Employee & Associate Role-Based Access Control Policy

Cardinal Financial

Policy Statement: The purpose of this policy is to establish mandatory standards for role-based access control for all employees and associates. It is the objective of Cardinal Financial to protect both employees and customers by limiting access by means of technical, administrative controls to prevent unauthorized access to critical data.

Scope: This policy applies to all personnel, associates, information systems and data

Section 1.0 Roles and Privileges Scheme

I. Privileges and permissions are allocated based on set role and are in alignment with the principal of least privilege

> *Least privilege- the practice of only having just enough access permissions to carry out duties and tasks

Section 2.0 Provisioning and Deprovisioning of Access

I. Roles will be assigned at time of onboarding; appropriate access will be given during onboarding that is in direct alignment with role.

II. Proper deprovisioning and deactivation of access will occur at time of resignation or termination

III. At time of a role change, the employee or associate's permissions shall be immediately adjusted manually or automatically

IV. Temporary permissions shall be given to allow pertinent tasks to be carried out

Section 3.0 Authentication & Restriction Guard Rails

I. In addition to credentials, users will be properly authenticated into systems using an MFA technology

II. Guard rails shall be applied to systems to disable access if any suspicious attempted authorization is detected

a. Any indications of malicious attempts to access systems shall be reported to the IT department immediately

Section 4.0: Policy Revision and Updates

Policy shall be reviewed and updated when changes are made in processes or protocols

Roles and Access Chart for Cardinal Financial

Role	Access/Privileges
Bank Manager	Full branch level access; employee oversight, financial reports, escalations
Assistant Manager	limited approval authority; staff scheduling, customer service resolution
Lead Bank Teller	Override capabilities for teller transactions, cash drawer access, vault access
Bank Teller	Basic transactions, cash drawer
Loan Processor	Loan applications, customer financials, document verification
Credit Analyst	Credit reports, financial statements, risk scoring tools, internal credit models
Investment Banker	Market data, client portfolios, trading platforms, deal documentation
Customer Service Rep	Customer profiles, account/closing, service requests, limited transaction view
Security Guard	Building key, access to cctv footage, emergency protocols
Accountant	General ledger, financial statements, reconciliation tools, budget systems
Auditor 1	Internal audit logs, transaction histories, compliance reports
Auditor 2	Broader audit access: cross-branch data, regulatory compliance systems
Mortgage Consultant	Mortgage applications, customer financials, property documents, approval workflows
Lead IT Associate- Cardinal	Full system admin rights, network access, user provisioning, incident response
IT Associate- Cardinal	System maintenance, helpdesk tools, limited admin rights, software deployment
Data Security Engineer-Duke	Encryption systems, intrusion detection, access logs, vulnerability mgt

Lead Security Analyst	Threat intelligence, SIEM dashboards, incident response coordination
Tier 1 Security Analyst– x5	Monitor alerts, escalate incidents, basic log access, endpoint security tools
Tier 2 –Security Analyst–x5	Deeper forensic access, threat hunting tools, firewall and network monitoring