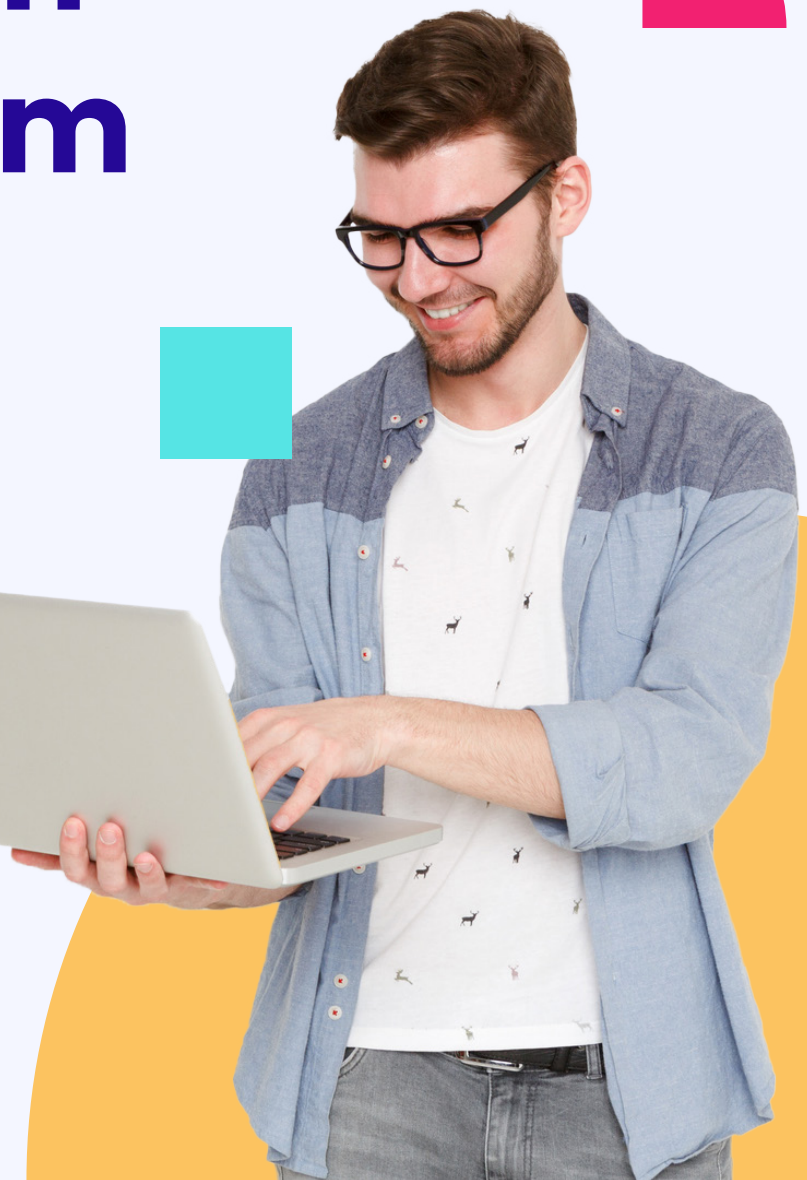
SPIFF

Spiff Information Security Program



April 20, 2022

Table of Contents

Information Security Policies (Summary Info)

AC5 - Passwords

Organization members use strong passwords.

AC9 - Server Security

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

AC10 - Database Credentials

The organization uses strong passwords and protects credentials for databases using industry best practices.

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.

AM1 - IT Asset Management

The organization closely manages IT systems and the data that they contain from purchase to disposal.

Annual Security Awareness Training

All employees and contractors must view the annual Security Awareness Training video.

AU1 - Internal Audit

The organization conducts Internal Audits on its existing policies and controls in order to ensure the best level of service to its customers.

Backup and Restoration

The organization actively manages risks associated with data loss by defining a sound backup regime for all the data services.

BC1 - Business Continuity Policy

Spiff has a Business Continuity Plan that ensures that the organization can quickly recover from natural and man-made disasters while continuing to support customers and other stakeholders.

Bring Your Own Device (BYOD)

This policy is intended to protect the security and integrity of organization's data and technology infrastructure when employees are using their personal device(s) to connect to organization's corporate network.

Data Retention and Disposal

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

DGP1 - Data Classification

The organization understands how to determine what information is sensitive and how to handle each level of sensitive information. This includes public, company confidential and 3rd party confidential information.

Disciplinary Policy

The organization has implemented a disciplinary process in order to deal with instance(s) of indiscipline including (but not limited to) non-compliance to information security policies and procedures by users.

GDPR Privacy Field Manual

Field Manual for Spiff Employees.

IC3 - Internet Usage

Organization members use the organization internet connection responsibly and appropriately.

IC4 - Information Sensitivity

The organization understands how to determine what information is sensitive and how to handle each level of sensitive information. This includes public, company confidential and 3rd party confidential information.

IC7 - Wireless Communication

The organization uses wireless devices and infrastructure responsibly.

