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

Security Metrics

Updated: 03 May 2025

Shameless Plug: My book, Converged Security Metrics, provides over 500 metrics that can be considered, when implementing these rules/policies. Also not that some of these rules may DISCOURAGE people from wanting to measure security, so get input from both the provider of the metrics and the audience of the metrics.

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.

- I will report security concerns, vulnerabilities, and threats to my supervisor or the organization's Ethics Hotline, or if they are unavailable, and I feel unsafe, I will call law enforcement.
- I will track, with statistics and metrics, all security functions under my management control.
- I will equally manage statistics-based security reporting AND metrics-based security reporting to senior leadership
- I will measure both transactional/incident/event type of statistics and metrics, but also maturity-based security metrics
- I will not withhold security statistics or security metrics from senior leadership that can have a positive or negative impact on individuals, leadership or the organization
- If I am pressured to withhold any security statistics or security metrics by leadership, I will report the issue to the organization's Ethics Hotline or General Counsel or government whistleblower program.
- I will verify that all data and information that I use to create my security statistics and security metrics is checked for integrity issues before publishing
- I will verify that all data and information that I provide to another group who is building/managing/presenting security metrics
- I will protect any legally sensitive metrics using the principle of least privilege
- All presentations of statistics and metrics will be annotated with a fully transparent scope statement and any known integrity issues.

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
