QUANTA

CCPA IT General Controls (ITGCs) Guidance v1.0

INTRODUCTION

California data privacy laws, including the California Consumer Privacy Act (CCPA), require that companies that serve California residents have "reasonable security" in environments where personal data (PII, etc.) is stored. Quanta believes that its security measures exceed this standards in most or all respects; however, it is important that we renew our focus on these efforts, beginning with information pertaining to California residents.

This document outlines the IT controls that should be in place to ensure proper compliance with Quanta policies where Sensitive Personal Information (SPI) or Personal Identifying Information (PII) is stored. Summary of key controls that should be in place for the protection of SPI are listed below; please consult ITGC policies and framework for more details.

Sensitive Personal Information (SPI) includes any documents or other records that contain any of the following:

- Social security number
- Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual
- Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
- Medical information
- Health insurance information
- Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Note that unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.
- A user name or email address, in combination with a password or security question and answer that would permit access to an online account

SELECTED MANDATORY CONTROLS

Type I - In-House Hosted Applications

Access Controls:

- User Management - Access Requests for adding, removing, or changing user access or permissions should be documented, approved and retained. (T0005A, 5B, 5C & 5D)
- User Termination Timeliness – Terminated users, should be removed timely. (T0007A, 7B, 7D, & 7E)
- Password Management - Passwords for accessing information should follow the Quanta password standard and changed periodically. (T00010A, 10B, 10C, 10D, 10E, 10F, 10G, 10H, 10I, 10J, 10K & 10L)
- Quarterly Access Reviews – Users with access to PII information should be reviewed quarterly to ensure that terminated user access has been removed. (T0040A, 40B, 40C)
- Annual Permission Reviews – Access and permissions to folders hosting SPI should be reviewed and formally approved annually. (T00012B, 12C, 12D, 12E, 12F, 12I & 12J)
- Annual Database Review – Access and permissions to databases hosting SPI should be reviewed and formally approved annually. (T0012H)

Change Controls:

- Application Change Management – Infrastructure and application changes (including interfaces and data conversions) should be formally managed to ensure the process is controlled, monitored, documented, and compliant with good practices. (T0033A, 33B, 33C, 33D, 33E, 33G, 33H, 33I, 33J, 33K & 34A)
- Documented Testing – Testing/validation for changes should be documented and retained for all change requests. For SPI, it is important that positive/negative security access testing should be performed. (T0035A & 35B)
- Patch Management – Patch processes should be used to ensure a consistently configured environment, secure against known vulnerabilities. (T0036A, 36B, 36C, 36D & 36E)
- Project Management – For new application deployments or major changes, appropriate project management methodologies should be followed. (T0031A)

Operational Controls:

- Backups – Backups should be employed to ensure critical data is backed-up and available. (T0025A, 25B, 26A, 26B, 26C, 26D, 26E, 26F, 26G, 26H, 28A & 28B)
- Restore Testing – Backup restores should be tested to ensure data is accessible if needed. (T0027A, 27B, 27C, 27D, 27E & 27F)
- Malware Management – Security tools should be in place for all devices to ensure protection from malware. (T0018A & 18B)

Interface Controls:

- Interface Monitoring – SPI data should be monitored to ensure data is transmitted to and from authorized destinations accurately and completely. (T0022A, 24A)
- Interface Encryption – SPI data should be encrypted and secured in transit. (T0023A)

Third-party providers (e.g. Cloud Service Provider (CSP)) Review:

- Third-party providers including Cloud Service Providers hosting SPI must be reviewed by IT Compliance before selection for service.

Type II - Cloud Hosted Applications

Access Controls:

- User Management - Access Requests for adding, removing, or changing user access or permissions should be documented, approved and retained. (T0005A, 5B, 5C & 5D)
- User Termination Timeliness – Terminated users, should be removed timely. (T0007A, 7B, 7D, & 7E)
- Password Management - Passwords for accessing information should follow the Quanta password standard and changed periodically. (T00010A, 10B, 10C, 10D, 10E, 10F, 10G, 10H, 10I, 10J, 10K & 10L)
- Quarterly Access Reviews – Users with access to PII information should be reviewed quarterly to ensure that terminated user access has been removed. (T0040A, 40B, 40C)
- Annual Permission Reviews – Access and permissions to folders hosting SPI should be reviewed and formally approved annually. (T00012B, 12C, 12D, 12E, 12F, 12I & 12J)
- Annual Database Review – Access and permissions to databases hosting SPI should be reviewed and formally approved annually. (T0012H)

Change Controls:

- Vendor Managed per SSAE 16 (SOC) - However, customer is responsible for documenting and retaining Successful Testing/validation evidence. (T0035B & 37A)

Operational Controls:

- Vendor Managed per SSAE 16 (SOC).

Interface Controls:

- Interface Monitoring – SPI data should be monitored to ensure data is transmitted to and from authorized destinations accurately and completely. (T0022A, 24A)
- Interface Encryption – SPI data should be encrypted and secured in transit. (T0023A)

Third-party providers (e.g. Cloud Service Provider (CSP)) Review:

- Third-party providers including Cloud Service Providers hosting SPI must be reviewed by IT Compliance before selection for service.

QUESTIONS?

If you have any questions, please reach out to ITCompliance@QuantaServices.com.