**Policy 2225: Digital Banking**

**Model Policy Revised Date: 05/13/2024**

**General Policy Statement:**

(Credit Union) follows the guidelines set forth below regarding digital banking. Digital banking refers to any banking service or platform that utilizes Internet or mobile cellular network communications for providing users and members with banking services or transactions. In order to keep pace with members’ needs and the evolution of digital banking services and solutions, the credit unions will adopt digital banking products and services understanding the risks and the need for effective risk management analysis and controls. The Credit Union will employ risk management principles and practices that support the Credit Union’s strategic priorities and consider associated risks with the proper management and balance of technology. The critical elements of a successful digital banking ensure are outlined in this policy and adopted by the Board of Directors. The Board of Directors further instructs Management to insure all digital banking services that are offered are in compliance with applicable laws and regulations.

1. **STRATEGIC PLANNING.** The Credit Union will create and maintain a strategic plan outlining the Credit Union’s use and evolution of technology.
2. **THREAT LANDSCAPE.** The Credit Union understands the risks associated with digital banking. One form of risk is authentication that arises from expanded remote access to information systems, the different types of devices and third parties accessing information systems, use of applicable program interfaces (APIs) and increased connectivity to third parties. When possible, the Credit Union will utilize multi-factor authentication (MFA), combined with network segmentation and least privilege user access to mitigate the risk of unauthorized access that can result in a threat actor changing system configuration, exfiltrating data, or moving laterally within a network or system.
3. **RISK ASSESSMENT AND MITIGATION PROCESS.** Before implementing new digital banking services, and on a periodic basis, the Credit Union will perform a risk assessment to understand and mitigate the associated risks. The Credit Union will review and update its risk assessment as new information becomes available (prior to implementing new digital banking services) or at least once every 12 months. The risk assessment will include input from different business functions/departments throughout the Credit Union to get relevant data and perspective (e.g., cybersecurity, member service, fraud research, etc.) As part of this process, the Credit Union will do the following:  
   1. Inventory all information systems and their components, such as hardware, operating systems, applications, infrastructure devices, APIs, data, and other assets, which require authentication and access controls. This inventory includes information systems provided by the Credit Union’s third parties, such as cloud service providers.
   2. Inventory digital banking services, members, and transactions that may warrant authentication and access controls. The Credit Union will include components such as membership type (business vs. consumer), transactional capabilities (bill payment, wire transfer, loan origination, etc.), member information accessed and transaction volumes. The Credit Union will also take into consideration digital services that have shorter processing windows, push-payment capabilities, and limited fraud management functionality.
   3. Identify digital banking members engaged in transactions who present a higher risk of financial loss or potential breach of information for which enhanced authentication controls are warranted. This may include higher dollar amount, large volume, the sensitivity and amount of information accessed, the irrevocability of the transactions and the likelihood and impact of fraud.
   4. Identify all users, including employees, service accounts, and users of third parties that access the Credit Union’s information systems and data. Consider functionality, criticality, and associated risks of information systems and data, along with user access rights or permission.
   5. Identify users who represent high risk, and for which enhanced authentication controls are warranted to protect information systems. This includes access to critical systems and data and privileged users who are trusted to perform security-relevant functions that ordinary users are not authorized to perform. This would include security administrators, remote access to information systems and key positions such as senior management. These users would warrant enhanced controls and should be considered “high-risk users.”
   6. Risk will vary based on the electronic payment systems utilized. The Credit Union will identify the payment systems utilized based on transaction types and methods of settlement and distribution such as P2P (peer-to-peer) transactions processed on the ACH network and will implement proper controls to mitigate risk. As further outlined within this policy and procedures, mitigation will include transaction limits (daily and monthly), verification of first-time transactions, right to revoke access, etc.
   7. Identify threats with reasonable probability of impacting the Credit Union’s systems, data and user/member accounts. Examples may include malware including ransomware, man-in-the-middle (MIM) attacks, credential abuses, and phishing attacks. Threat identification intelligence from Information Sharing and Analysis Organizations and a review of actual or attempted incidents of security breaches, identify theft or fraud experienced by the Credit Union or industry will be used. Consider risks associated with fraud, processing errors, system disruptions, or other unanticipated events that might result in an inability to deliver the digital products and services.
