UNIVERSITY OF TORONTO | Information Security

Office of the Chief Information Security Officer

Insider threat guidelines

UNIVERSITY OF TORONTO | Information Security

Insider threat guidelines

Last reviewed:

Overview

Preamble

This guideline is designed to highlight the risks posed by insider threats and mitigate these risks by establishing a secure environment through proactive measures, continuous monitoring and effective response strategies. Insider threats can stem from current or former employees, contractors or other trusted individuals who have access to the institution's resources and may misuse this access. These threats can result in:

- **Data breaches**: Unauthorized access to sensitive information, leading to exposure of confidential data.
- **Intellectual property theft**: Stealing proprietary information, trade secrets or research, which can undermine the University of Toronto's competitive edge.
- **Operational disruptions**: Interfering with the institution's processes and systems, causing delays, inefficiencies or complete shutdowns.
- **Financial losses**: Direct theft or fraud, as well as costs associated with responding to and recovering from insider incidents.
- **Reputational harm**: Damage to the institution's reputation and trustworthiness, which can affect relationships with stakeholders, partners and the public.
- **Endangering the safety and well-being of our community**: Actions that compromise the physical or psychological safety of employees, students or other community members.

Insider threats may be intentional or unintentional, arising from negligence, malicious intent or coercion, which are mitigated by the following strategies:

- **Asset management:** Identify all assets, implement automated systems to maintain complete and accurate records and prioritize critical assets to ensure they receive the highest level of protection.
- **Strong access controls and identity management**: Implement robust access controls and identity management practices, including role-based access, multi-factor authentication and password management to enhance security.
- **Continuous monitoring and behaviour detection**: Use security information and event management (SIEM) tools for continuous monitoring and detection of unusual behaviour, maintaining comprehensive system documentation to facilitate effective incident response.
- **Incident response and business continuity**: Develop and maintain an incident response plan, conduct regular tabletop exercises and ensure business continuity plans are in place for disruptions to critical services resulting from natural disasters, cyber attacks and other incidents.
- **Building a security culture**: Cultivate a security-aware environment through regular security awareness training, clear contractual and access agreements and comprehensive personnel screening to prevent insider threats.

These strategies aim to create a secure environment by proactively addressing potential insider threats.

Purpose

The purpose of these guidelines is to provide a comprehensive framework for identifying, mitigating and responding to insider threats within U of T. By implementing these guidelines, the institution aims to protect its assets, maintain the integrity of its operations and ensure the safety of its community.

Audience

These guidelines are intended for the entire University community, including executive management, IT security teams, human resources, faculty, staff and students. It is essential that everyone understands their role in preventing and responding to insider threats.

Scope and applicability

These guidelines apply to all individuals who have access to the institution's information systems, data and physical facilities. They encompass all forms of insider threats, whether intentional or unintentional, and cover a wide range of activities, including data access, handling and sharing. The guidelines are designed to be in alignment with the University's Information Security Control Standard.

Guidelines

To effectively mitigate insider threats, the following guidelines outline a comprehensive approach that includes establishing a culture of security, implementing personnel screening and training, enforcing access control and monitoring, developing incident response and management strategies and protecting critical assets and data. These guidelines aim to create a secure environment by integrating proactive measures, continuous monitoring and effective response strategies.

Security culture and training:

- **Leverage the Security Awareness and Training (SAT) platform to conduct regular security awareness training for all employees**, emphasizing the importance of recognizing and reporting insider threats. This ongoing training ensures employees stay informed about the latest threats and are equipped with the knowledge to respond effectively.
    - If SAT onboarding isn't in place, update user onboarding to include it by default for all new staff.
    - Educate the community on secure data handling to prevent breaches. SAT covers storage, access control, encryption and secure communication.

- **Utilize institutional policies, security standards and procedures that outline acceptable use of resources** and the consequences of policy violations. Clear policies provide a framework for acceptable behaviour and set expectations, helping to prevent insider threats.
- **Perform background checks for new hires and regularly reassess** the backgrounds of current employees—depending on their role—to uncover potential risks. These checks

help detect individuals with a history of risky behaviour, thereby decreasing the chances of insider threats.

- **Leverage specialized training for individuals in higher-risk roles** to ensure they comprehend the specific threats and mitigation strategies pertinent to their positions. Such targeted training equips employees in sensitive roles with the necessary knowledge to address and mitigate specific threats.
    - If there are gaps in training for higher-risk roles, request a new module on the SAT platform.

Asset management and physical security

- **Maintain an accurate inventory of physical and logical assets** and implement tracking and recovery processes to ensure assets are accounted for, protected and recoverable. Accurate asset management ensures that all assets are tracked and protected, reducing the risk of insider threats exploiting unaccounted-for resources.
- **Identify critical assets and implement security measures** such as encryption and data loss prevention to prevent access to and exfiltration of sensitive information.
- **Manage risks from partners and third-party providers** by conducting thorough due diligence, establishing clear security requirements and regularly assessing their compliance with institutional security policies and standards. Managing third-party risks ensures that partners and providers adhere to the same security standards, reducing the risk of insider threats originating from external sources.
- **Implement physical access controls**, ensuring that physical keys are treated as assets and access is revoked when necessary. Migrate to digital locks and auditing to enhance security and track access. Physical access controls prevent unauthorized individuals from accessing sensitive areas, reducing the risk of physical insider threats.

