Last Revision Date: February 4th, 2024

Information Security Policy

(For SimplyCyber Financials: Mid-sized financial management company)

Purpose:

Information and systems are used by the company to deliver value to our customers and business partners/ as such, the information has value and must be protected per its sensitivity.

This policy outlines the expectations and behaviors of the organization to protect those systems, applications, and information confidentiality, integrity, and availability.

This policy's approach is to comprehensively provide the full scope of policy for delivering sound information security to the organization.

Scope:

This policy applies to all staff at "SimplyCyber Financials" and its subsidiaries, including any third-party staff contracted or providing services on behalf of "SimplyCyber Financials". This policy applies to all systems, applications, and data within the "SimplyCyber Financials" business and information technology (IT) systems including Software-as-a-Service (SaaS) (aka cloud systems).

Policy:

The following statements provide the information security policy for the organization. Any exclusion to the policy statements below must be explicitly documented.

Information Security

The organization shall ensure information security is part of the overall risk management strategy.

Access Control

The following policies are associated with the control of access to systems and data.

1. Any access granted to "SimplyCyber Financials" systems, applications, and data shall require appropriate approval.
2. All access to systems, applications, and data shall be documented and reviewed for validity on Management-approved frequency.
3. Account access to systems, applications, and data shall be removed when no longer appropriate on demand, or as discovered during review.
4. User account types shall be appropriate for the user access required, i.e. general user, privileged user, non-staff (3rd-party), guest, and emergency users.

Authentication

1. All access to organizational systems, applications, and data that is accessible via the Internet (i.e. internet-facing systems) shall require multi-factor authentication).
2. All mobile devices (i.e. tablets, mobile phones) shall have an authentication mechanism to unlock and access the device.

Remote Access

1. Remote access shall be allowed using management-approved remote access solutions.
2. Third-party remote access shall be reviewed and approved.
3. third-party remote access shall require a member of SimplyCyber Financials to explicitly authorize or approve the access on demand
4. No attended access shall be granted to any company resources (systems, data, applications).

Related Procedures:

1. Access control approval procedure
2. Remote access approval
3. MDM enrollment

Non-Compliance:

1. Any individuals to whom this policy applies are required to follow the policy. Non-compliance with the policy will result in appropriate management-guided sanctions.

Management Commitment/Authority:

This policy is supported and approved by [name/role]. This is the published information security policy effective publish date.

CEO Nato Riley ----------

Review Schedule:

This policy shall be reviewed and updated per management-defined frequency and disseminated to all applicable users as updates occur.

Definitions:

1. Systems, applications, and data are the software, hardware, and third-party, and cloud assets that the organization uses to perform business.
2. Mobile device - Devices that are "travel" and are typically on an individual's persons and travel outside the office environment. This includes mobile phones, tablets, and laptops.