P3 Phase 2 “Processes, Operations, Architectures” Baseline Requirements

Suggested Baseline Requirements	Description
Security Management Program	A security management program based on best practices shall be established and implemented to continuously improve the security posture.
Risk Management Process	Security risk shall be managed in the organization for critical assets based on risk assessment.
Human Resources Security	Processes shall be established in Human Resources to support security management prior to and during onboarding, as well as offboarding, of personnel.
Training	A minimum level of security education and training on key security issues shall be regularly deployed for employees.
Asset Management	Policies and procedures shall be in place for the management of assets throughout their lifecycle, including onboarding, changes and offboarding.
Identity and Access Management	Access to assets shall be limited to authorized identities only for the time needed, and managed based on risk and the principle of least privilege.
Credentials Management	Organizations shall have a process of enforcing current security best practices to manage credentials and cryptographic material throughout their entire lifecycle.
Physical Security	Physical security shall be in place to protect assets by providing access control and protecting information.
Security Documentation	Process shall be in place to ensure proper and accessible security documentation, including information about capabilities, risks and mitigation strategies.
Continuous Monitoring	Robust monitoring for critical assets shall be put in place for all relevant events and logged information shall be protected.
Vulnerability Management	A Vulnerability Management Process shall be established for the duration of the support lifecycle of assets, including the collection of vulnerability notifications, proactive monitoring, responding to vulnerabilities and related communication. Security updates shall be implemented to address vulnerabilities in a timely, transparent and secure manner throughout the entire asset lifecycle.
Threat Identification and Mitigation	Procedures and policies shall be in place to monitor, identify and monitor threats to assets.
Segmentation	Physical and logical segmentation shall be in place to minimize security risks and to protect critical assets.
Secure Development Lifecycle	Policies and procedures shall be in place for secure development best practices to ensure the integrity of the developed assets and minimize vulnerabilities.
Security Incident Management	Policies and procedures for the management of security incidents shall be established to mitigate risks and minimize damage should an incident occur.
Business Continuity and Disaster Recovery	Policies and procedures shall be in place to identify, maintain and re-establish necessary business operations in a timely manner, including ensuring of proper restoration of data and services in case of disruption.
Security Auditing	Regular and ad hoc internal and external security audits/assessments shall take place to verify for compliance with company security policies and relevant regulations.

Charter of Trust