Important Note to User: This is a sample agreement and not "one-size-fits-all" and should not be used by any organization without review and modification to fit the needs of such organization. Organizations should cross-reference with relevant existing policies where appropriate, comparing against relevant policies (e.g. mobile device and acceptable use policies), ensuring terms are defined consistently across policies. Additional changes to this policy may be necessary to account for varying individual organizational security needs and user privacy expectations. In addition, while efforts have been made to ensure that the terms of this policy comply with employee rights under the National Labor Relations Act, this is a contentious and ever-changing area of the law, and therefore total compliance cannot be guaranteed. **Delete this note before publishing.**

Sample Payment Card Information Security Policy

Establishment date, effective date, and revision procedure

This policy was established and approved by [Organization Name] on [mm,dd,yyyy]. The [Organization Name] Information Security department shall review this policy at least once a year, and at any additional time when there are changes that may affect corporate management with respect to Information Security. In the event that amendment or repeal of this policy becomes necessary as a result of such review, the [Organization Name] Information Security department shall prepare a draft and apply for authorization, and with prior confirmation of the Executive(s) in charge of the area(s) that will be affected by amendment or repeal, the [Organization Name] CISO/Security Director will authorize the amendment or repeal.

Table of revision history

Version	Date	Details of change	Issued by	Approved by

Overview

[Organization Name] seeks to meet the data security expectations of customers and vendors with whom it has a business or professional relationship. As a processor of payment card information, the organization understands that it is responsible for highly sensitive information belonging to customers and/or vendors that must be appropriately safeguarded in accordance with the Payment Card Industry Data Security Standards (PCI-DSS). In order to provide adequate safeguards for this information, the organization will create and implement a PCI-DSS Compliance Plan.

Purpose

The purpose of this policy is to create and maintain a PCI-DSS Compliance Plan to ensure payment card and other sensitive information is adequately safeguarded against unauthorized access, acquisition, alteration, or disclosure.

Scope

This policy applies to employees, contractors, consultants, volunteers, temporary and other workers at [Organization Name], and all personnel affiliated with company subsidiaries or third parties. This policy applies to all equipment that is owned or leased by, or otherwise in the custody or control of [Organization Name].

Policy

Development of a PCI-DSS Compliance Plan

As a processor of payment card information, [Organization Name] understands its compliance obligations under the PCI-DSS and seeks to protect sensitive customer information in its possession or control. As such, the organization's executive management including the Chief Executive Officer, Chief Information Officer, and Chief Financial Officer, and a designated Information Technology Officer [*and anyone else within the organization deemed necessary*], will work together to develop an organization-wide PCI-DSS Compliance Plan (Plan). Such Plan will comply with the most up-to-date version of the PCI-DSS and will be reviewed for updates on at-least an annual basis. Additional review of the Plan shall be undertaken as soon as practicable after release of any new versions of the PCI-DSS to ensure the organization's continued compliance.

At all times data security standards implemented in the Plan shall meet the minimum requirements set forth in the latest version of the PCI-DSS. However, in their discretion, [Organization Name] executive management may require additional safeguards in the Plan than those required by the PCI-DSS in order to address evolving organizational needs.

[Organization Name] understands that it may have additional data security and privacy compliance obligations under federal and/or state law which shall be addressed through additional safeguards, as necessary.

Policy Compliance

Compliance Measurement

Compliance with this policy will be verified by the [*Organization Name*] through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the [Policy Owner].

Exceptions

Any exception to the policy must be approved by the [Policy Owner] in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

By signing below, I acknowledge that I have read and fully understand my obligations under this Policy and hereby agree to abide by its terms.

_____	_____
Name	Date