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

Supply Chain Contracts

Updated: 22 July 2025

This policy is a set of rules focused toward a supplier/vendor/third party ("supplier") that can have an impact, small or large, on the organization's brand, security, confidentiality, integrity, data, information, availability, personnel, facilities, etc. This document will be slightly different to make it simple, one document with a few "One Pagers". The rules for the major areas of security will be their individual One Pagers that all should be considered for supplier contracts.

The "I" in "I will…" would be the person signing the contract for the supplier, of which, they should provide a designated security professional in their organization who actually "will" be accountable for the implementation and ongoing compliance with these rules.

Rules (General Security Governance / Security Management)

- I will ensure all security requirements of this contract are implemented within _____ days of execution
- 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 identify the Chief Security Officer (CSO) and Chief Information Security Officer (CISO) and supply their full 24x7 contact information to the customer/client's CSO/CISO and Supplier Management Organization, within 5 days after signing.
- I will ensure our organization maintains a strong incident response program covering all types of security, safety, and fraud incidents that includes notification of CSO and CISO of Customer/Client within 24 hours (calendar hours) of awareness of incident impacting Customer/Client.
- I will maintain a current inventory of all assets (people, processes, technology, buildings, suppliers, etc.) that are used to support this contract, in particular assets that access, store, or process the customer/client's assets (information, buildings, people).
- I will ensure that all parts of our organization's assets that will service the customer/client will be subject to independent accreditation through a minimum of ISO 27001:2022
- I will ensure any identified flow-down requirements from the customer/client are implemented within ___days of execution of the agreement. I will also ensure all security requirements of this agreement are flowed down to any suppliers being used to service this agreement.
- I will ensure all assets being used to support this contract will come under a documented, tested, and exercised business continuity and disaster recovery program
- I will ensure all personnel (employees and non-employees) being used to support this contract will have initial documented training based on the contract requirements and recurring sustainment training, at least once per year or any significant changes to the contract or SOW.
- I will ensure, we can provide attestation and evidence of compliance to all security elements of this agreement within 5 days of former request for attestation
- I will ensure industry-leading metrics and stats are collected, verified, and used for the security and compliance of all security elements of this contract
- I will ensure a 24x7 insider threat program is in place to prevent, detect, and respond to any insider threats that could impact the delivery of the services of this contract or the customer/client.
- I will ensure a 24x7 capability for monitoring of information security, cyber security, personnel security, physical security, and fraud, threats, and attacks against all assets supporting this contract

Rules (Personnel Security)

- I will ensure all customer/client personnel going onsite to supplier location or events will be provided personnel security commiserate with the level of security and threat in/around the environment on that particular day. If I can not ensure this level of security, I will communicate with the customer/client CSO as soon as feasible.
- I will ensure I notify the CSO of the customer/client when any of my organization's personnel are going to be onsite or at events of the customer/client to make sure personnel security measures are shared and verified.
- I will ensure any of my organization's personnel who will be onsite at customer/client location or event are fully briefed on their/our responsibility for their security and procedures, if there are any special rules, concerns, or incidents.

Rules (Information Security / Cyber Security)

- I will ensure all accounts used on assets servicing this contract will have multi-factor authentication implemented and monitored. This includes accounts at the operating system, database, application, and other layers of assets.
- I will ensure all software on all assets servicing this contract will have no end-of-life/end-of-service software. If EOL/EOS is required, this will be documented to the customer/client with a remediation date.
- I will ensure all access to assets servicing this contract will be implemented with the strict principle of least privilege access
- I will ensure all physical assets (computers, servers, paper files, etc.) will be physically secure
- I will ensure all technology used to service this contract will have implemented and verified (random restores) Backups based on the 3-2-1 standard.
- I will ensure all functional/generic login accounts will have secondary authorization implemented to support individual accountability
- I will ensure network segmentation is implemented to only allow assets servicing this contract to communicate with assets only servicing this contract
- I will ensure that an all-layer vulnerability management system (reporting, scanning, evaluation, threat intel, patch/configuration management is implemented across all assets servicing this contract
- I will ensure that if there is any software development that supports the servicing of this contract that it will use strong SDLC standards (e.g., Secure Coding practices from CMU)
- I will ensure all information/data is retained and disposed of based on the customer/client's legal requirements
- I will ensure all technology assets used to service this contract will have strong configuration management controls based on industry secure configuration management standards, along with the strictest hardening settings feasible while still operationally practical.
- I will ensure all assets used to service this contract will have documented and controlled classification levels for confidentiality, integrity, and availability.

Rules (Physical Security)

- I will ensure all physical access to rooms used to store assets servicing this contract will have multi-factor authentication implemented and monitored. This includes IDF, MDF, Data Center, Computer Rooms, Safe Storage, non-public paper storage, etc.
- I will ensure all software on all assets servicing this contract will have no end-of-life/end-of-service software. If EOL/EOS is required, this will be documented to the customer/client with a remediation date.
- I will ensure all access to assets servicing this contract will be implemented with the strict principle of least privilege access, whether by badge or key.
- I will ensure all logging of physical human access to areas used to service this contract is (electronically) logged and IDs verified for entering and exiting areas.
- I will ensure industry-standard coverage by security cameras that record for at least ____ days is in place for all areas used to service this contract.
- I will ensure all facilities used to service this contract, go through a certified CPTED assessment at least once a year and gaps mitigated within ____ days, based on agreement with the customer/client's CSO
- I will ensure physical intrusion detection technology (e.g., cameras, door alarms, anti-passback, window alarms, etc.) is implemented for all areas servicing this contract and is monitored 24x7
- I will ensure panic buttons are available at perimeter lobby(ies) for all locations used to service this contract

Rules (Fraud)

- I will ensure fraud (as defined and scoped by the Association of Certified Fraud Examiners) controls, analytics, monitoring, and investigations are implemented for all potential areas of fraud related to the servicing of this contract, particularly financial elements (e.g. AP, ACH, Billing, Expenses, Travel, PCard, etc.)

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