Access control and identity management

- **Implement role-based access controls** to ensure that individuals only have access to the information necessary for their role. This limits the exposure of sensitive information, reducing the risk of insider threats.
- **Standardize and automate onboarding, cross-boarding and offboarding** procedures to ensure consistent application of access controls, timely revocation of access for departing employees, adjustments for changes in responsibilities within the same role and proper entitlement management. This prevents former employees or those with changed roles from retaining unnecessary access.
- **Regularly review and attest to access entitlements**, identifying and addressing any cross-boarding and off-boarding process failures. Regular reviews help ensure that only authorized individuals have access to sensitive information.
- **Reduce multiple user-level identities** by consolidating accounts and simplifying access management. This reduces the risk of insider threats exploiting multiple accounts.
- **Implement federated, conditional access and reduce access mechanisms** to streamline and secure access control. Limit the use of external systems to verified and trusted services to minimize potential security risks.

- **Ensure the use of strong, unique passwords** and implement multi-factor authentication (MFA) to enhance security and prevent unauthorized access. Strong passwords and MFA add layers of security, making it more difficult for insider threats to gain access.
- **Leverage a password manager** (e.g. 1Password) to generate and store passwords. This ensures that passwords are strong, unique and securely stored.
    - **1Password employee vault**: Provided to staff and faculty for generating and storing passwords for University-issued identities under an enterprise agreement, ensuring enterprise monitoring and recoverability.
        - **Personal credentials (e.g. online banking) must *never* be stored in an employee vault** to protect the individual and prevent unnecessary potential liability for the University.
    - **1Password family vault**: Provided to students, staff and faculty to generate and store passwords for personal identities (e.g. Gmail) securely. This is a personal agreement with the vendor, not the University, ensuring access is not lost with role changes and enabling protection capabilities beyond the individual to their family.
        - **Institutional-issued credentials must *never* be stored in the family vault** to protect the individual from unnecessary liability and their assigned identities from accidental exposure.
- **Leverage privileged identity access management (PIAM) tools for managed accounts** for applications, services and system recovery to enhance security and streamline privileged access management. This helps secure and control access to critical systems and data.

Monitoring and detection

- **Utilize SIEM tools** to ensure continuous monitoring, visibility, correlation, detection and response to unusual behaviour, such as unauthorized access attempts or data exfiltration.
- **Monitor, respond to and mitigate unusual behaviour** that may indicate an insider threat, such as accessing restricted areas or disclosing sensitive information. Monitoring and responding to unusual behaviour helps detect and mitigate insider threats before they cause significant harm.
- **Maintain comprehensive system and service documentation**, including integrations and dependencies, to ensure a clear understanding of the system architecture and facilitate effective monitoring and incident response.
- **Implement dual authorization** for the sanitization of media, the backup and auditing of records outside retention schedules and the execution of high-privileged operations to ensure accountability and prevent unauthorized deletions and changes. Dual authorization adds a layer of accountability, ensuring that high-risk actions are verified by multiple individuals.
- **Embed data or capabilities in systems or system components** to determine if the University's data has been exfiltrated or improperly removed from the organization. Embedding tracking capabilities helps detect and respond to data exfiltration attempts.

Incident response and business continuity

- **Develop and maintain an incident response plan** that includes procedures for handling insider threats. An incident response plan ensures that the organization is prepared to respond quickly and effectively to insider threats.
    - Use the institutional Incident Response Plan to guide the creation of your unit's plan.
    - Utilize the institutional insider threat playbooks to build and customize procedures for your unit.
- **Conduct regular incident response tabletop exercises** to ensure preparedness and improve response capabilities. Regular exercises help identify gaps in the incident response plan and improve the institution's ability to respond to insider threats.
- **Ensure critical service business continuity plans (BCP)** are in place for both natural and cyber incidents to maintain operations during disruptions. Business continuity plans ensure that critical services can continue operating during and after an insider threat incident.

