless an exception has been made by IT Security Officer/IT Management.

Scope & Applicability

Cloud based productivity solutions include but are not limited to; Office 365 and Google Workspace.

Role & Responsibilities

The **Board of Directors and Chief Executive Officer (CEO)** are ultimately responsible for the cybersecurity program and thus also for the implementation of this policy.

Managers and team leaders shall ensure that all employees are aware and complying with these practices.

The **CAO** shall be responsible for defining appropriate security measures for these tools.

The **Manager -Technology** will implement a management plan for these resources and ensure all security measures have been reviewed and implemented.

27. Personal and Corporate Mobile Device Usage Policy

Cybersecurity Policy Handbook (NIST Controls)

DE.CM-5

Purpose

The purpose of this policy outlines the use of mobile device(s) by employees of CU.

Policy Statement

This policy is for the safety and security of access and usage on mobile devices in compliance to CU business practices and handling of sensitive CU and client data.

Scope & Applicability

The use of personal and corporate mobile device(s) may be limited to certain employees as determined by management.

- Mobile devices are defined as but not limited to cell phones, tablets, laptops and any other hand held or portable device that can access the internet and/or the CU's network.

The CU employee must adhere to the following when using the device for CU purposes:

- Personal mobile device for CU business use must be approved by management before usage.
- All mobile devices must be password protected.
- Only approved apps can be used on corporate devices.
- Laptops may only be connected to a secure internet connection and a VPN is needed to access sensitive CU business and client information.

Roles & Responsibilities

The **Board of Directors and Chief Executive Officer (CEO)** are ultimately responsible for the cybersecurity program and thus also for the implementation of this policy.

Senior Management shall determine who requires access to CU resources either through corporate and/or personal mobile devices.

The **CAO** shall be responsible for defining appropriate security measures for mobile devices.

The **Manager -Technology** will implement a management plan for mobile devices and ensure all security measures have been reviewed and implemented.

28. Third Party Vendor/Partner Contract Policy

Cybersecurity Policy Handbook (NIST Controls)

ID.SC-1, ID.SC-2, ID.SC-3, ID.SC-4, ID.SC-5

Purpose

The purpose of this policy outlines the minimal contractual requirements for third party vendors/partners of CU.

Policy Statement

This policy is for the safety and security of access and services rendered to the CU in compliance to CU business practices and handling of sensitive CU areas and inadvertent viewing of client data.

Scope & Applicability

This policy is to regulate third party contracts with vendors/partners to ensure the safety and reliability of services offered and rendered. It is also to comply with security frameworks in relation to vendors accessing sensitive areas of the CU.

Role & Responsibilities

The following should be included in Supply Chain (SC) contracts with 3rd party vendors / partners:

- Security background checks are conducted by the vendor for their employees, especially for employees who provide support and services to the CU.
- Contact information (phone and email) is provided and updated for primary and secondary contacts at the vendor for security related matters and events.
- Evidence of security assessments and audits that include security, will be provided upon request (or regularly) to the CU.
- The vendor will provide (or contract includes) the process and procedure for reporting, escalating and responding to security related events that are related to or involve the vendor.
- The vendor will provide (or contract includes) the process and procedure for requesting, authorizing, gaining, removing and recording any access required by the vendor to the CU IT network, assets and/or premises.

This is a minimal requirement list which can be expanded to include any other items the CU views as necessary or valuable in vendor contracts.

The CU shall maintain a list of qualified vendors and review this list annually

The **Board of Directors and Chief Executive Officer (CEO)** are ultimately responsible for the cybersecurity program and thus also for the implementation of this policy.

Senior Management shall ensure all contracts are reviewed on a regular bases and complies with NIST 800-53.

The **Manager, Risk and Compliance** role shall be responsible for the security controls that are incorporated in all third party contracts and ensure all appropriate measures have been complied with.

