Data Privacy Governance Program

US CCPA

zanda

APRIL 24, 2023

Policies and Procedures

Information security policies (summary info)

Access Control

Access Control Policy defines high-level requirements and guidelines on user account management, access enforcement and monitoring, separation of duties, and remote access.

Business Continuity and Disaster Recovery

The organisation has a Business Continuity and Disaster Recovery Policy that ensures that the organisation can quickly recover from natural and man-made disasters while continuing to support customers and other stakeholders.

Change Management

A formal change management policy governs changes to the applications and supporting infrastructure and aid in minimising the impact that changes have on organisation processes and systems.

Consumer Rights Policy and Procedure

This document explains the rights granted by CCPA and CPRA to consumers with their relevant obligations for the business and sets out a proposed methodology for implementing these rights into business operations.

Data Protection Policy

This document sets out the general principles to be applied by the organisation when handling the personal data referred to as "Individuals" in this document.

Data Retention and Disposal

This policy is about the organisation's approach for data retention and secure disposal.

Incident Management

It is critical to the organisation that security incidents that threaten the security or confidentiality of information assets are properly identified, contained, investigated, and remediated.

Information Security

Zanda utilises InfoSec Platform to manage policies, provide security awareness training, implement and document security controls, and track compliance with customers, third-party vendors, independent auditors and regulatory agencies.

Internal Privacy Policy

This document sets out the general principles to be applied by the organisation when handling the personal data of EU and UK-based individuals ("Data Subjects") or California residents ("Consumers")—collectively referred to as "Individuals" in this document. Demonstrate also the organisation's commitment to safeguarding and appropriately handling our employees' and contractors' personal information.

Network Security

The organisation provides a protected, interconnected computing environment through the use of securely configured network devices to meet organisational missions, goals, and initiatives.

Privacy Impact Assessment (PIA) Policy and Procedure

This document provides guidance on the Privacy Impact Assessment (PIA) methodology to be implemented by the organisation to support the efforts of ongoing compliance with CCPA.

Privacy Policy for Websites

The Privacy Policy describing the generic use and disclosure of personal information that is collected from the individuals online, through websites. This is published on the Zanda website here: zandahealth.com/privacy-policy

Risk Assessment

The organisation institutes regular risk assessments and uses industry best practices in remediation.

Server Security

The organisation manages, configures and protects organisation servers and hosts based on industry best practices.

Vendor Management

The organisation actively manages risks around third-party vendors and their access to the organisation's data.

Workstation and Mobile Device

The organisation protects laptops and workstations and their contents using industry best practices.

Policy Implementation Controls

Access Authentication

TBL3—User Identification and Authentication

Unique user IDs and strong passwords are required to gain access to information assets (database, servers) and applications. Multi-factor authentication (MFA) is enforced for user accounts with access to the organisation's production platform.

Access Management

TBL2—Access Management

The organisation has a formalised process to manage user access requests, changes, and revocations.

User access rights are reviewed on a quarterly basis.

Asset Management

TBL12—Asset Inventory

A list of all data within the organisation is maintained, including the data owner, classification and where it is stored. The asset listing is reviewed and updated by management on an as-needed basis.

Awareness and Training

TBL7—Security Awareness Training

The organisation uses Tugboat Logic's awareness training module to conduct annual information security awareness training for all employees.

Capacity and Performance Monitoring

TBL9—System Performance and Capacity Monitoring

The IT team in the organisation continuously monitors system capacity and performance in its cloud environment(s) to identify anomalies that could compromise the systems' availability.

Change Management

TBL15—Change Management Process

A defined change management process guides changes to the applications and supporting infrastructure. IT management reviews the process document on an annual basis, and it is updated as needed.

Consumer Rights

C—Right to Access/Know

Requests from consumers to access their personal information are documented, retained, and acted upon within 45 days from the receipt of the request. Any delay or denial on request is communicated to consumers and handled in accordance with applicable privacy regulations.

C—Right to Request Deletion

Requests from consumers for deletion of their personal information are documented, retained, and acted upon within 45 days from the receipt of the request. Such requests are communicated to third parties that have access to consumers' personal information in a timely manner.

CS—Opt-in Consent

Explicit consent ("opt-in") is obtained and maintained from consumers prior to the sale or sharing of their personal information. Consumers are provided with a mechanism to withdraw their opt-in consent, and any such requests on withdrawal are handled in a timely manner.

Continuity and Resilience

TBL19—Data Backup and Monitoring

Back-ups are performed with the organisation's defined frequency using an automated system, replicated to a separate location, and monitored for failure.

