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

Secure Software Development

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.

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 do any software development, or script writing without following these rules
- I will engage security teams before any internal or outsourced software development projects or enhancements begin.
- I will manage any development schedule, I manage, to make sure security verification and validation along with code reviews are completed before moving through the software life cycle and into production.
- I will always include security requirements in any new and enhancement software development I perform or manage
- I will always conform, with independent verification, to secure coding standards (e.g. CERT, OWASP, STIGs, etc.)
- I will always perform static, dynamic, and code security reviews/testing on all software development activities under my management.
- I will always develop software that supports strong secure configurations by default and strong access control that allows for strict principle of least privilege.
- I will always update all software, drivers, and libraries during each new development, enhancement, and maintenance activity for software under my management control.
- I will attend, deliver, and make sure my team has proper secure software development training throughout each year.
- I will subscribe to and monitor all software 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 make sure all outsourcing, whether software development or services involving technology, will include secure software development requirements in the contract.
- I will implement metrics to manage the security and safety aspects of software development of environments under my management control
- I will manage or support a State of Software Development 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
