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

Technology Software Updates

Updated: 20 March 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, emotionally. Our organization has a significant amount of operation that operates or depends on electronic / online, whether its technology in our facilities or on the public internet and we must protect the access we have been entrusted with

Key Definition:

Technology = all the stuff with wires with the priority set to technology that is connected (wired or wireless) to a network. (Projectors, Laptops, Refrigerator, IoT, Drones, Cameras, Watches, Scanners, Bar Code Scanners, Mobile Phones, yes ALL)

Software = This would include firmware or software installed on the technology. This must not be limited to software listed in visible menus like Start Menu, Launchpad, etc.

- I will report technology software security concerns, vulnerabilities, and threats to my supervisor or the organization's Ethics Hotline
- I will not install any software that isn't licensed and authorized for use by our organization
- I will not install any updates to software that our organization is no longer licensed to get these updates. Just because it is installed, doesn't mean it is still licensed to get updates
- I will report to my supervisor any software that isn't updated to most secure version
- I will not upgrade any software without plans for backups
- I will not upgrade any software without plans to configure its security attributes before use
- I will upgrade software as soon as operationally feasible on all technology under my operational responsibility
- I will not use technology that has end of life or end of service hardware or software unless it is a life or death emergency
- I will budget, yearly, software upgrades to maintain the latest secure software for all technology under my operational responsibility
- I will not install software or upgrades without appropriate personnel involved to determine if there would be a operational impact from the software, upgrades, or timing.

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
