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, defendable, 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
Ask McConnell, LLC
https://askmcconnell.com

Vulnerability Management

Updated: 8 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's lives, physically, financially, and emotionally.

For scoping, not covering human vulnerabilities, primarily physical, cyber, and fraud vulnerabilities

Rules

- I will report 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 act, produce or introduce any activity that would create a vulnerability in our facilities or technology environment
- If a vulnerability is known, introduced, or discovered in an environment that I manage, I will eliminate the vulnerability as soon as safely able to, in coordination with our security or safety teams.
- I will track all physical and technology assets under my management control that are susceptible to being vulnerable, especially assets that are End of Life and End of Service.
- I will subscribe to and monitor all asset manufacturers' security notification processes/websites for new vulnerability information and fixes so I can integrate the mitigations into my overall mitigation implementation schedule.
- I will support testing, scanning, and assessing all assets under my management control, for vulnerabilities on a schedule based on the impact of the asset being breached but no less than once per quarter
- I will NOT test, scan, or assess assets not under my management control unless this type of vulnerability management is under my control across the enterprise
- I will report any vulnerability discovered to the appropriate asset owner as soon as safely possible including vulnerabilities discovered that are owned by customers or suppliers.
- I will support and respond to Ethics Hotlines, Bug Bounty programs and other types of reporting mechanisms for reporting vulnerabilities.
- I will budget (yearly) for the replacement of End of Life, and End of Service assets along with budgeting for the replacement of assets that are vulnerable and can not be mitigated.
- I will implement metrics to manage the security and safety aspects of vulnerability management of environments under my management control
- I will manage or support a State of Vulnerability Management Security Report and Presentation, under Executive Session, at least yearly, that covers incidents, vulnerabilities, improvements, and metrics across all domains of Security.

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