   8. Initially and periodically assess the design and effectiveness of access and authentication controls employed, including the availability of more advanced security options and configuration settings. With proper risk assessments, residual risk is considered for acceptance or additional corrective action according to internal policies that define risk appetite and tolerance.
4. **LAYERED SECURITY.** Layered security includes multiple preventative, detective, and corrective controls and is designed to compensate for potential weakness in any one control. The Credit Union may use different controls to mitigate inherent risk associated with, and protection against unauthorized access to information systems and digital banking services. These controls may include (but are not limited to), MFA, user time-out, system hardening, networking segmentation, monitoring processes, and transaction amount limits. The Credit Union will apply authentication controls commensurate with the increasing level of risk associated with a transaction or access to an information system.
   1. Multi-factor Authentication (MFA) is an authentication system that requires more than one distinct authentication factor for successful authentication. MFA can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have and something you are (NIST – National Institute of Standards and Technology). When the Credit Union’s risk assessment indicates that single-factor authentication with layered security is inadequate, MFA or controls of equivalent strength as part of a layered security will be used to more effectively manage risk. Some MFA factors may include:  
      1. Memorized secrets;
      2. Look-up secrets;
      3. Out-of-band devices;
      4. One-time password devices;
      5. Biometrics identifiers; or
      6. Cryptographic keys.
   2. MFA solutions and other layered security controls may vary depending on the different risks presented by the type of member (consumer vs. business) and the different services. For high-risk users, strong authentication, such as MFA solutions using hardware and crypto graphic factors may be used to mitigate risks associated with unauthorized access to information. The Credit Union will also use standards and controls to protect the integrity of authentication factors and communication channels.
5. **MONITORING AND REPORTING.** In order to determine if attempted or realized unauthorized access to information systems and accounts has occurred, the Credit Union will conduct appropriate monitoring, activity logging and have a system of reporting processes and controls. The Credit Union will also conduct timely investigations of unusual or unauthorized activity in compliance with applicable regulation.
6. **EMAIL AND INTERNET ACCESS POINTS.** Email accounts and Internet browsers are common access points used by threat actors to gain unauthorized access, obtain or compromise sensitive data, or to initiate fraud. In order to mitigate this risk for email systems, the Credit Union will implement secure configurations, MFA or equivalent access techniques, provide continuing educating to users, patch vulnerabilities, and implement software vendor and service provider recommended controls for outsourced services. In order to mitigate risk for Internet browsers the Credit Union will block browser pop-ups and redirects and limit the running of script languages.
7. **SOCIAL ENGINEERING.** Social engineering and other techniques are frequently used by threat actors to deceive member call center and IT help desk representatives into resetting passwords and other credentials, which may grant unauthorized access to information systems, member accounts or confidential information. Members may also fall victim to fraud by providing digital banking credentials and/or using P2P transactions for unintended fraudulent transactions. The Credit Union will mitigate this risk by identifying emerging threats, setting secure processes, conducting employee training, and establishing effective controls for the Call Center and IT Help Desk Operations. The Credit Union will also communicate with members to generate awareness of possible fraudulent threats in an effort to mitigate the impact when possible.
8. **DATA AGGREGATORS.** Data aggregators and other customer-permissioned entities (collectively CPEs) provide data aggregation and other services to business and consumer members. As part of the Credit Union’s risk management process, it will include an assessment of risks and effective mitigation controls for credential and API-based authentication when CPEs access the Credit Union’s information systems and member information.
9. **IDENTITY VERIFICATION.** Reliable identity verification methods can help reduce risk when establishing new member accounts and when access is first requested for new users of information systems. Identity verification can reduce the risk of identity theft, fraudulent account applications, and unenforceable account agreements or transactions. The Credit Union complies with the requirements of the USA PATRIOT Act as outlined in Policy 2110: Bank Secrecy Act/Anti-Money Laundering Program and has a member identification and due diligence program.
