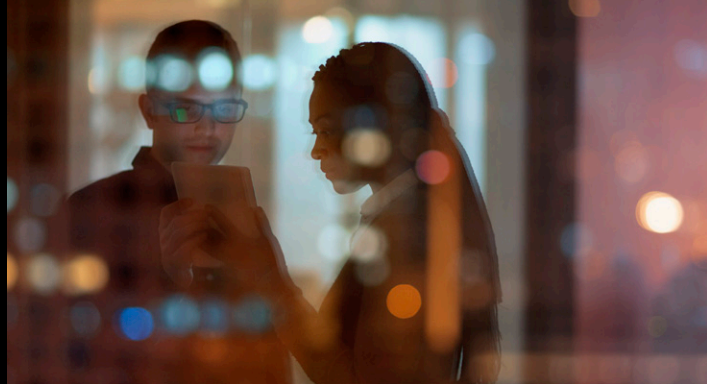
exterro®

INSIDER THREAT PROGRAM CHECKLIST



INSIDER THREAT DEFENSE GROUP

Creating an insider threat program from scratch can be overwhelming. A checklist is a great place to start to ensure you don't bite off more than you can chew.

Below are essential elements of an insider threat program that you should consider:

Insider Threat Program (ITP)

- ○ Do you have management and legal support for ITP?
- ○ What is the scope of the clearance for ITP?
- ○ Do you have funding? How much?
- ○ CEO to roll out the program via a company-wide message.
- ○ Have you appointed an ITP manager?
- ○ Will you establish an ITP working group?
- ○ Collect signed NDA's from everyone in the working group.
- ○ Create an ITP Program Operations Plan.
- ○ Create an ITP Threat Program Policy (high-level).

Data Sources to Support an ITP

- ○ Do you have internal and external data sources to support ITP?
- ○ Establish information sharing agreements between the ITP and the ITP working group members that includes record handling and use procedures.
- ○ Create the processes and procedures to collect, integrate and analyze various data sources for potential or actual insider threats.
- ○ Marking ITP information (privacy / PII marking, ITP official use only).

Insider Threat Detection

- ○ Computer use activity monitoring (desktop, laptop, smartphones, tablets).
- ○ Computer login banners.
- ○ Signed information systems security acknowledgment agreements.
- ○ Physical searches of boxes and briefcases at facility entrance/exit.

Insider Threat Awareness Training

- ○ Guidelines on what employees should report.
- ○ How will you communicate the ITP (training, emails, etc.)?
- ○ How will you document the completion of the ITP awareness training (certificates, sign-in sheets, spreadsheets)?
- ○ How will supervisors be educated on what to report? Suggestion: DSS Roles And Responsibilities For Personnel Security—A Guide For Supervisors.

Insider Threat Report/Investigations

- ○ How will reporting be handled (tip line, drop box, email, etc)?
- ○ Have procedures been established for insider threat incident reporting, response and investigations?
- ○ Will an internal investigation be conducted?
- ○ Who should be notified within and outside of the company?
- ○ How will ITP information be documented (case management, hard copy)?
- ○ How long will ITP information be retained?

INSIDER THREAT PROGRAM CHECKLIST

Insider Threat Risk Mitigation/Assessments

- ○ Has your organization conducted a data inventory?
- ○ Has your organization conducted an Insider Threat Risk Assessment to identify gaps in security controls and business processes?
- ○ Has the organization conducted an Insider Threat Data Exfiltration Assessment? (How easy can a malicious insider exfiltrate data)?
- ○ Will contracts include Insider Threat Risk Mitigation language?
- ○ Will Insider Threat Risk Assessments be conducted on trusted business partners and sub-contractors?
- ○ Does the organization have an Electronic Device (ED) Policy?
- ○ Has the organization conducted a Technical Surveillance Countermeasures Inspection for covert / hidden electronic devices?
- ○ Has the organization considered implementing a Security Vulnerability Rewards Program?

INSIDER THREAT DEFENSE GROUP

This checklist was created in partnership with the Insider Threat Defense Group (ITDG), a trusted source for insider threat mitigation (ITM) training and consulting services to over 640 organizations, including U.S. Government agencies, Fortune 100 and 500 companies and many other retail and financial services organizations, airlines, universities and more.