How to Mitigate Insider Risk Throughout the Employee Lifecycle

As a corporate security professional, you know your company's own employees can be your greatest risk — that applies to partners and contractors, too. Anyone with access to facilities, systems, and information can use that access to intentionally or unintentionally harm your organization.

Thankfully, there are several steps you can take throughout the entire employee lifecycle — from onboarding to offboarding — to mitigate this risk and keep your organization safe.

Use this checklist throughout the lifecycle of anyone employed or contracted with your organization to protect your people, assets, and reputation from insider risk.

Benchmarking your insider risk program

Before diving into the checklist, ask yourself these strategic questions to assess the effectiveness of your insider risk program.

Is your insider risk program tailored to your organization's needs? Every organization is different and requires unique policies and processes	☐
Do you have technology in place to surface alerts in real time? The longer an insider incident goes undetected, the greater the damage to the company	☐
Does your team work closely with cyber, HR, and legal? Integrated cross-departmental processes serve as an important foundation to mitigate insider risk	☐
Do your efforts to monitor for insider risks comply with federal and state regulations? Knowing the laws of your state and municipality will put you in a more confident (and legally compliant) position to assess risk	☐

If you answered no to any of the above questions, you may have some work to do before diving into the following checklist. Watch this on-demand webinar for insights on setting up your insider risk program for success.

Continued on next page

Pre-employment or partnership screening

Complete the necessary due diligence before extending an offer to a new employee or partner.

Criminal records check Check for reports of past violence in the last seven years	☐
Public records search Review undisclosed listings on government watchlists, national sex offender registries, motor vehicle records, civil records, and credit history	☐
Reference checks Verify the candidate's education, past employment, co-worker conflicts, and title discrepancies	☐
Interview process observations Discuss any red flags with HR, being mindful not to violate relevant privacy laws	☐
Social media activity Monitor for behaviors or patterns that may indicate risks or value misalignments, following legal and HR privacy guidelines — with deeper scrutiny for more sensitive roles	☐

If you're in a state with a "Ban the Box" law, which requires employers to eliminate the question on a job application that asks about an applicant's criminal history, your organization might not be aware of a candidate's criminal history

Post-contract considerations

Proactively mitigate insider risk during onboarding and throughout employment.

Require insider risk training All new employees or partners should complete formal insider risk training during onboarding, with refresher sessions annually, after significant policy changes, or when relevant use case learning opportunities arise	☐
Promote a risk-aware culture Ensure that employees and managers understand their critical role in recognizing and reporting indicators of risk like deceptive time logs, expense reports, conflicts, vocalized stressors, or negative online behavior	☐
Enable anonymous reporting Promote a supportive reporting culture that protects employees' privacy, including easily accessible feedback channels to share information with leadership	☐
Review systems regularly Including visitor management, access control, HR portals, and video systems to detect unusual patterns and uncover additional information related to a threat signal	☐

TIP:
These indicators may differ by department or context, so remain adaptive to the changing risk environment

Continued on next page

Post-employment or partnership termination

Anticipate incidents that may occur, whether intentional or unintentional, during offboarding and afterward.

Conduct a threat assessment where appropriate Security teams with strong insider risk programs consult a cross-functional Insider Risk Council, typically including HR, cybersecurity, and legal, to determine if a threat assessment is necessary	☐
Disconnect network access Coordinate with IT to ensure systems access is disconnected simultaneously with the employee's notification of termination	☐
Practice secure offboarding For departing employees who pose no risk, remind them of their responsibilities for secure offboarding, including promptly returning equipment and refraining from downloading sensitive information	☐
Continuously monitor Evaluate the resources available for ongoing observation for signals and threats that may indicate a potential risk	☐
Embrace technology Leverage a platform that effectively collects, stores, and manages data throughout the risk lifecycle, with attention to key dates such as termination anniversaries	☐