GRC Security Policy Practical Lab

SimplyCyber Financials

Information Security Policy

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 in accordance with its sensitivity.

Risk policy outlines the expectations and behaviors of the organization to protect those systems, applications, and information confidentiality, Integrity, and Availability

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

Scope

This policy applies to all staff at SimplyCyber Financial and its subsidiaries, including any third-party staff contracted or providing services on behalf of SimplyCyber Financial.

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 exclusions 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 Financial systems, applications, and data shall require appropriate approval.
2. All-access to systems, applications, and information 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 as review.
4. User account types shall be appropriate for the user access required, i.e. general user, privileged user, non-users (3rd party), guest, and emergency users.
5. Shared user accounts shall be explicitly approved for use by management on a case-by-case basis

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, and 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 the SimplyFinancial Financials to explicitly authorize or approve the access on-demand.
4. No attended access shall be granted to any company resources (systems, data, apps)

Related Procedures

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

Non-Compliance

1. Any individual to whom this policy applies is required to follow the policy will result in appropriate management-guided sanctions.

Management Commitment / Authority

This policy is supported and approved by {name/roll}. This is the published information security policy effective publish date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CEO Nate Rile

Review Schedule

This policy shall be reviewed and updated in accordance with management-defined frequency and disseminated to all applicable users.

Definitions

1. Systems, applications, and data - These are the software, hardware, third-party, and cloud assets that the organization uses to perform business
2. Mobile device - A piece of portable electronic equipment that can connect to the internet, especially a smartphone or tablet computer.