Index

Contingency Planning Policy, pg37

Backup and Recovery Policy, pg43

Data Classification Policy, pg45

ID.BE-5:

Asset Management Policy, pg27

Contingency Planning Policy, pg37

Backup and Recovery Policy, pg43

Data Classification Policy, pg45

ID.GV-1:

Cybersecurity Program Management Policy, pg11

Security and Privacy Planning Policy, pg14

Personnel Security Policy, pg15

Risk Assessment Policy, pg16

Access Control Policy, pg20

Identification and Authentication Policy, pg25

System and Communication Protection Policy, pg26

Antivirus, Patch Management and Vulnerability Management Policy, pg30

Assessment, Authorization and Monitoring Policy, pg32

Media Protection Policy, pg36

Physical and Environmental Protection Policy, pg42

ID.GV-2:

Cybersecurity Program Management Policy, pg11

Security and Privacy Planning Policy, pg14

Personnel Security Policy, pg15

Risk Assessment Policy, pg16

ID.GV-3:

Security and Privacy Planning Policy, pg14

Risk Assessment Policy, pg16

Audit and Accountability Policy, pg22

Assessment, Authorization and Monitoring Policy, pg32

Contingency Planning Policy, pg37

Acceptable Use Policy, pg39

Privacy Authorization Policy, pg44

Data Classification Policy, pg45

ID.GV-4:

Risk Assessment Policy, pg16

System and Information System Ownership Policy, pg19

Antivirus, Patch Management and Vulnerability Management Policy, pg30

ID.RA-1:

Risk Assessment Policy, pg16

Application Security Policy, pg29

Antivirus, Patch Management and Vulnerability Management Policy, pg30

ID.RA-2:

Awareness and Training Policy, pg13

ID.RA-3:

Cybersecurity Program Management Policy, pg11

Risk Assessment Policy, pg16

System and Information System Ownership Policy, pg19

Configuration/Change Management Policy, pg23

System and Communication Protection Policy, pg26

Antivirus, Patch Management and Vulnerability Management Policy, pg30

Assessment, Authorization and Monitoring Policy, pg32

ID.RA-4:

Risk Assessment Policy, pg16

System and Information System Ownership Policy, pg19

Asset Management Policy, pg27

Antivirus, Patch Management and Vulnerability Management Policy, pg30

Assessment, Authorization and Monitoring Policy, pg32

ID.RA-5:

Risk Assessment Policy, pg16

System and Information System Ownership Policy, pg19

System and Communication Protection Policy, pg26

Antivirus, Patch Management and Vulnerability Management Policy, pg30

Assessment, Authorization and Monitoring Policy, pg32

ID.RA-6:

Risk Assessment Policy, pg16

System and Information System Ownership Policy, pg19

System and Communication Protection Policy, pg26

Antivirus, Patch Management and Vulnerability Management Policy, pg30

Assessment, Authorization and Monitoring Policy, pg32

ID.RM-1:

Risk Assessment Policy, pg16

ID.RM-2:

Risk Assessment Policy, pg16

ID.RM-3:

Risk Assessment Policy, pg16

ID.SC-1:

Cybersecurity Program Management Policy, pg11

Risk Assessment Policy, pg16

System and Service Acquisition Policy, pg18

Third Party Vendor/Partner Contract Policy, pg49

ID.SC-2:

Cybersecurity Program Management Policy, pg11

Risk Assessment Policy, pg16

Asset Management Policy, pg27

Third Party Vendor/Partner Contract Policy, pg49

ID.SC-3:

Personnel Security Policy, pg15

System and Service Acquisition Policy, pg18

Third Party Vendor/Partner Contract Policy, pg49

ID.SC-4:

Cybersecurity Program Management Policy, pg11

Risk Assessment Policy, pg16

Third Party Vendor/Partner Contract Policy, pg49

ID.SC-5:

Contingency Planning Policy, pg37

Third Party Vendor/Partner Contract Policy, pg49

PR.AC-1:

Security and Privacy Planning Policy, pg14

Personnel Security Policy, pg15

System and Information System Ownership Policy, pg19

Access Control Policy, pg20

Identification and Authentication Policy, pg25

Acceptable Use Policy, pg39

PR.AC-2:

