Security & Privacy by Design Principles (S|P)

The S|P establishes 32 common-sense principles to guide the development and oversight of a modern security and privacy program. The S|P is sourced from the Secure Controls Framework (SCF), which is a free resource for businesses. The SCF's comprehensive listing of nearly 750 cybersecurity and privacy controls is categorized into 32 domains that are mapped to over 100 statutory, regulatory and contractual frameworks. Those applicable SCF controls can operationalize the S|P principles to help an organization ensure that secure practices are implemented by design and by default. Those 32 S|P principles are listed below:

SCF SECURE CONTROLS FRAMEWORK

version 2019.2

1. Security & Privacy Governance

Govern a documented, risk-based program that encompasses appropriate security and privacy principles to address all applicable statutory, regulatory and contractual obligations.

2. Asset Management

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

3. Business Continuity & Disaster Recovery

Maintain the capability to sustain business-critical functions while successfully responding to and recovering from incidents through a well-documented and exercised process.

4. Capacity & Performance Planning

Govern the current and future capacities and performance of technology assets.

5. Change Management

Govern change in a sustainable and ongoing manner that involves active participation from both technology and business stakeholders to ensure that only authorized changes occur.

6. Cloud Security

Govern cloud instances as an extension of on-premise technologies with equal or greater security protections than the organization's own internal controls.

7. Compliance

Oversee the execution of cybersecurity and privacy controls to create appropriate evidence of due care and due diligence, demonstrating compliance with all applicable statutory, regulatory and contractual obligations.

8. Configuration Management

Govern the establishment and ongoing management of secure configurations for systems, applications and services according to vendor-recommended and industry-recognized secure practices.

9. Continuous Monitoring

Maintain situational awareness of security-related events through the centralized collection and analysis of event logs from systems, applications and services.

10. Cryptographic Protections

Utilize appropriate cryptographic solutions and industry-recognized key management practices to protect the confidentiality and integrity of sensitive data both at rest and in transit.

11. Data Classification & Handling

Publish and enforce a 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.

12. Embedded Technology

Provide additional scrutiny to the risks associated with embedded technology, based on the potential damages posed when used maliciously.

13. Endpoint Security

Harden endpoint devices to protect against reasonable threats to those devices and the data they store, transmit and process.

14. Human Resources Security

Foster a security and privacy-minded workforce through sound hiring practices and ongoing
personnel management.

15. Identification & Authentication

Implement an Identity and Access Management (IAM) capability to ensure the concept of "least privilege" is consistently implemented across all systems, applications and services for individual, group and service accounts.

16. Incident Response

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

17. Assurance

Utilize an impartial assessment process to validate the existence and functionality of appropriate security and privacy controls, prior to a system, application or service being used in a production environment.

18. Maintenance

Utilize secure practices to maintain technology assets, according to current vendor recommendations for configurations and updates, including those supported or hosted by third-parties.

19. Mobile Device Management

Govern mobile devices through a centralized or decentralized model to restrict logical and physical access to the devices, as well as the amount and type of data that can be stored, transmitted or processed.

20. Network Security

Architect a defense-in-depth methodology that enforces the concept of "least functionality" through restricting network access to systems, applications and services.

21. Physical & Environmental Security

Implement layers of physical security and environmental controls that work together to protect both physical and digital assets from theft and damage.

22. Privacy

Implement a privacy program that ensures industry-recognized privacy practices are identified and operationalized throughout the lifecycle of systems, applications and services.

23. Project & Resource Management

Utilize a risk-based approach to prioritize the planning and resourcing of all security and privacy aspects for projects and other initiatives to alleviate foreseeable governance, risk and compliance roadblocks.

24. Risk Management

Govern a risk management capability that ensures risks are consistently identified, assessed, categorized and appropriately remediated.

25. Secure Engineering & Architecture

Implement secure engineering and architecture processes to ensure industry-recognized secure practices are identified and operationalized throughout the lifecycle of systems, applications and services.

26. Security Operations

Assign appropriately-qualified personnel to deliver security and privacy operations that provide reasonable protective, detective and responsive services.

27. Security Awareness & Training

Develop a security and privacy-minded workforce through ongoing user education about evolving threats, compliance obligations and secure workplace practices.

28. Technology Development & Acquisition

Govern the development process for any acquired or developed system, application or service to ensure secure engineering principles are operationalized and functional.

29. Third-Party Management

Implement ongoing third-party risk management practices to actively oversee the supply chain so that only trustworthy third-parties are used.

30. Threat Management

Identify, assess and remediate technology-related threats to assets and business processes, based on a thorough risk analysis to determine the potential risk posed from the threat.

31. Vulnerability & Patch Management

Utilize a risk-based approach to vulnerability and patch management practices that minimizes the attack surface of systems, applications and services.

32. Web Security

Govern all Internet-facing technologies to ensure those systems, applications and services are securely configured and monitored for anomalous activity.