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

Non-Public Information Security (Including PII)

Updated: 31 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.

Definition

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.

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 forward non-personal info from company email/systems / computers to unauthorized email addresses, including personal email addresses
- I will not communicate Non-Public information in any form, via any method, without prior approval by Legal, HR, Corporate Communications, or other designated persons with authority.
- I will follow all Legal provided rules on Attorney-Client Privilege (ACP) communications
- I will encrypt all non-public information based on the classification, recipient requirements (e.g. customer contract requirements), or other legal requirements.
- I will not communicate any Non-Public Information in violation of export control or deemed export control laws and regulations
- I will not communicate any Non-Public Information at public venues/events such as restaurants, hotels, or conferences without prior approval and scoping
- I will fully all one-way and Mutual Non-Disclosure Agreements when communicating Non-Public Information
- If I am authorized to communicate Non-Public Information of the organization, I will only communicate the least amount of information necessary, in the most secure form, and only to specific individuals with a strict need-to-know.
- For individuals not under NDA, where I am authorized to communicate Non-Public Information, I will use the FIRST Traffic Light Protocol, defaulting to TLP:Red
- I will not disclose Non-Public Information via phone, email, or other "faceless" methods without approval AND strict authentication of the recipient(s).

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
