Summary: ACENET Cybersecurity Policy

1. Introduction

ACENET is committed to protecting the confidentiality, integrity, and availability of assets managed by ACENET.

This document is intended as a high-level summary of our security policy, which provides a framework for:

- Protecting information and infrastructure from unauthorized access, misuse, and exfiltration
- Ensuring the availability and effectiveness of security controls
- Communicating roles and responsibilities shared by all parties
- Ensuring business continuity and mitigating the cybersecurity risks

The overviews provided in Sections 2 through 12 are supported by a number of controls delivered through detailed internal policies, standards, processes, and procedures.

In addition to ACENET's role and responsibilities, our users agree to protect information and prevent misuse of resources by adhering to the Compute Canada's Terms of Use - https://www.computecanada.ca/research-portal/information-security/

2. Asset Management

2.1 All assets managed by ACENET including, but not limited to data, devices, systems and facilities are appropriately identified and protected.

2.2 Following the determination of asset ownerships, roles and responsibilities to ensure their security are defined in the asset's related policies and procedures.

3. Risk Management

3.1 All known cybersecurity risks to ACENET operations, assets, and individuals are identified, assessed, managed, and reviewed on a regular basis.

3.2 ACENET's priorities, constraints, assumptions, and risk tolerances are established and are used to support operational risk response decisions.

4. Access Control

4.1 ACENET follows proper identification and authentication management standards for all users on all systems.

4.2 Access limitations are enforced through the Separation of Duties and Least Privilege principles.

5. Awareness & Training

5.1 ACENET's cybersecurity team is developing and implementing a security awareness program to ensure that all ACENET employees and system users are attentive to the importance of information security.

5.2 All cybersecurity team members subscribe to authoritative security mailing lists and alert notification services to maintain the awareness of cybersecurity industry alerts.

6. Data Security

6.1 ACENET data is managed in accordance with its internal security policies to protect the confidentiality, integrity, and availability of information.

6.2 Client data is managed according to ACENET's Data Policies and/or user agreements.

7. Configuration Management

7.1 System configuration management is consistent with industry-accepted system-hardening standards.

7.2 Changes to systems are tested, validated, and documented prior to their implementation.

8. Operations Management

8.1 The ACENET cybersecurity team conducts regular reviews to confirm operators and users are adhering to security policies and procedures.

8.2 Appropriate audits, vulnerability scans and continuous monitoring activities are implemented to ensure security vulnerabilities are assessed and patches are up to date.

9. Incident Management

9.1 Security incidents are identified, reported, handled, documented and monitored in a timely manner according to an established incident response procedure.

9.2 Post-incident analyses and reports are prepared following critical cybersecurity incidents. Legal or contractual advice may be included, if applicable.

10. Business Continuity Management

10.1 A business continuity plan is in place to minimize the impact of cybersecurity events on assets managed by ACENET. It is reviewed regularly.

10.2 Recovery processes and procedures are maintained and executed to ensure timely restoration of assets managed by ACENET and services affected by cybersecurity events.

11. Auditing

11.1 ACENET creates, protects, and retains system audit records for monitoring analysis, investigation, and reporting of unauthorized or inappropriate activities by ensuring traceability and accountability.

12. Compliance

12.1 ACENET abides by all federal and provincial laws, statutory, regulatory or contractual obligations applicable to its information systems.