10. **MANAGING THIRD-PARTY RELATIONSHIPS.**
    1. **Assessing Outsourcing Arrangements.** Prior to outsourcing digital banking, the Credit Union will perform a requirements analysis to identify the Credit Union’s specific needs (i.e., the level of services and support required; the functionality and capacity required; and system performance requirements), pursuant to its Vendor Due Diligence & Oversight policy.
    2. **Understanding Risks.** The Credit Union will determine the following:
       1. The Credit Union’s ability to evaluate and oversee the outsourced relationship;
       2. The importance and criticality of services provided;
       3. The requirements for outsourced activity;
       4. The contractual obligations and requirements for the service provider, including independent validation/certification of the service provider’s control environment and financial condition;
       5. The service provider’s and the Credit Union’s responsibilities for security, privacy, and regulatory compliance; and
       6. Contingency plans, including availability of alternative service providers, costs and resources required to switch the service provider.
11. **Contractual Considerations.** Management will ensure that the contract between the Credit Union and the service provider is clearly written and sufficiently detailed to provide assurances for performance (operational, financial and system), reliability, security (firewalls, intrusion detection, bonding of employees), privacy, ownership of data, disaster recovery capabilities, and reporting (e.g., performance, audited financial reports, Service Organization Controls (SSAE 16), security evaluation summaries, security incidents impacting the Credit Union, etc.). The Credit Union will obtain a legal review of all contracts associated with its digital banking products.
12. **Oversight Program.** The Credit Union will monitor its digital banking service provider’s controls, conditions, and performance. As part of this process, Management will do the following:
    1. Clearly assign responsibility for the administration of any digital banking service provider(s);
    2. Ensure the level of effort (i.e., number of personnel assigned, functional responsibilities, and amount of time needed) to monitor the service provider equals the scope, complexity, and risk relative to the service provider; and
    3. Set standards for the maintenance of documentation to be used for contract negotiations, termination issues, and contingency planning.
13. **Awareness and Education.** The Credit Union’s consumer awareness and education efforts will address both consumer and business members and, at a minimum, will include the following:
    1. Education about a range of authentication risks and other security considerations when using digital banking services;
    2. An explanation of how members can determine the legitimacy of communications from the financial institution, particularly communications that seek information that could be used to access the member’s account.
    3. An explanation of the legal and other rights and protections a member may have in the event of unauthorized access to an account, including protections under Regulation E;
    4. Educational information regarding prevalent external threats and methods used to illegally access accounts and account information, such as phishing, social engineering, mobile-based trojans, and business email compromise;
    5. An explanation of controls the Credit Union offers that members can use to mitigate risk, such as MFA.
    6. An explanation of communication mechanisms that members may use to monitor account activity, such as transaction alerts;
    7. An explanation of situations in which the Credit Union uses enhanced authentication controls, such as call center contact or certain types of account activity like password reset;
    8. A listing of Credit Union contacts for members’ discretionary use in the event they notice suspicious activity or experience member information security-related events they want to report.
14. **CONTROLS.** The Credit Union should ensure adequate controls are in place to minimize risk. The following types of controls may be utilized by the Credit Union.   
    1. **Password Control.**
       1. **Password Protection**. Passwords are stored in a manner that makes them resistant to attack and possible compromise.
       2. **Unique Passwords.** The Credit Union requires unique passwords for members and users to minimize the risk of account takeover.
       3. **Password Strength.** The Credit Union maintains requirements for password strength such as password length, defined character combinations, and the use of passphrases.
       4. **Prohibited Password Lists.** The Credit Union monitors passwords to discourage passwords associated with prior account or data breaches, weak passwords and/or common passwords.
    2. **Access and Transaction Controls.** The Credit Union will utilize the following access and transaction controls.
       1. **Account Maintenance Controls.** Enhanced authentication controls are applied for account maintenance activities performed or requested by members or users.
       2. **Transaction Value, Frequency and Timing Controls.** Transaction controls such as transaction value limits, restrictions on devices for adding payment recipients, limits on the number of transactions allowed per day and allowable payment windows are applied for certain account and digital banking services.
