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

Original by Ask McConnell, LLC – A Converged Security Service Provider – This statement must not be removed without written approval

Physical Security Policy

Updated: 13 April 2025

Physical Security is about protecting human lives and organizational assets (e.g. employees, buildings, equipment, vehicles, etc.). These policies/rules are meant to be a baseline for personnel to comply with at all times while on organizational time or at organizational locations.

- I will report physical security concerns, vulnerabilities, and threats to my supervisor or the organization's Ethics Hotline immediately upon discovery. If I suspect a crime is involved, I must call 911, if it safe, and then my supervisor
- I will not share or let another individual use my Access Badges unless responding to a life or death emergency
- I will badge into a badge-controlled location, no piggy-backing. Where there is an anti-passback exit badge reader, I will also badge out each time.
- I will check and lock all padlocks (internal and external), that I am responsible for before leaving premises. If I am the last person exiting a organization gate that has a pad lock, I must also lock that pad lock after I leave.
- I will verify that all visitors that I am overseeing, haved signed in and signed out through the paper or electronic sign-in process of each visit to any organizational facility.
- I will not share or let another person borrow any keys assigned to me, unless life or death emergency.
- I will verify that all keys assigned to me are logged in the established Key Management System
- I will not prop open any Perimeter or Key/Badged door, unless for immediate safety reasons and a organizational employee or guard, is monitoring the door
- If I lost or aware of any lost or stolen keys or access badges, I will report this issue immediately to the my supervisor.
- I will not allow human or vehicular tailgating
- I will lock all non-public information, that I control, away in approved secured/locked storage containers (e.g. locking desk drawers, locking file cabinets. I will not rely on just a locked office/building door or security of non-public information
- I will check all buildings' internal environment and perimeter, I am responsible for, for security vulnerabilities or violations before leaving the location at end of my shift. If any issues are discovered, I will report them to my supervisor before leaving the site.
- If I am responsible for security cameras, I will check all cameras via the camera console, at the beginning and end of each shift/day to verify they are all working, not blocked or out of focus. If any issues are discovered, I will report the issue(s) to my supervisor before leaving site.
- I will manage or support the destruction of all paper-based information by cross-cut shredder through the in accordance with law and the organization's Records Retention Policy and Procedures.
- I will verify fleet and other moveable/motorized vehicles or equipment, that I or my team uses or is responsible for, are locked (passenger doors and equipment/storage locks) before end of each shift, even if stored in locked building.
- I will verify all hazmat material, that my team uses or is responsible for, is stored properly and the storage containers are locked before the end of each shift.
- I will verify all perimeter (people, rollup, and other entrances) doors are closed and locked before the end of each shift if I believe I am the last person to leave the facility.
- I will verify all portable equipment stored outside of locked buildings, that I or my team uses or manages, is tongue locked or wheel chuck locked before the end of each shift
- I will make sure all my visitors/suppliers/customers, that need to be escorted, will either be escorted at all times while on the organization's property or monitored by organizational personnel to make sure they remain only in areas they are authorized and only perform the duties they are authorized to perform.
- If I am in charge of facilities/key (cores), I will have key cores replaced when >2 keys are lost or stolen. I will make sure this is done within 3 days of lost/theft.
- If I am in charge of facilities/access control, I will have badge access control disabled within 24 hours of the lose of a badge or termination of personnel with access.
- I will only approve the issuance of a key or badge that is limited to a specific door(s) and only if they are going to need access for a significant amount of time (think weeks/months/years). All access I approve must be reviewed for continued validity every 6 months

Original by Ask McConnell, LLC – A Converged Security Service Provider – This statement must not be removed without written approval

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

Original by Ask McConnell, LLC – A Converged Security Service Provider – This statement must not be removed without written approval