



This Rules/Policy document is provided to you and your organization as a starting point or maturity checkpoint for existing rules/policies. It is brought to you on behalf of Jim McConnell, Principal Owner, and Ask McConnell, LLC – A Converged Security Services Provider. The content is not meant to cover every circumstance, industry, law, regulation, contractual requirement, threat, environment, or risk, but it provides an easy, defensible, highly accountable starting point for any organization. Please consult with your legal counsel and insurance provider about added requirements. If you know of peers that you think would find value in these resources, please have them contact us. These will be updated on our website regularly. We are not legally protecting these documents; we just ask for credit, shout-outs, and referrals if you find them helpful. If you have recommended updates, we are all ears. And if you need Converged Security Consulting and Training, please reach out, we would be honored to serve you and your organization.

Jim McConnell

[info@askmcconnell.com](mailto:info@askmcconnell.com)

Ask McConnell, LLC

<https://askmcconnell.com>

# Insider Threat Management

Updated: 29 April 2025

Protecting human lives is the highest requirement of our entire organization, whether they are employees, customers, volunteers, visitors, or part of our supply chain while under some nexus to our organization. Many times things we do online will impact people lives, physically, financially, and emotionally.

Definition: Insider Threat – The threat of security violations by employees and select suppliers.

## Rules

- I will report insider threat and security incidents, concerns, vulnerabilities, and threats to my supervisor or organization's Ethics Hotline as soon as possible and safe, but if they are not available and I feel unsafe, I will contact law enforcement.
- I will not commit or support insider threats or other unethical violations
- I will manage and reduce all aspects of insider threat in all operations I support.
- I will engage insider threat experts, including but not limited to Certified Fraud Examiners in all parts of my operation where I don't have the insider threat management expertise on my team.
- I will manage and support the evaluation of insider risks across all systems, processes, roles, customers, and suppliers that are under my management control.
- I will implement a full insider threat prevention and detection training program, including needs assessment, initial training, sustainment training, and tabletop exercises for all systems, roles, customers, suppliers, and employees under my management
- I will implement and manage insider threat incident reporting for the areas of the organization that I managed and/or fully support any centralized reporting program if it exists.
- I will implement, manage, and use insider threat data analytics (e.g. AP, Travel, VPN, DLP, PCard, Fleet, call center data access, physical access controls, etc.) on all processes and systems that are under my management control, that involve an insider threat risk
- I will implement, manage, and sustain strong yearly background checks on all personnel under my management control who are involved in financial transactions, and due diligence on suppliers who are involved in financial transactions.
- I will perform or support insider threat audits, table top exercises or include insider threat elements in other audits of internal processes and supplier-managed environments under my management control.
- I will develop, maintain, and report strong, ever-maturing metrics on a variety of insider threat prevention, detection, and response activities under my management, on a minimum quarterly basis to leadership
- I will manage and support job rotation and mandatory vacation for all personnel, under my management, who are in high-risk insider threat roles, including myself.
- I will manage, cooperate, and support insider threat investigations that impact my operations, except where I don't have the expertise, for which I will engage appropriate internal or third parties with the expertise.
- I will support insider threat inclusion into the organization's State of Security reporting to leadership.

[Your Logo]	File Name: AskMcConnell_OnePager_Insider_Threat_Management.docx Printed: 04/29/2025 Last Saved: 04/29/2025	[Classification]
-------------	--	------------------

Signature Note: I am a huge fan of wet signatures on these types of documents for accountability and investigation reasons. So you can add the parts below to each rule/policy document or have a collective wet signature and references in the Security Agreement document, located on the same webpage you got this rule / policy from. Organizational preference.

---

\_\_\_\_\_  
Print Full Legal Name

\_\_\_\_\_  
(Blue Ink) full Legal Name Signature  
Style of signature must closely match Driver's License

\_\_\_\_\_  
Date

---