Risk Management Policy

Purpose

The purpose of this policy is to establish a framework for managing risk at <Company Name> and incorporating risk assessments throughout the company's operations, ensuring that risk is kept within an acceptable tolerance. Well-managed risk helps<Company Name> provide transparency and justification for the various security controls implemented throughout the company.

Scope

This policy applies to all company information systems and data.

Ownership

[POLICY OWNER]

is responsible for implementing and maintaining this policy.

Policy Statement

<Company Name> uses formal risk management practices to gain accurate and thorough understanding of the potential risks to and vulnerabilities of the confidentiality, integrity, availability, and safety of the company's information and information systems.

Risk Management

The company maintains a risk management program to identify, prioritize, and mitigate risk to acceptable levels.

<Company Name> follows a risk-based approach to security. In a risk-based approach, security controls are prioritized and adopted based on the risk they mitigate and the value of the asset they protect, as opposed to the requirement they satisfy. A risk-based approach ensures that all relevant compliance, regulatory, and contractual requirements are satisfied, but balances the rigor with which they are satisfied against the level of risk they mitigate.

<Company Name>'s risk-based security approach is integrated into its information security program by way of thorough and timely risk assessments. During each assessment, risk is evaluated for all potential threats and vulnerabilities to the confidentiality, integrity, and

availability of Customer Confidential and any other regulated data that <Company Name> stores and/or processes.

All company employees have a responsibility to identify, analyze, evaluate, monitor, and communicate risks associated with any activity, technology, function, or process within their relevant scope of responsibility and authority.

Overall, the execution, development, and implementation of risk assessments and remediation

is the joint responsibility of the company's security team, and the department or individuals responsible for the area being assessed. All staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff are further expected to work with the risk assessment project lead in the development of a remediation plan for each risk assessment performed.

A completed risk assessment produces a risk register with a risk treatment action plan to manage or mitigate any residual risk that exceeds the organization's risk tolerance.