Principle 3 - Phase 1 “Products, Functionalities, Technologies” Baseline Requirements

Baseline Requirements	Description
Unique identity	Assets shall be uniquely identifiable.
Secure onboarding	When an asset is being onboarded into an environment the asset shall be able to assert its unique identity.
Secure credentials	Universal default, hardcoded and weak credentials shall not be used.
Login protection	Either the asset or the system will implement account lockout or an authentication back off timer.
Access control	Assets shall include strong authentication mechanisms and have them enabled by default. Authorization shall be used to ensure legitimate use and mediate attempts to access resources in/from a system.
Secure storage	Storage for security–sensitive data shall be secured.
Secure communications	Sensitive data and system information, including management and control process data shall be protected while in transit.
Minimize attack surface	Security features shall be enabled by default and functionalities that are not required or are insecure shall be disabled by default.
Secure data deletion	Manufacturers shall provide functionality for customers to securely wipe customer data.
Backup feature	Relevant assets shall provide a backup feature for data.
Security documentation	Manufacturers shall provide a comprehensive security guide for the asset which details minimal steps and follows security best practices on usability.
Validate input data	All input data shall be validated prior to use by the asset.
Password changed on first use	Relevant assets shall force a password change during the initial setup.
Secure updates	Assets shall have the ability to securely update and remove / mitigate vulnerabilities and bugs, during their lifecycle, in a timely fashion.
Telemetry & event monitoring	Assets shall implement logging for telemetry and security related events.
Maintain settings after outage	Assets shall maintain settings after power outage.
Factory reset	Assets shall provide a means to return to original factory configuration with all customer data securely removed.
No backdoors	No undocumented ways to remotely connect to the asset shall be put in place by the manufacturer.
Conceal password characters	Assets shall mask all passwords during input by default.