

Statement on Members United Information Security Program July 1, 2009

Members United recognizes that members and business partners have an interest in knowing that Members United and its subsidiaries' information systems are appropriately secure and that member information is kept confidential. This statement is intended to provide visibility to Members United's approach to information security, as well as provide assurance that Members United and its subsidiaries have addressed security related issues appropriately. This document may be distributed to members and other interested parties upon request.

Members United and its subsidiaries have and maintain a comprehensive information security program and associated policies and processes. The security approach consists of the following:

Guidance and Oversight

- A comprehensive program description documents the organization's objectives, strategies, and tactics for ensuring that Members United and its subsidiaries have an appropriate information security environment.
- A Security Policy, approved by the Board of Directors, provides strategic, tactical, and oversight guidance.
- Reports recapping activity, incidents, and violations provide senior management with visibility required to manage the program.
- An annual examination by the NCUA ensures that Members United meets the regulatory agency's requirements.
- An annual program review ensures that the objectives, strategies, and tactics are current and appropriate for Members United, its subsidiaries and its members.

Validation

- Monthly managed external vulnerability assessments are conducted by a third party, ensuring that potential vulnerabilities are detected and addressed in a timely manner. Findings of these exams are reported directly to the Supervisory Committee and Internal Audit.
- Quarterly managed internal vulnerability assessments are conducted by a third party, ensuring that potential vulnerabilities are detected and addressed in a timely manner. Findings of these exams are reported directly to the Supervisory Committee and Internal Audit.

Security Architecture

- Members United and its subsidiaries employ a secure electronic product delivery channel. These systems allow members to conduct transactions in a secure manner via the Internet by utilizing the industry standard security certification approach (Verisign certificate with 128-bit SSL encryption). All transactions are logged and monitored. In addition, Internet facing applications employ industry best practices such as complex passwords, strong password length requirements, frequency of password changes, and dual controls on system administration functions within the application.
- An advanced firewall solution. Members United and its subsidiaries utilize a premier clustered firewall solution that ensures information is well protected, while also providing a highly available infrastructure for production use.
- A robust intrusion detection system. A highly advanced intrusion detection and prevention system is constantly monitoring data and systems for the latest security threats. The system provides for immediate response if a security incident ever occurs.
- Multiple anti-virus scanning engines. Anti-virus scanners are updated every hour to ensure that even the newest viruses are detected and quarantined. Multiple scanners from different vendors are used to ensure that a complete anti-virus solution is installed and operational.
- Automated Windows patch management. The security management program ensures that all servers and workstations receive the latest patches after they are announced and tested.
- Automated security monitoring and alerting. Systems send out alerts to security staff whenever a suspicious event occurs. The security staff also monitors external security services on an ongoing basis.
- Employee security awareness training. Members United and its subsidiaries invest in regular security awareness training for all employees. This training ensures that all employees are alert to security threats, aware of their responsibilities, and know what action to take if they encounter a security incident.

Staff

- Members United's security program is led by a Certified Information Systems Security Professional (CISSP) who reports to the Vice President, Operational Integrity.

The Board of Directors, Supervisory Committee, management and staff are committed to maintaining an industry-leading information security program that protects Members United, its subsidiaries and its members.