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

User IDs / Login IDs – Cyber / Information Security

Updated: 20 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, emotionally. Our organization has a significant amount of operation that operates or depends on electronic / online, whether its technology in our facilities or on the public internet and we must protect the access we have been entrusted with

- I will not share my User ID with another party without verified proof the other party is authorized to get that information
- I will not share my password, passcode, pin with anyone (company or human) unless there is a life or death emergency that I have verified.
- I will set a password that meets or exceeds the organization's password quality requirements. If there is no documented requirements I will follow industry guidance like from NIST
- I will report security concerns, vulnerabilities, and threats to my supervisor or the organization's Ethics Hotline that is or might be related to my User ID or Password
- I will not use the same password for all access for the organization, unless the access is controlled by a centralized secure single sign-on technology
- I will not introduce any security vulnerabilities that would jeopardize myself, other personnel, or my organization.
- I will follow the strictest User ID and Password rules for all access if there is a conflict between supplier/vendor, customer, or internal rules.
- I will notify the appropriate party internally when I don't need access to an organization's asset, within 24 hours of not needing it anymore.
- I will notify the appropriate party internally when I have been given access to an organization's asset that I shouldn't have access to, within 24 hours.
- I will not use personal User IDs for business purposes.
- I will use business User IDs for business purposes only
- I will not give anyone or anything access to organization assets without written/signed authorization and verification of need.
- I will not give anyone or anything more access than the absolute minimum they/it needs access to.
- If I manage any technology that supports/requires User IDs, I will implement individual accountability for all access
- If I manage any technology that supports/requires User IDs, I will implement secure logging and monitoring management capabilities (people, process, and technology)
- I will not use any generic/functional user ID that doesn't have secondary authorization capabilities and multi-factor authentication.

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
