WaterISAC Physical Security Advisory Committee

INSIDER THREAT MANAGEMENT FACT SHEET

Insider threats are an enduring risk to the water and wastewater sector. Given that, an insider threat management program is essential for water and wastewater utilities aiming to strengthen their security and operational resilience. Unlike external risks, insider threats originate from individuals with legitimate access—such as employees, contractors, or trusted third parties—who may intentionally or inadvertently compromise sensitive systems or processes.

Implementing a formal insider threat management program helps utilities establish clear policies, monitor user behavior, and respond swiftly to suspicious activity. These efforts not only protect vital systems from misuse but also promote a culture of accountability and awareness across a utility. With water and wastewater utilities facing increasing physical and cybersecurity threats, insider threat management is a foundational step for safeguarding a utility's operational capabilities across the all-hazards threat landscape.

To help water and wastewater utilities with enhancing their insider threat management policies, WaterISAC's Physical Security Advisory Committee formulated the following best practices.

Best Practices for Insider Threat Management:

1. Program Culture & Governance

Focuses on strategic alignment, leadership, and organizational values.

- ☑ **Provide training and awareness**
  Educate staff on insider threat risks, reporting mechanisms, and the importance of security culture.
- ☑ **Include Insider Threat in Enterprise Risk Management (ERM)**
  Treat insider threats as a strategic risk category and integrate them into broader risk governance and corporate reporting.
- ☑ **Engage leadership and foster a security culture**
  Build a culture of transparency and accountability, where employees feel valued and less likely to become disgruntled towards the utility.
- ☑ **Establish an insider threat program**
  Create a formal, cross-functional program with defined roles, responsibilities, and procedures.

2. Access & Privilege Management

Covers how to control and minimize exposure to sensitive data and systems.

- ☑ **Control and Track Physical Keys and Locks**
  Implement strict procedures for issuing, tracking, and recovering physical keys. Maintain a key log, restrict master key access, and rekey locks when keys are lost or unaccounted for.
- ☑ **Adopt the principle of least privilege**
  Grant users only the minimum access necessary to perform their duties—both physical and digital.
- ☑ **Regularly review and revoke unnecessary access**
  Ensure access rights are promptly removed when employees change roles or leave the organization.
- ☑ **Conduct exit interviews and offboarding checks**
  Assess potential risks and ensure return of all access credentials and sensitive materials.

>>>

3. Detection & Monitoring

Addresses proactive identification of suspicious or harmful behavior.

- ☑ **Enable Real-Time Alerting and Response**
  Set up automated alerts for high-risk activities—such as access to sensitive files outside of business hours, large downloads, or use of unauthorized devices.
- ☑ **Implement continuous monitoring**
  Monitor user behavior, system activity, and access patterns for signs of misuse or anomalies.
- ☑ **Monitor for behavioral indicators**
  Watch for warning signs such as disgruntlement, policy violations, or attempts to bypass controls.
- ☑ **Use data loss prevention (DLP) tools**
  Deploy technology that detects and blocks unauthorized data transfers or exfiltration attempts.
- ☑ **Conduct Random or Targeted Spot Audits**
  Periodically audit access records, user behavior, and file integrity to uncover patterns that may not trigger automated alerts.
- ☑ **Monitor Third-Party and Contractor Activity**
  Extend monitoring to vendors and contractors, especially those with network or facility access, to detect unusual or policy-violating behavior.

4. Risk Assessment & Prevention

Focuses on understanding and reducing vulnerabilities.

- ☑ **Conduct regular risk assessments**
  Evaluate insider threat risks across departments and systems, adjusting controls accordingly.
- ☑ **Perform background checks and vetting**
  Conduct thorough pre-employment screening and periodic re-screening of employees and contractors.

5. Integrated Response & Reporting

Prepares the organization to handle insider threats when they occur.

- ☑ **Develop and test incident response plans**
  Prepare for insider incidents with predefined response protocols and coordination across departments.
- ☑ **Enable anonymous reporting mechanisms**
  Provide a safe, confidential way for employees to report suspicious behavior.
- ☑ **Integrate physical and cyber security efforts**
  Share insights and alerts between departments to form a unified security response.

These practices help create a strong, proactive defense against insider threats by blending technical controls with organizational culture and policy. Utilities should also understand their unique local and state regulations regarding employee hiring and termination policies. (For more information access this American Water Works Association report, "Protecting the Water Sector's Critical Infrastructure Information: Analysis of State Laws").

Ultimately, a robust insider threat management program can significantly strengthen a utility's overall security footprint and reduce their risk of operational disruptions.

Insider Threat Mitigation Resources:

- CISA - Insider Threat Mitigation Guide
- CISA - Insider Threat Reporting Templates
- CISA - Resources for Onboarding and Employment Screening Fact Sheet
- Insider Risk Mitigation Program Evaluation (IRMPE)
- HR's Role in Preventing Insider Threats Fact Sheet

For additional information on Insider Threats and mitigating security risks, watch this previous WaterISAC webinar on the topic here.