Acceptable Use Policy

Cardinal Financial

November 23, 2025

Policy Statement: The purpose of this policy is to advise employees and associates of how to properly access and utilize sensitive and confidential information contained in any media, data information and banking systems. This acceptable use policy will help meet security objectives and reduce the risk of security breaches.

Scope: This policy applies to all employees, associates, information systems, banking systems and all devices where data is being accessed, exchanged, altered or viewed.

Section 1.0 Authorized Use of Resources

I. Banking resources and data shall only be accessed, altered or updated if needed to perform a work-related task for Cardinal Financial. Data accessed for personal knowledge or gain could be escalated to termination and legal penalties for misuse.

Section 2.0 Access Control and Authentication

I. Role-based access control protocol shall be in place to ensure only resources will be accessed by the appropriate personnel.

II. Multi-factor authentication shall be used as a technical control to verify identity before access to critical resources

II. Strong passwords shall be used as a layer of security before accessing resources; sharing of passwords is prohibited

Section 3.0 Data Protection and Confidentiality

I. Secure encryption protocols shall be used when data is at rest, in transit and in use.

II. Data and banking information shall be securely stored with appropriate security mechanisms such as hashing and symmetric encryption

III. Physical data storages and medias shall be properly secured using appropriate security measures

Section 4.0 Prohibited Activities

I. Sharing of data and media to unauthorized persons or entities is strictly prohibited and can result in termination and or legal penalties

II. Unauthorized software or hardware shall not be downloaded nor installed without change approval

III. Personal devices shall not be used for official Cardinal Financial business unless authorized

IV. Engaging in fraudulent or illegal activities will result in legal penalties

Section 5.0 Monitoring & Reporting

I. Data loss prevention systems shall be used to monitor and prevent critical or sensitive data from being exfiltrated

II. Monitoring and alerting systems shall be used to detect, alert and prevent unauthorized retrieval of information

III. Employees and associates shall report any misuse of resources and data to supervision and or law enforcement authorities

IV. Any breaches in security shall be investigated and remedied appropriately, following the incident response plan implemented by Cardinal Financial

Policy Updates and Review

The user acceptance policy shall be updated and reviewed as needed to ensure compliance with regulatory standards and best practices

Auth: Briana A. Robinson