       3. **Limit on Log-in Attempts.**The number of log-in submissions over a set timeframe are applied for correct and incorrect log-in attempts from the same user or from different users from the same IP address.
       4. **Incorrect Log-in Attempts.** Members and users are locked out of accounts after a certain number of log-in attempts. Passwords are reset only after requiring strong authentication.
       5. **Application Timeouts.** Members and users are re-authenticated after a period of inactivity within a service or system.
       6. **Automatic Suspension or De-provisioning of User Credentials.** System controls are in place to de-provision or suspend access credentials after a certain period of account inactivity.
       7. **Revocation of Access.** Fraud detection and controls are in place to conduct additional review of certain transactions to report suspicious activity, including the right to revoke access to services such as (but limited to) P2P or remote deposit capture (RDC).
       8. **Notification to Security Administrators of Change in User Status.** System administrators are informed in a timely manner of changes to user status.
    3. **Member Controls.**
       1. **Transaction Blocks.** Debit blocks, positive pay, and other techniques may be provided to business members to monitor and control transactions on their accounts.
       2. **Transaction Alerts.** The Credit Union may also use automated alerts, which are sent to members based on transaction size or risk parameters established by members or the Credit Unions.
       3. **Dual Control Transactions.** Controls can be made are available to business members to require more than one employee to authorize and approve certain transactions.
    4. **Monitoring Controls.** The Credit Union may utilize different monitoring processes, which may include:
       1. Transaction and Audit Logs.
       2. Fraud and Anomaly Detection Monitoring.
       3. Suspicious Behavior Monitoring.
       4. Fraud Response Policies.
       5. Monitoring and Reporting of Unauthorized Access by Third Parties.
    5. **User Access Controls.**
       1. **Approval Policies.** The Credit Union will have processes in place to establish approval and documentation standards for defining users’ authority to access the Credit Union’s systems.
       2. **Privilege Access Provisioning.** The Credit Union limits access to those information systems and resources related to the user’s job function or role.
       3. **Single sign-on.** Single sign-on capability is established for users to allow access to multiple internal information systems with a single authentication solution. Risk can be mitigated by reducing the number of passwords and credentials employees would have to manage and allow the application of strong authentication and risk monitoring to the single sign-on process.
       4. **User Communication and Training.** Credit Union users periodically receive authentication security awareness training.
    6. **Privileged User Controls.**
       1. **Change Defaults.** Default passwords and other credentials for privileged users or system, service, or administrative are changed or disabled.
       2. **Dedicated Devices or Accounts.** Privileged users have dedicated devices or account for all privileged or administrative activities. The dedicated devices cannot access the Internet.
       3. **Log and Alert.** Systems are configured to log and alert when a privileged user is added or removed and when unsuccessful logins or other anomalous behavior occurs.
       4. **Log Access**. Privileged user access is limited and defined between log-related privileges and other privileges. The logs of privileged user activity cannot be modified or deleted by the privileged user.
       5. **Periodic Review or Privileged User Activity.** Staff independent of the privileged user’s organization or business unit is alerted of, and periodically reviews, privileged user activity for anomalous behavior.
       6. **Dual Controls for Certain Critical Systems or Administrative Changes.** More than one privileged user at the Credit Union must approve access to certain critical systems or certain requests for administrative changes.
       7. **Enhanced Authentication for System and Software Updates.** Privileged users are reauthenticated with MFA prior to making system configuration changes, uploading or updating software or firmware, or executing significant system processes.
    7. **System and Network Design and Architecture Controls.**
       1. **Endpoint/Device Authentication**. Controls are in place to ensure only authorized devices can connect to the Credit Union’s information systems, networks, or services.
       2. **Device Blocking or Network Indicators.** Connections to the Credit Union’s systems or servers are blocked based on devices, networks, or IP addresses known or suspected to be associated with fraudulent or malicious activities.
       3. **Network Segmentation**. Networks, systems, services, and data are physically and logically segmented based on the Credit Union’s asset classification and risk assessment.
