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

Minimum Cyber Security

Based on CISecurity.org's CIS Critical Security Controls v8.1

Updated: 3 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.

Key Definition: "Manage or support" – This means operating the program or supporting others in the organization operating the program. Funding the program yearly for people, process, technology and third-party support.

General Rule

- I commit that my management and support of these rules will use the Center for Internet Security (CIS)'s controls, as a baseline, unless there is a strong set of standard controls required elsewhere in my organization.

Rules

- I will report security concerns, vulnerabilities, and threats to my supervisor or the organization's Ethics Hotline as soon as discovered, if they are not available, and I feel unsafe, I will contact law enforcement.
- I will manage or support proactive, through manual and automated methods, discovery tools and logs, inventory all risk-impacting hardware assets under my management and include classification, criticality, security management ownership information. Ref: CIS – SG 1.x
- I will manage or support proactive, through manual and automated methods, discovery tools and logs, inventory all risk-impacting software assets under my management and include classification, criticality, security management ownership information and compare to the organization's "Allow List". Ref: CIS – SG 2.x
- I will manage or support proactive, through manual and automated methods, discovery tools and logs, inventory all risk-impacting information/data assets under my management and will classify them, maintain zero trust access controls, encrypt the data, maintain access logs, backup and retention processes, and dispose of these assets as required by Legal. Ref: CIS – SG 3.x
- I will manage or support proactive, through manual and automated methods setup and maintain secure configurations of all software (operating system, applications, cloud, databases, middleware, scripts, network devices, etc.) under my management. Ref: CIS – SG 4.x
- I will manage or support proactive, through manual and automated methods setup and maintain access accounts used for all hardware, software, information, and data assets under my management, including provisioning, minimizing access, monitoring, and removing access as the needs of the organization and role changes. Ref: CIS – SG 5.x

- I will manage or support proactive, through manual and automated methods setup and maintain access controls (single factor and multifactor) used for all hardware, software, information, and data assets under my management, including provisioning, minimizing access, monitoring, and removing access as the needs of the organization and role changes. Ref: CIS – SG 6.x
- I will manage or support proactive, through manual and automated methods, to discover, detect, and remediate all vulnerabilities for all hardware, software, information, and data assets under my management. Ref: CIS – SG 7.x
- I will manage or support the enablement, monitoring, appropriate length of storage of logs across all hardware, software, information, and data assets under my management, including making sure all logs have time and content integrity controls. Ref: CIS – SG 8.x
- I will manage or support the enablement, monitoring, and ongoing management of internet access controls via inbound and outboard email and web browsing/browsers, including filtering, logging, whitelisting, and access control for all internet access under my management (Ref: CIS – SG 9.x)
- I will manage or support the installation, configuration, monitoring, and updates to anti-virus/anti-malware/anti-breach software for all devices under my management that support this type of software. (Ref: CIS – SG 10.x)
- I will manage or support the backup of critical hardware, software, data and information regardless of its form or location and regular verify these backups are geographically distributed and test restored, on a quarterly basis. (Ref: CIS – SG 11.x)
- I will manage or support the implementation, secure configuration, monitoring, manage, maintain, and upgrade network devices that impact the security of the areas of the organization that are under my management. (Ref: CIS – SG 12.x)
- I will manage or support the implementation of a 24x7 logging and network monitoring capability with a primary focus on internally and externally originating security events. (Ref: CIS – SG 13.x)
- I will manage and support a security awareness and security training pathway for all personnel under my management to include a baseline for all personnel then specialized training for each unique role. (Ref: CIS – SG 14.x)
- I will manage and support the use of any third-party service provider under my management that impacts the risk of any asset of our organization; this includes due diligence, background checks, references, RFP/RFI/RFQ, appropriate contracts and documented operational requirements, metrics, security verification and validation, formal security audits, testing and training and incident response. (Ref: CIS – SG 15.x)
- I will manage and support security controls for requirements, coding, pre-production, protection, and enhancements of internal and third-party application/software development, including security requirements, secure coding requirements, security testing, secure configuration management, license management, and OSS controls. (Ref: CIS – SG 16.x)
- I will manage and support the development, training, testing and implementation of security incident response capabilities for all environments under my control or support environments outside my control based on the governance of NIMS Incident Command System (ICS). ((Ref: CIS – SG 17.x)
- I will manage and support regular security penetration testing across all OSI layers (including Layer 8, aka People) for all environments under my control using existing resources AND third-party, independent resources. (Ref: CIS – SG 18.x)

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
