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

Records Retention/Destruction

Updated: 23 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.

Definition (legal definitions may vary by organization)

Non-Public Information – This is ANY organization information, data that it owns, created, licenses, or is under a legal obligation to protect such as employee information, customer information, financial information, Personally Identifiable Information (PII), etc., that has not been approved for Public release. Organizational information only becomes "Public" if approved by Legal, HR, and Corporate Communications teams/authorities.

Records – Operationally, this is any physical or electronic (regardless of where it is stored) data or information that would be considered non-public information that must be protected by law, regulation, customers, governing body, or "just a good idea".

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 follow all Legal provided rules on Attorney-Client Privilege (ACP) communications involving retention and destruction of these unique communications.
- I will follow all Legal provided rules on Legal Hold requirements upon notification.
- I will fully comply with all one-way and mutual records retention and destruction rules with third parties or customers.
- I will keep and delete my organizational emails and their backup(s)/archives, in accordance with the organization's records retention schedule (Sample Below)
- I will manage or support the destruction of all paper-based information by cross-cut shredder based on the organization's records retention/destruction schedule (Sample below)
- I will manage or support the destruction of all electronic media (thumb drives, CD/DVDs, Hard Drives after all the data/information that must be retained is removed.
- I will not access records/email/documents that were controlled by an employee/contractor/volunteer who has left the organization, except under my User ID and only if approved by the person's supervisor or governing leader.
- I will manage, support the verification that all data/information is removed from laptops, desktops, and mobile devices according to these requirements including being wiped to NIST standards before physical disposing or recycling or donating the device.
- If somone under my (administrative) management authority leaves the organization, I will make sure they have attested that they have returned all organization assets, I will advise 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.
- I will manage or support any fire resistant or offsite secure storage services for any long term retention requirements.

Sample Retention Schedule – If an asset fits two or more categories, all choose the longer period.

Record Type	Retention Period	After
Project Information	1 Year	Project Completed
M&A Information	3 Years	M&A Documentation
“Regular” Emails	90 Days	Emails Received
General Information	90 Days	Documents no longer needed by the organization
Legal Information	3 Years	After Legal Action has been finalized
Financial Information	7 Years	After IRS filing have been confirmed as cleared
Security Information	3 Years	After audit log entry or investigation closure.

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