Roles and responsibilities

Executive Management	• Provide oversight and ensure the allocation of resources for insider threat mitigation. • Approve policies related to insider threat management.
Chief Information Security Officer (CISO)	• Approve standards, guidelines and procedures related to insider threat management.
Insider Threat Program Manager	• Develops, implements and oversees the insider threat program. • Coordinates with various units to ensure comprehensive coverage and effectiveness of the program. • Regularly reviews and updates insider threat mitigation strategies.
Legal Counsel	• Provides legal guidance on insider threat policies and procedures. • Ensures that the insider threat program complies with relevant laws and regulations. • Assists in handling legal aspects of insider threat incidents.
Training and Awareness Coordinator	• Develops and delivers training programs focused on insider threat awareness. • Ensures that all employees are educated on recognizing and reporting insider threats. • Continuously updates training materials to reflect the latest threat trends and mitigation strategies.
Service Owner	• Is accountable for the overall delivery and management of specific applications/services, ensuring they meet the needs of the institution and align with security policies. • Ensures application/service continuity and security plans are developed and maintained.
IT Security Manager	• Implements and manages technical controls for access, monitoring and incident response.

	• Conducts regular audits to ensure compliance with security policies and standards, and identifies areas for improvement.
IT System Administrator	• Manages and monitors the day-to-day operations of IT systems, ensuring they are secure, available and performing optimally. • Maintains an accurate inventory of systems, applications, components and their dependencies.
Risk Manager	• Identifies, assesses and manages risks to the institution's information assets, ensuring that appropriate mitigation strategies are in place.
Human Resources	• Conduct background checks and manage employee onboarding and offboarding processes. • Provide and mandate security training and awareness programs.
Physical Security Manager	• Oversees physical security measures to protect against insider threats. • Ensures that physical access controls are in place and effective. • Coordinates with IT security to integrate physical and digital security measures.
Data Protection Officer (DPO)	• Ensures that data protection policies are in place and adhered to. • Monitors compliance with data protection regulations. • Manages data breach incidents and coordinates with relevant authorities.
Incident Response (CSIRT)	• Monitor systems and gather threat intelligence. • Coordinate response efforts and analyze digital evidence. • Implement containment measures and restore operations. • Manage public communication and handle legal issues. • Conduct reviews and provide recommendation for further remediations and training.
End Users (General Community)	• These are the main users of institutional services, responsible for knowing and following institutional policies, standards, codes of conduct, access agreements and legal requirements. • Participate in security training and awareness programs. • Report any suspicious activities or security incidents.

Glossary

- **Insider threat:** A threat posed by individuals within an organization who have access to sensitive information and may misuse it.
- **Access control (AC):** Mechanisms that restrict access to information based on user roles and permissions.
- **Audit and accountability (AU):** Processes for logging and monitoring user activities to ensure accountability.
- **Incident response (IR):** Procedures for detecting, responding to and recovering from security incidents.
- **Personnel security (PS):** Measures to ensure the trustworthiness of individuals with access to sensitive information.
- **Privileged identity and access management (PIAM)**: A framework that focuses on managing and securing privileged accounts and access within an institution. It ensures that only authorized individuals have elevated access to critical systems and data,

reducing the risk of insider threats and unauthorized access. The framework includes, but is not limited to:

- **Shared account management**: Ensuring that shared recovery credentials are managed with traceability to the individual performing the action. This involves implementing mechanisms to track and audit activities performed by each user, even when using shared recovery credentials.
- **Automatic password rotation**: Managing automatic password rotation to enhance security. This involves regularly changing passwords for privileged accounts to prevent unauthorized access and reducing the risk of compromised credentials.
- **Rogue privileged account detection and takeover**: Implementing systems to detect and take over rogue privileged accounts. This involves monitoring for unauthorized access and suspicious activities, and swiftly taking control of compromised accounts to prevent further misuse.

Review period

This document will be reviewed and updated as the threat landscape changes.

Revision history

Version ID	Date of Change	Author(s)	Rationale	Reviewed by	Approved by
1.0	2025-03-21	Joe Bate	Interim guidelines release	Deyves Fonseca	

References

Institutional requirements

Policies

- Policy on Information Security and the Protection of Digital Assets
- Policy on Information Technology
- Appropriate use of information and communication technology
- Freedom of Information & Protection of Privacy (FIPP) Office policies and procedures

Standards

- Digital Asset Classification Standard
- Data Classification Standard
- Information Security Incident Response Plan
- Information Security Control Standard

Further reading

Institutional resources

- Set up your 1Password account (Students)
- Set up your 1Password account (Faculty, Libraries and Staff)

Government of Canada resources

- Canadian Program for Cyber Security Certification (CPCSC)
  - ITSP.10.171 (coming)
  - ITSP.10.172 (coming)
- Enhancing Canada's Critical Infrastructure Resilience to Insider Risk
- How to protect your organization from insider threats (ITSAP.10.003)
- Insider Risk Assessment Tool (IRAT)
- Levels of security clearance

Other resources

- Protecting Controlled Unclassified Information in Non-federal Systems and Organizations (NIST SP 171 Rev. 3)
- Enhanced Security Requirements for Protecting Controlled Unclassified Information (NIST SP 172 Rev. 3, Draft)
- National Institute of Standards and Technology's Cybersecurity Framework (CSF)
- Securities Industry and Financial Markets Association (SIFMA) Insider Threat Best Practices Guide
- National Insider Threat Policy and Minimum Standards