BOARD POLICY
Information Security

Policy Management Responsibility
Chief Transformation Officer
Oversight by the Finance Audit and Technology Committee
Approval by Board of Directors

PURPOSE AND SCOPE

United Way of Calgary and Area (United Way) is committed to protecting its corporate Information Assets and supporting Information System Assets, and meeting all legal, regulatory, statutory, contractual, and operational requirements.

United Way's Information Security Policy (Policy) and the Operating Policy and Procedures – Information Security (Procedures) contain operational policies, standards and guidelines intended to establish reasonable and appropriate requirements for the secure delivery of United Way's services. Secure service delivery requires the assurance of confidentiality, integrity, availability, and privacy of United Way's valuable Information Assets through:

- Governance processes for information technology;
- Defined security responsibilities;
- Management business processes that include and enable security processes;
- Providing operational security, and protection of networks and Information System Assets;
- Safe-guarding Information Assets and Information System Assets utilized by third parties; and,
- Monitoring for compliance.

United Way recognizes that the management of information security is a process which to be effective, requires executive and management commitment, the active participation of all staff, and ongoing awareness programs.

The Information Security Policy establishes requirements to ensure that information security controls remain current as business needs evolve and technology changes. It is a key factor in ensuring the business continuity of United Way and helps minimize the risk of damage by preventing security incidents and reducing their potential impact.

The Policy's goal is to protect the United Way's Information Assets and supporting Information System Assets against all internal, external, deliberate, or accidental threats.
To create ongoing awareness and compliance, this Policy must be published and communicated to all staff, volunteers, and relevant external parties.

DEFINITIONS

Information Asset

Information and Information Asset includes any data relating to United Way's business, used in the management (storing, transmitting, accessing, capturing, sharing, and reporting) of corporate information, no matter what form it is in (including electronic and paper-based) or how it is created, distributed or used, and can pertain to United Way's brand, reputation, ideas, inventions, improvements, intellectual property, registered and

	unregistered copyrights, trademarks, patents, and service marks or trade secrets that are conceived, developed, or practiced. Examples of Information and Information Assets include, but are not limited to, confidential information of donors, staff, agencies, contractors, vendors, partners, and volunteers.
Information System Asset	Information System Asset or IS Asset includes any equipment or service owned, licensed or otherwise utilized by United Way that can be used for communication or to create, reproduce, or distribute information. Examples include, but are not limited to, desktop computers, laptops, tablets, mobile phones, smart phones, mobile devices (whether personally owned or corporately owned by United Way), Wi-Fi, remote access, shared drives, document management systems, email systems, instant messaging systems, file-servers, network equipment, databases, applications, web applications, software-as-a-service, platform-as-a-service, internet connections, printers, multifunction devices, and telephones.

POLICY STATEMENT

Information developed by or for United Way is considered a valuable and confidential corporate asset is to be treated as United Way property and must be appropriately protected. United Way Information Assets and Information System Assets obtained and used by staff, volunteers, contractors, and supervisors must be properly managed and protected.

United Way will deploy and regularly upgrade suitable software, and follow current leading practices for:

- Protection of information against any unauthorized access;
- Confidentiality of information ;
- Integrity of information ; and,
- Availability of information for business processes.

United Way will take reasonable steps to:

- Meet legislative and regulatory requirements;
- Develop, maintain and test business continuity plans;
- Provide Information Security Policy awareness and appropriate training for all staff, contractors, volunteers, and supervisors, vendors, partners, and third parties;
- Design physical security requirements for Information System Assets appropriate to United Way's needs;
- Report all actual or suspected information security breaches and thoroughly investigate and remediate;
- Support the Policy with procedures, including malware control measures, passwords, and business continuity plans; and,
- Properly classify, label, and handle Information Assets with appropriate disposal.

Applicability and Accountability

Compliance with the Information Security Policy and related policies, Procedures, and standards is mandatory. All United Way staff, contractors, volunteers, supervisors, vendors, partners, and third-parties are required to:

- Protect United Way's Information Assets in accordance with this Policy and related practices;
- Take accountability for applying appropriate security measures for Information entrusted to them; and,
- Report security incidents and assist investigations relating to information mismanagement and misuse.

All supervisors are directly responsible for implementing the Policy and ensuring staff compliance in their respective departments.

The Chief Information Security Officer (currently the Chief Transformation Officer) is responsible for overseeing compliance with the Policy and providing support and advice during its implementation.

Exceptions

Deviations from this Policy and Procedures, must be based on a legitimate business need and must follow the United Way's Information Security Exception Request Process as set out and defined in the Procedures. Exceptions are granted on a temporary basis and require joint approval from the Chief Information Security Officer and the appropriate level of management.

Enforcement

Violation of this Information Security Policy and related policies, Procedures, and standards may result in disciplinary action up to and including termination of employment, contract or services agreement and/or legal action. Reports of violations of this Policy will be forwarded to the appropriate Supervisor, People and Culture representative, and Chief Information Security Officer. In cases where local or international law is violated, United Way has a responsibility to involve the relevant law enforcement agencies.

Related Policies

Board Policies
• Privacy

Operating Policies and Procedures
• Acceptable Use of Technology
• Information Security
• Information Classification
• Mobile Devices
• Privacy and Security Breach Management
• Privacy Procedure and Guidelines for staff

Effective date
This Policy shall have effect from November 2018

Revisions
Review Frequency: 12 months
Last review: June 2023
Last revision: June 2023
Date of last Board approval: October 19, 2023