Cybersecurity & Data Protection by Design Principles (C|P)

The C|P establishes 33 common-sense principles to guide the development and oversight of a modern cybersecurity & data privacy program. The C|P is sourced from the Secure Controls Framework (SCF), which is a free resource for businesses. The SCF's comprehensive listing of over 1,000 cybersecurity & data protection controls is categorized into 33 domains that are mapped to over 100 statutory, regulatory and contractual frameworks. Those applicable SCF controls can operationalize the C|P principles to help an organization ensure that secure practices are implemented by design and by default. Those 33 C|P principles are listed below:

1. Cybersecurity & Data Protection Governance (GOV)
Execute a documented, risk-based program that supports business objectives while encompassing appropriate cybersecurity & data protection principles that addresses applicable statutory, regulatory and contractual obligations.

2. Artificial Intelligence and Autonomous Technology (AAT)
Ensure trustworthy and resilient Artificial Intelligence (AI) and autonomous technologies to achieve a beneficial impact by informing, advising or simplifying tasks, while minimizing emergent properties or unintended consequences.

3. Asset Management (AST)
Manage all technology assets from purchase through disposition, both physical and virtual, to ensure secured use, regardless of the asset's location.

4. Business Continuity & Disaster Recovery (BCD)
Maintain a resilient capability to sustain business-critical functions while successfully responding to and recovering from incidents through well-documented and exercised processes.

5. Capacity & Performance Planning (CAP)
Govern the current and future capacities and performance of technology assets.

6. Change Management (CHG)
Manage change in a sustainable and ongoing manner that involves active participation from both technology and business stakeholders to ensure that only authorized changes occur.

7. Cloud Security (CLD)
Govern cloud instances as an extension of on-premise technologies with equal or greater security protections than the organization's own internal cybersecurity & data privacy controls.

8. Compliance (CPL)
Oversee the execution of cybersecurity & data privacy controls to ensure appropriate evidence required due care and due diligence exists to meet compliance with applicable statutory, regulatory and contractual obligations.

9. Configuration Management (CFG)
Enforce secure configurations according to vendor-recommended and industry-recognized secure practices that enforce the concepts of "least privilege" and "least functionality" for all systems, applications and services.

10. Continuous Monitoring (MON)
Maintain situational awareness of security-related events through the centralized collection and analysis of event logs from systems, applications and services.

11. Cryptographic Protections (CRY)
Utilize appropriate cryptographic solutions and industry-recognized key management practices to protect the confidentiality and integrity of sensitive/regulated data both at rest and in transit.

12. Data Classification & Handling (DCH)
Enforce a standardized data classification methodology to objectively determine the sensitivity and criticality of all data and technology assets so that proper handling and disposal requirements can be followed.

13. Embedded Technology (EMB)
Provide additional scrutiny to reduce the risks associated with embedded technology, based on the potential damages posed from malicious use of the technology.

14. Endpoint Security (END)
Harden endpoint devices to protect against reasonable threats to those devices and the data those devices store, transmit and process.

15. Human Resources Security (HRS)
Execute sound hiring practices and ongoing personnel management to cultivate a cybersecurity & data privacy-minded workforce.

16. Identification & Authentication (IAC)
Enforce the concept of "least privilege" consistently across all systems, applications and services for individual, group and service accounts through a documented and standardized Identity and Access Management (IAM) capability.

17. Incident Response (IRO)
Maintain a viable incident response capability that trains personnel on how to recognize and report suspicious activities so that trained incident responders can take the appropriate steps to handle incidents, in accordance with a documented Incident Response Plan (IRP).

18. Information Assurance (IAO)
Execute an impartial assessment process to validate the existence and functionality of appropriate cybersecurity & data privacy controls, prior to a system, application or service being used in a production environment.

19. Maintenance (MNT)
Proactively maintain technology assets, according to current vendor recommendations for configurations and updates, including those supported or hosted by third-parties.

20. Mobile Device Management (MDM)
Implement measures to restrict mobile device connectivity with critical infrastructure and sensitive/regulated data that limit the attack surface and potential data exposure from mobile device usage.

21. Network Security (NET)
Architect and implement a secure and resilient defense-in-depth methodology that enforces the concept of "least functionality" through restricting network access to systems, applications and services.

22. Physical & Environmental Security (PES)
Protect physical environments through layers of physical security and environmental controls that work together to protect both physical and digital assets from theft and damage.

23. Data Privacy (PRI)
Align data privacy practices with industry-recognized data privacy principles to implement appropriate administrative, technical and physical controls to protect regulated personal data throughout the lifecycle of systems, applications and services.

24. Project & Resource Management (PRM)
Operationalize a viable strategy to achieve cybersecurity & data privacy objectives that establishes cybersecurity as a key stakeholder within project management practices to ensure the delivery of resilient and secure solutions.

C|P 2025.2

SCF | SECURE CONTROLS FRAMEWORK

25. Risk Management (RSK)
Proactively identify, assess, prioritize and remediate risk through alignment with industry-recognized risk management principles to ensure risk decisions adhere to the organization's risk threshold.

26. Secure Engineering & Architecture (SEA)
Utilize industry-recognized secure engineering and architecture principles to deliver secure and resilient systems, applications and services.

27. Security Operations (OPS)
Execute the delivery of cybersecurity & data privacy operations to provide quality services and secure systems, applications and services that meet the organization's business needs.

28. Security Awareness & Training (SAT)
Foster a cybersecurity & data privacy-minded workforce through ongoing user education about evolving threats, compliance obligations and secure workplace practices.

29. Technology Development & Acquisition (TDA)
Develop and/or acquire systems, applications and services according to a Secure Software Development Framework (SSDF) to reduce the potential impact of undetected or unaddressed vulnerabilities and design flaws.

30. Third-Party Management (TPM)
Execute Supply Chain Risk Management (SCRM) practices so that only trustworthy third-parties are used for products and/or service delivery.

31. Threat Management (THR)
Proactively identify and assess technology-related threats, to both assets and business processes, to determine the applicable risk and necessary corrective action.

32. Vulnerability & Patch Management (VPM)
Leverage industry-recognized Attack Surface Management (ASM) practices to strengthen the security and resilience systems, applications and services against evolving and sophisticated attack vectors.

33. Web Security (WEB)
Ensure the security and resilience of Internet-facing technologies through secure configuration management practices and monitoring for anomalous activity.