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

Email Security

Updated: 25 March 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.

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 not access my personal email from organization computers
- I will not forward non-personal info from company email / systems / computers to unauthorized email addresses, including personal email addresses
- I will review all external emails to visually verify (not open) if they are spam, phishing and report them to the organization's email administrator then delete.
- I will not disable any email security, monitoring, malware prevention tools on any organization technology.
- If I am the email administrator, I will make sure the following minimum email security standards are implemented to highest security configuration the organization can support: DMARC, DKIM, SPF, BIMI, RFC 2142, SMTP and Email service logging, along with Spam, Link, and Attachment scanning for malware and data loss prevention.
- I will delete and keep emails and backup of emails, in accordance with the organization's records retention rules
- I will follow all Legal provided rules on Attorney-Client Privilege (ACP) communications through email
- I will encrypt all emails and attachments based on the classification, recipient requirements (e.g. customer contract requirements) or other legal requirements.
- I will use standard email signatures and notices on all organization emails whether from a computer or mobile phone.

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