Acceptable Use Policy, pg39

Physical and Environmental Protection Policy, pg42

PR.AC-3:

Access Control Policy, pg20

PR.AC-4:

Access Control Policy, pg20

Identification and Authentication Policy, pg25

Acceptable Use Policy, pg39

PR.AC-5:

Assessment, Authorization and Monitoring Policy, pg32

PR.AC-6:

Access Control Policy, pg20

Identification and Authentication Policy, pg25

Acceptable Use Policy, pg39

PR.AT-1:

Awareness and Training Policy, pg13

Incident Response Policy, pg34

Email Policy, pg41

PR.AT-2:

Access Control Policy, pg20

Identification and Authentication Policy, pg25

Acceptable Use Policy, pg39

PR.AT-3:

Personnel Security Policy, pg15

PR.AT-4:

Personnel Security Policy, pg15

PR.AT-5:

Physical and Environmental Protection Policy, pg42

PR.DS-1:

System and Communication Protection Policy, pg26

Backup and Recovery Policy, pg43

PR.DS-2:

System and Communication Protection Policy, pg26

PR.DS-3:

Media Protection Policy, pg36

PR.DS-4:

System and Communication Protection Policy, pg26

PR.DS-5:

System and Communication Protection Policy, pg26

PR.DS-6:

System and Communication Protection Policy, pg26

PR.DS-7:

Configuration/Change Management Policy, pg23

Application Security Policy, pg29

PR.DS-8:

System and Information System Ownership Policy, pg19

Antivirus, Patch Management and Vulnerability Management Policy, p30

PR.IP-1:

Configuration/Change Management Policy, pg23

PR.IP-2:

Configuration/Change Management Policy, pg23

Application Security Policy, pg29

PR.IP-3:

Configuration/Change Management Policy, pg23

PR.IP-4:

Backup and Recovery Policy, pg43

PR.IP-5:

Physical and Environmental Protection Policy, pg42

PR.IP-6:

Media Protection Policy, pg36

Acceptable Use Policy, pg39

Backup and Recovery Policy, pg43

Data Classification Policy, pg45

PR.IP-7:

Risk Assessment Policy, pg16

System and Communication Protection Policy, pg26

PR.IP-8:

Awareness and Training policy, p13

Antivirus, Patch Management and Vulnerability Management Policy, p30

PR.IP-9:

Incident Response Policy, pg34

Contingency Planning Policy, pg37

Backup and Recovery Policy, pg43

PR.IP-10:

Incident Response Policy, pg34

Contingency Planning Policy, pg37

Backup and Recovery Policy, pg43

PR.IP-11:

System and Information System Ownership Policy, pg19

Access Control Policy, pg20

Acceptable Use Policy, pg39

PR.IP-12:

Risk Assessment Policy, pg16

Antivirus, Patch Management and Vulnerability Management Policy, pg30

Contingency Planning Policy, pg37

PR.MA-1:

Asset Management Policy, pg27

PR.MA-2:

Access Control Policy, pg20

PR.PT-1:

Audit and Accountability Policy, pg22

Application Security Policy, pg29

PR.PT-2:

Configuration/Change Management Policy, pg23

Media Protection Policy, pg36

Acceptable Use Policy, pg39

PR.PT-3:

Access Control Policy, pg20

Identification and Authentication Policy, pg25

System and Communication Protection Policy, pg26

Acceptable Use Policy, pg39

Privacy Authorization Policy, pg44

PR.PT-4:

Audit and Accountability Policy, pg22

Application Security Policy, pg29

PR.PT-5:

Incident Response Policy, pg34

Backup and Recovery Policy, pg43

Contingency Planning Policy, pg37

DE.AE-1:

Configuration/Change Management Policy, pg23

DE.AE-2:

Risk Assessment Policy, pg16

System and Communication Protection Policy, pg26

Incident Response Policy, pg34

Contingency Planning Policy, pg37

DE.AE-3:

Audit and Accountability Policy, pg22

Application Security Policy, pg29

Assessment, Authorization and Monitoring Policy, pg32

Privacy Authorization Policy, pg44

DE.AE-4:

Risk Assessment Policy, pg16

System and Communication Protection Policy, pg26

Incident Response Policy, pg34

Contingency Planning Policy, pg37

DE.AE-5:

Incident Response Policy, pg34

Contingency Planning Policy, pg37

DE.CM-1:

Risk Assessment Policy, pg16

Assessment, Authorization and Monitoring Policy, pg32

Incident Response Policy, pg34

DE.CM-2:

Risk Assessment Policy, pg16

Physical and Environmental Protection Policy, pg42

DE.CM-3:

Personnel Security Policy, pg15

Physical and Environmental Protection Policy, pg42

DE.CM-4:

System and Information System Ownership Policy, pg19

Antivirus, Patch Management and Vulnerability Management Policy, pg30

DE.CM-5:

System and Information System Ownership Policy, pg19

Access Control Policy, pg20

Antivirus, Patch Management and Vulnerability Management Policy, pg30

Personal and Corporate Mobile Device Usage Policy, pg48

DE.CM-6:

Access Control Policy, pg20

DE.CM-7:

System and Information System Ownership Policy, pg19

Access Control Policy, pg20

Audit and Accountability Policy, pg22

Configuration/Change Management Policy, pg23

Antivirus, Patch Management and Vulnerability Management Policy, pg30

Assessment, Authorization and Monitoring Policy, pg32

Incident Response Policy, pg34

DE.CM-8:

Risk Assessment Policy, pg16

Application Security Policy, pg29

Antivirus, Patch Management and Vulnerability Management Policy, pg30

DE.DP-1:

Risk Assessment Policy, pg16

System and Information System Ownership Policy, pg19

Application Security Policy, pg29

Antivirus, Patch Management and Vulnerability Management Policy, pg30

DE.DP-2:

Antivirus, Patch Management and Vulnerability Management Policy, pg30

DE.DP-3:

Assessment, Authorization and Monitoring Policy, pg32

DE.DP-4:

Incident Response Policy, pg34

DE.DP-5:

Incident Response Policy, pg34

RS.RP-1:

Incident Response Policy, pg34

Contingency Planning Policy, pg37

RS.CO-1:

Incident Response Policy, pg34

RS.CO-2:

Incident Response Policy, pg34

RS.CO-3:

Incident Response Policy, pg34

RS.CO-4:

Incident Response Policy, pg34

RS.CO-5:

Incident Response Policy, pg34

RS.AN-1:

Risk Assessment Policy, pg16

System and Information System Ownership Policy, pg19

Assessment, Authorization and Monitoring Policy, pg32

RS.AN-2:

Assessment, Authorization and Monitoring Policy, pg32

Contingency Planning Policy, pg37

RS.AN-3:

Risk Assessment Policy, pg16

Incident Response Policy, pg34

RS.AN-4:

Incident Response Policy, pg34

Contingency Planning Policy, pg37

RS.MI-1:

Incident Response Policy, pg34

RS.MI-2:

Risk Assessment Policy, pg16

Antivirus, Patch Management and Vulnerability Management Policy, pg30

Incident Response Policy, pg34

RS.MI-3:

Risk Assessment Policy, pg16

System and Information System Ownership Policy, pg19

Antivirus, Patch Management and Vulnerability Management Policy, pg30

Incident Response Policy, pg34

RS.IM-1:

Incident Response Policy, pg34

Contingency Planning Policy, pg37

RS.IM-2:

Incident Response Policy, pg34

Contingency Planning Policy, pg37

RC.RP-1:

Contingency Planning Policy, pg37

Backup and Recovery Policy, pg43

RC.IM-1:

Contingency Planning Policy, pg37

Backup and Recovery Policy, pg43

RC.IM-2:

Contingency Planning Policy, pg37

Backup and Recovery Policy, pg43

RC.CO-1:

Contingency Planning Policy, pg37

RC.CO-2:

Contingency Planning Policy, pg37

RC.CO-3:

Contingency Planning Policy, pg37