       4. **Remove Access Software Controls.** Remote access software is disabled if not being used. If remote access software is used, controls to mitigate threats can include placing a firewall in front of systems that use remove access software, having remove users connect with a virtual private network (VPN) or other secure channel, and implementing strong passwords with MFA.
       5. **Configure and Update Security Devices and Software.** Network security devices and software are securely configured. Software and firmware are updated to address vulnerabilities.
       6. **Limit Access to Certain Automated Command Features.** Only authorized users and accounts have access to configuration management frameworks that utilize command-line shells. User access to these features is logged.
       7. **Transport Layer Security**. Transport Layer Security (TLS) protocols that utilize encryption and authentication to create private, secure channels between machines are implemented. TLS protocols are periodically updated to address vulnerabilities and implement additional security.
       8. **Digital Certifications.** An inventory of machines that utilize digital certificates is maintained, and digital certificates and underlying protocols are continually updated to address emerging threats.
       9. **Device Credentials.** Controls are in place to preserve the authenticity of machine credentials in the form of digital keys and certificates, and to protect these credentials from compromise while in transit.
    8. **Email System Controls.**
       1. **Service Provider Recommended Configuration.** Email service vendor-recommended controls are implemented. Systems are monitored for unauthorized configuration changes.
       2. **Patch Management.** Email systems are updated and patched periodically, and the email system vendor is monitored for email system end-of-life.
       3. **Layered Security and MFA Consideration.** Layered security controls, to include the use of MFA or equivalent techniques are applied for the mail user population.
       4. **Monitoring.** Email systems are monitored to detect suspicious activity.
       5. **Anti-Phishing Controls.** Anti-phishing controls are applied to identify and block malicious emails and attachments. Specific controls may include:  
          1. Watermarks being in place to detect unauthorized emails;
          2. Enabling domain-based Message Authentication Reporting and Conformance policy and verification are enabled;
          3. Disabling macro scripts transmitted via email; and
          4. Blocking malicious email attachments and moving them to a segregated environment.
       6. **External Email Alerts.** External email messages are labeled with a prominent notice or banner to alert the receiver that the email message comes from outside the Credit Union.
       7. **User Education.** Users are educated on common email compromise tactics and techniques and offered ways to avoid or mitigate attacks.
       8. **Testing and Training Users.** Social engineering campaigns are administered to test users’ comprehension of and adherence to security policies. User training techniques are adjusted based on test results.
    9. **Internet Browser Controls.**
       1. **Current Updated Browsers.** Vendor-supported and management-approved Internet browsers are installed on systems and updated to the most current version in a timely manner.
       2. **Blocks on Certain Browser Features.** Internet browser pop-ups and redirects are blocked to protect against malware. Browser plug-ins and add-on applications are evaluated, with unnecessary plug-ins/applications disabled or removed.
       3. **Blocking of Certain Scripting Languages.** Scripting languages that are run in Internet browsers are evaluated and allowed or blocked. Cross-Site Scripting is an example where the attacker uses a scripting language to execute malware within a victim’s browser.
       4. **Limit User Access.** Domains inconsistent with the Credit Union’s risk profile and polices are blocked.
       5. **Domain Filtering.** Domain Name System filtering services are implemented to prevent access to known malicious domains. Credit Unions will consider the use of a reputation service or similar technology for remaining domains.
    10. **Internal Audit System.** The Credit Union will have an internal audit system that is appropriate to its size and the complexity of activities. It will provide for the following:
        1. Adequate monitoring of the system of internal controls through an internal audit function or a system of independent reviews of key internal controls.
        2. Independence and objectivity.
        3. Qualified person.
        4. Adequate testing and review of information systems.
        5. Adequate documentation of tests and findings and any corrective actions.
        6. Verification and review of management actions to address material weaknesses.
        7. Review by the institution's audit committee or board of directors of the effectiveness of the internal audit systems.

**Record Retention.** The Credit Union may retain electronic copies of all disclosures required to be retained. An accurate electronic copy will satisfy the requirements that the "original" disclosure or other record be retained, provided the electronic disclosure or other record is accessible by all persons legally entitled to access, for the period of time required by applicable law, "in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise. The Credit Union will follow their record retention policies for applicable timeframes.