SUZY

Security Measures

Suzy employs appropriate technical and organizational measures to protect against unauthorized or unlawful Processing of Client Personal Data and against accidental loss or destruction of, or damage to, Client Personal Data (“*Information Security Program*”), in accordance with applicable law including Data Protection Laws. Suzy’s Information Security Program includes specific security requirements (“*Security Measures*”) and cover the following areas:

A. Information Security Policies and Standards

Suzy maintains written information security policies, standards, and procedures. These policies, standards, and procedures are kept up to date and revised whenever relevant changes are made to the information systems that use or store Client Assets and Client Personal Data (collectively, “*Client Data*”). These policies, standards, and procedures are designed and implemented to:

1. Prevent unauthorized persons from gaining physical access to Client Data Processing systems (e.g., physical access controls);
2. Client Data Processing systems from being used without authorization (e.g., logical access control);
3. Ensure that Data Personnel gain access only to such Client Data as they are entitled to access (e.g., in accordance with their access rights) and that, in the course of Processing or use and after storage, Client Data cannot be viewed, copied, modified or deleted without authorization (e.g., data access controls);
4. Ensure that Client Data cannot be viewed, copied, modified, or deleted without authorization during electronic transmission, transport or storage, and that the recipients of any transfer of Client Data by means of data transmission facilities can be established and verified (e.g., data transfer controls); and
5. Ensure that all systems that Process Client Data are the subject of a vulnerability management program that includes without limitation regular internal and external vulnerability scanning with risk rating findings and formal remediation plans to address any identified vulnerabilities.

B. Physical Security

Suzy maintains commercially reasonable security systems at all Suzy sites at which an information system that uses or stores Client Data is located (“*Processing Locations*”) that include reasonably restricting access to such Processing Locations, and implementing measures to detect, prevent, and respond to intrusions.

C. Organizational Security

Suzy maintains information security policies and procedures addressing:

1. Data Disposal. Procedures for when media are to be disposed or reused have been implemented to prevent any subsequent retrieval of any Client Data stored on media before they are withdrawn from the Suzy's inventory or control.
2. Data Minimization. Procedures for when media are to leave the premises at which the files are located as a result of maintenance operations have been implemented to prevent undue retrieval of Client Data stored on media.
3. Data Classification. Policies and procedures to classify sensitive information assets, clarify security responsibilities, and promote awareness for all employees have been implemented and are maintained.
4. Incident Response. All security incidents are managed in accordance with appropriate incident response and remediation procedures.
5. Network Security. Suzy maintains commercially reasonable information security policies and procedures addressing network security.

D. Access Control (Governance)

Suzy governs access to information systems that Process Client Data. Only authorized Suzy staff can grant, modify, or revoke access to an information system that Processes Client Data. Suzy implements commercially reasonable physical and technical safeguards to create and protect passwords.

E. Endpoint Security

Suzy maintains commercially reasonable information security policies, procedures, and technical controls when addressing endpoint security.

F. Personnel

Suzy has implemented and maintains a security awareness program to train all employees about their security obligations. This program includes training about data classification obligations, physical security controls, security practices, and security incident reporting. Suzy takes reasonable steps to ensure the reliability of any Data Personnel who may Process Client Data.

G. Sub-Processors

Suzy will only select and contract with Sub-Processors that are capable of maintaining appropriate security safeguards that are no less onerous than those imposed upon Suzy.

H. Confidentiality

Data Personnel with access to Client Data are subject to confidentiality obligations, including Non-Disclosure Agreements.

I. Business Continuity

Suzy implements disaster recovery and business resumption plans. Business continuity plans are tested and updated annually (minimum) to ensure that they are up to date and effective. Suzy shall also adjust its Information Security Program in light of new laws and circumstances, including as Suzy's business and Processing of Personal Data change.

J. Audits

At least once per year, Suzy will conduct site audits of its Client Data Processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under its agreements with clients, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognized third-party audit firm based on recognized industry best practices.

K. Risk Management Program

Suzy performs a risk assessment where appropriate before Processing Personal Data.

Last Updated: January 17, 2024