Control Assessment

TBL22—Control Assessment/Internal Audit

The organisation uses the Tugboat Logic Audit Project module to document its internal controls and continuously monitor its effectiveness. An assessment of the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.

Data Breaches

C—Breach Notifications

Procedures are in place to notify impacted consumers of the personal information breach. Such notifications are documented and provided without unreasonable delay.

C—Incident Management Process

A formal incident management process has been established, which requires incidents (breaches) to be tracked, documented and resolved in a timely manner in accordance with the breach notification rule. The process document is reviewed and updated by management on an annual basis.

Data Privacy

C—Awareness Training

Employees and contractors are required to complete an information security and privacy awareness training as part of the onboarding process and annually thereafter.

C—Data Inventory

Organisations identify and maintain an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection. The documented inventory is reviewed by management on at least an annual basis or during significant changes to ensure it aligns with the organisation's privacy notice.

C—Data Protection Policy

Data Protection policy is established and communicated to employees and contractors within the organisation. The policy is reviewed by management on an annual basis or in case of significant changes.

C—Employee Privacy Notice

The organisation has established a privacy notice for its employee and contractors which specifies their rights, purpose of their personal information collection and organisation's privacy obligations in accordance with applicable privacy laws and regulations. The policy has been communicated and acknowledged by the employees and contractors.

C—Periodic Assessments

Periodic assessments of the systems, tools and processes are performed to identify all locations where personal information is collected, processed and distributed. Deficiencies are tracked, resolved and reported to management in a timely manner.

C—Privacy Impact Assessment

Organisations assess the need for and implement, where appropriate, a privacy impact assessment whenever new processing of personal information or changes to existing processing is planned.

C—Retention of Personal Information

The organisation retains personal information consistent with its privacy commitments and as long as it is required for its intended purpose.

TBL20—Privacy Statement and Terms of Business

The organisation has a privacy policy on its website that defines privacy obligations in accordance with local laws and regulations and is reviewed by management on at least an annual basis. In addition, the organisation has formal agreements in place with customers that acknowledge compliance with security, confidentiality, and privacy commitments.

Data Security
C—Security Procedures and Practices

Appropriate security procedures and practices have been implemented by the organisation for the security and protection of consumers' personal information. These measures are assessed by management on an annual basis, and deficiencies identified are remediated in a timely manner.

TBL6—Encryption of Cloud Data at Rest

The organisation encrypts sensitive data at rest (stored and backup) in its cloud hosting data stores.

Incident Management
TBL14—Incident Notification and Resolution

All incidents related to security are logged, tracked and communicated to affected parties. Incidents are resolved in a timely manner in accordance with the formal incident management process.

Privacy Notice
C—Privacy Notice

The organisation has a privacy policy published on its website, which outlines privacy obligations and specifies individual rights in accordance with applicable laws and regulations. The policy is reviewed by management on an annual basis.

Risk Management
TBL21—Risk Management

The organisation utilises Tugboat Logic's Risk Assessment module to perform an annual risk assessment (which includes risks related to security, fraud, regulatory and technology changes) or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the organisation's executive management.

Security Events Logging and Monitoring
TBL10—System Event Logging

Logging is enabled to monitor activities in the organisation's cloud environment(s). Automated alerts are configured to notify IT management, and issues identified are resolved in a timely manner in line with the incident management process.

Security Operations
TBL13—Encryption of Data in Transit

Encryption technologies are used to protect communication and transmission of data over public networks.

TBL16—Patch Management

The organisation maintains a patch management process to confirm the timely remediation of operating system vulnerabilities. In addition, production systems are scanned to test for patch compliance on a quarterly basis.

TBL17—Vulnerability Assessment or Penetration Testing

A vulnerability assessment or penetration test is conducted on an annual basis to identify security exploits. All identified issues are classified according to the risk analysed and remediated in a timely manner.

Vendor Management

C—Contracts with Service Providers

The organisation maintains written contracts with service providers who process the personal information of consumers on behalf of the organisation. These contracts outline the security and privacy requirements that are required to be implemented by the service provider for the protection of consumer's personal information.

C—Vendor Management Process

A vendor management process has been implemented whereby management performs risk assessments of potential new vendors/ service providers and evaluates the compliance of existing vendors on an annual basis. Corrective actions are taken as required based on the results of the assessments.

Workstation Security

TBL4—Workstation Antivirus and Firewall

The Organisation has installed and enabled Anti-Virus, Anti-Malware and Firewall on all workstations.