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

Termination / Offboarding Personnel

Updated: 30 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.

Clarification: The use of the term “Termination” is not meant to focus on hostile termination/firing for cause. In this document, it is simply the broad process of removing an employee or supplier’s employee from payroll, contract, etc., whether through hostile firing, normal downsizing, retirement, for-cause, or career change support.

- I will report termination / offboarding security concerns, vulnerabilities, and threats to my supervisor or the organization’s Ethics Hotline
- If I am terminated
    - I will not introduce any security vulnerabilities to organizational assets at any time before notification, after notification or after my termination date
    - I will not transmit any personal information (photos, resume, performance reports, etc.) to external resources (e.g., personal email) without full inventory and disclosure to my supervisor or HR.
    - I will not remove (electronically or physically) organizational assets before or after my termination notification.
    - I will return ALL (electronic or physical) organizational assets to the organization at the time of termination and any additional items I discover after termination, within 3 business days of my termination
    - I will advise my supervisor or HR of ALL my organizational physical or electronic access, internal and external, that needs to be removed
    - I will not access any organizational access, even if still accessible after my termination. (e.g. organization forgot to terminate your access to a cloud application)
    - I will maintain all confidentiality requirements until my death
- If one of my employees/supplier’s employee is terminated
    - I will manage the removal of all the employees’/suppliers’ access within 3 days of termination
    - If someone under my (administrative) management authority leaves the organization, I will make sure they have attested that they have returned all organization assets, I will enage Legal to determine if any Legal Hold requirements. I will then retain ONLY documents, emails, files, paper that are required for the organization to continue to legally function and destroy all other documents, emails, files, paper according the Retention/Destruction Schedule.
- If the termination may involve/involves hostile behavior or threats
    - I will engage with organizational security, contracted security, or law enforcement at least 2 days before notification.
- Other Offboarding Requirements
    - I will limit notification of any termination to strict need-to-know
    - If termination is “for cause”, I will support a review and response to all complaints and after-action reports, including but not, updating rules/policies documents.
- I will manage or support a State of Security Report and Presentation, under Executive Session, at least yearly, that covers incidents, vulnerabilities, improvements, and metrics across all domains of Security, included termination and onboarding elements.

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