IC8 - Workstation Security

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

IC12 - Network Security

Spiff provides a protected, interconnected computing environment through the use of securely configured network devices to meet organizational goals.

IC13 - Processing Integrity

Spiff ensures that system processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

Internal Privacy Policy

Demonstrate the organization's commitment to safeguarding and appropriately handling our employees' and contractors' personal information.

IR1 - Data Breach Computer Incident Response Plan

The purpose of this document is to establish a collaboratively developed, documented, and validated plan that enables Spiff to immediately respond to a data compromise in a manner that demonstrates appropriate Due Diligence in order to protect the integrity of our systems, defend against potential litigation, maintain confidence in the Spiff brand, and ultimately preserve shareholder value and customer privacy.

IR2 - Malware Outbreak Computer Incident Response Plan

A collaboratively developed, documented, and validated plan that enables Spiff to immediately respond to a malware outbreak in a manner that demonstrates appropriate Due Diligence in order to protect the confidentiality, integrity, and availability of our systems, continue to provide quality products and services to our customers, maintain confidence the Spiff brand, and ultimately preserve shareholder value.

ISMS2 - Information Security Policy

This is the high-level Information Security Policy

Key Management and Cryptography

The organization utilizes the latest commercially accepted encryption protocols.

OM2 - Information Security Program Management

An ISMS (information security management system) provides a systematic approach for managing an organisation's information security. It's a centrally managed framework that enables you to manage, monitor, review and improve your information security practices in one place. It contains policies, procedures and controls that are designed to meet the three objectives of information security: Confidentiality: making sure data can only be accessed by authorised people. Integrity: keeping data accurate and complete. Availability: making sure data can be accessed when it's required.

OM3 - Personnel Security

Organization members understand their roles and responsibilities around security and privacy.

OM4 - Acceptable Use

Organization members are informed about what they can and cannot do with company resources.

OM8 - Corporate Ethics

The organization values ethics trust and integrity throughout our business practices.

OM10 - Security Awareness Training

In addition to the monthly awareness videos, Spiff employees and contractors are required to attend/watch the comprehensive security awareness training. This page (not a policy) will hold the link to the training, and users can attest if they've watched it.

Physical and Environmental Security

Physical and Environmental Security is paramount to protecting any organizations assets. Regardless of the technical controls implemented, if an organization does not have good physical security then they may be vulnerable. This policy seeks to limit those vulnerabilities.

Public Privacy Policy

The generic use and disclosure of personal information that is collected from the individuals online, through websites.

RM1 - Risk Assessments

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

RM2 - Third-Party Vendor Management

The organization actively manages risks around 3rd party vendors and their access to Spiff data.

SD1 - Software Development Security

The organization designs and builds software with security and privacy as design principles.

Serverless Security

The organization has established guidelines for the secure deployment and maintenance of the serverless architecture.

SM3 - Vulnerability Scanning

The organization uses regular application/network scanning, penetration tests.

SO4 - Change Control and Configuration Management

The organization closely manages process changes and system configurations to ensure availability and integrity of those processes and systems.

TBL-001 Product/Service Description

Spiff imports sales tracking data and uses it to implement an incentive compensation plan specified by customers. Spiff provides access, auditing, management and tracking of sales performance compensation to customer employees.

TBL-102 Clean Desk

Organization members keep their workspaces neat and organized while protecting sensitive information.

TBL-103 Customer Information

Spiff maintains a strong commitment to customer information security and protection. The Customer Information Security Policy defines what information can be disclosed to non-employees, as well as the sensitivity of information that should not be disclosed outside of Spiff without proper authorization.

TBL-104 Email Use

Employees and contractors representing Spiff with an Spiff email address approach all external email with professionalism and integrity in mind.

TBL-106 Email Retention

The organization retains email messages critical to the business and in accordance to local regulations.

TBL-107 Email Authentication

Email sent from organization domains are authenticated using standard protocols such as SPF, DKIM and DMARC.

TBL-120 Visitor Office Access

The organization tracks and controls visitor access to facilities and assets.

TBL-207 Environmental Protection

Spiff acknowledges a responsibility to the environment, and we express our commitment toward implementing practices that will promote environmental sustainability.

TBL-208 Equality and Diversity

Spiff stands in support of both inclusion and diversity in all operations, employment decisions and in all professional interactions, both within and outside the organization. Furthermore, Spiff recognizes that discrimination, harassment and similar mistreatment of others are unacceptable and sets the below guidelines to ensure the fair and appropriate treatment of employees and others.

TBL-315 Personal Devices and Voicemail

The organization requires protection of personal devices and voicemail.

TBL-317 Removable Media

The organization is aware of the risks of removable media in both loss of data and potential inbound attacks. Utilization of removable media is done carefully.

Technology Equipment Handling and Disposal

The organization appropriately disposes of equipment that contains sensitive information.

Working from Home

Working from home policy provides a framework for working from home where it is both practical andacceptable.