MUTUAL SECURITY CREDIT UNION

Security Policy Statement

Protecting your financial information is one of our highest priorities. Our credit union maintains a comprehensive security program designed to safeguard member data, ensure system integrity, and support a secure digital banking experience. While we do not disclose specific technologies for security reasons, the following summarizes our approach.

Information & Cybersecurity Program

We follow industry-recognized standards, including NIST and FFIEC guidance, to protect the confidentiality, integrity, and availability of member information. Our systems are monitored for suspicious activity, access is restricted to authorized personnel using least-privilege principles, and sensitive data is encrypted in transit and at rest. Regular risk assessments help us identify and address emerging threats.

Vulnerability Management & Testing

We conduct continuous vulnerability scanning on internal and external systems and use independent third-party firms for routine penetration testing. Findings are reviewed, prioritized, and remediated promptly. Security updates and patches are applied as part of our structured patch-management process.

Vendor & Third-Party Oversight

We maintain a formal Vendor Management Program that evaluates the security posture of all service providers. Vendors undergo risk-based due diligence, including review of independent audits and SOC reports, and must meet contractual requirements for data protection, regulatory compliance, and incident notification. Their performance and controls are monitored throughout the relationship.

Digital Banking & E-Banking Security

Our e-banking platform uses layered authentication, fraud monitoring, and regular security testing to protect your accounts. Controls are in place to prevent unauthorized access and account-takeover attempts. We also encourage members to support their own digital safety by using strong passwords, enabling multifactor authentication, and reporting suspicious activity.

Commitment to Continuous Improvement

Cybersecurity threats evolve constantly, and we continuously enhance our controls, processes, and employee training to stay aligned with industry best practices and regulatory expectations. Our commitment is to safeguard your information and maintain your trust in every interaction.

If you would like more information about our security practices, please contact us. We are always happy to answer questions and provide additional guidance.

Chris Horvath
Director, Information Technology