MGIC INFORMATION RISK MANAGEMENT PROGRAM

Program Objective

MGIC Investment Corporation and its subsidiary corporations (collectively, "MGIC") maintain a comprehensive information security program (the "program") to protect the security, confidentiality and integrity of consumer information and other information that is confidential and proprietary to MGIC, its employees, customers, suppliers, vendors and contractors (collectively, "confidential information"). The program is designed to:

- ensure the security and confidentiality of confidential information;
- protect against any anticipated threats or hazards to the security or integrity of confidential information; and
- protect against unauthorized access to or use of confidential information that could result in substantial harm or inconvenience to MGIC, its customers and consumers.

The program includes risk assessment activities, policies and procedures to manage and control the security of confidential information, and mechanisms to test the effectiveness of the controls, as summarized below.

Risk Assessment Activities

MGIC regularly identifies and assesses risks that may threaten the security, confidentiality and integrity of confidential information. These risks include, but are not limited to:

- unauthorized access to or use of confidential information by employees and third parties;
- unauthorized alteration of confidential information;
- loss or theft of confidential information.

Risk assessment activities also provide for the classification of information and security recommendations for communication of information, based on its sensitivity and importance, as confidential, for internal use or for general use, taking into consideration factors such as:

- regulatory and legal requirements, including provisions of the Gramm-Leach-Bliley Act, the Interagency Guidelines Establishing Information Security Standards, the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, NCUA regulations, Section 404 of the Sarbanes-Oxley Act and related regulations;
- financial significance;
- competitive advantage;
- privacy considerations of individuals, customers, vendors and employees; and
- public relations.

Security Controls

MGIC has policies, procedures, information systems and other arrangements in place to control the identified risks and achieve the overall objectives of the program. Information security controls are documented in handbooks, policy/procedural manuals, electronic databases and bulletin boards throughout MGIC and cover multiple aspects, including:

Storage and Disposal of Records

- Documents containing confidential information are kept in file cabinets that are locked when not in use.
- "Confidential — For Internal Use Only" labels are used on certain confidential documents.
- MGIC's records center is physically secured and access is limited to authorized personnel.
- A records retention policy specifies the retention periods and destruction requirements for records (including electronic records).
- Documents are accounted for and tracked until ultimate destruction.
- A shredding policy is in effect requiring all documents containing confidential information to be shredded.
- Computer media is physically secured in MGIC's data center and at an off-site disaster recovery facility.
- Corporate data is backed up for recovery purposes. Backup tapes are physically secured in an off-site location and at a secure third-party storage facility.

Physical Security of Facilities

- Entryways to MGIC's home office facilities are limited and guarded by security personnel.
- Employees are required to wear identification badges. Visitors are required to sign in at the security desk, show identification and obtain a visitor's identification badge.
- Building access is restricted to employees with proper identification and authorization.
- Security systems are in place to prevent forced entry during non-business hours. Security cameras are used to monitor certain areas of MGIC facilities.
- Security detection systems are in place to monitor MGIC facilities in the event of fire or other emergencies.
- All computer equipment and PBX equipment is maintained within secured areas of the MGIC facilities.
- MGIC's information technology ("IT") center is physically secured and is equipped with firewalls, raised floors, and environmental monitoring, fire suppressant and emergency power systems.

Data Security Practices, Policies and Standards

- Proper segregation of duties exists within MGIC's IT department, including the functions of computer operations, system software maintenance, network administration, database administration, application programming, program change management, data entry and data security.
- Written security policies and procedures are provided to employees.
- The IT security group independently administers user ID and password permissions.
- The IT security group administers security awareness programs and issues security awareness reminders to employees.
- MGIC has a defined business resumption planning process and routinely conducts business continuity testing.
- MGIC application source code is maintained in version control repositories.
- Moves to production require a manager's approval.
- Testing is performed in a QA or test environment before new systems or system enhancements are moved into production.
- Platform updates and patches are identified, reviewed and installed, as appropriate.

Access Controls

- Internal and external access to all computer files and systems is controlled by user IDs and passwords.
- User access capabilities are configured with least privilege so that users have only the minimum access rights and privileges needed to perform their job functions. Access authorization requires management approval.
- A security software tool is used to control access to data on the enterprise server.
- The Human Resources department notifies the IT security group of all job changes, and access privileges are adjusted accordingly.
- A weekly reconciliation process is performed to ensure revoked accounts are removed on a timely basis.
- Employee passwords must include a prescribed minimum number of characters and must be changed regularly.
- A user's account is locked after 3 unsuccessful logon attempts.

Security Architecture and Hardware/Software Filtering

- MGIC has a Demilitarized Zone architecture which includes separation of internal and external networks and separation of web servers from application and database servers.
- Security alert management software is installed to detect security breaches, such as port scans, denial of service attacks and other external penetration attempts.
- Data and network integrity software is installed on MGIC's web servers.
- MGIC has anti-virus policies and procedures. Anti-virus scanning is performed at desktops and servers.
- E-mails containing certain file types that may contain viruses are blocked.
- Procedures are in place to respond to a network intrusion or virus attack.

Security Monitoring

- MGIC has been certified by Cybertrust Corporation.
- MGIC periodically contracts with independent third parties to perform vulnerability assessments and/or penetration tests of its networks and uses QualysGuard vulnerability scanner.
- MGIC's Internal Audit department (with the assistance of independent auditors) performs periodic security audits.
- Failed logon attempts and certain other security-related events are logged and reviewed.
- Password cracking software is run regularly to identify weak passwords.
- All network devices are monitored for performance and failure notifications are automatically sent to appropriate support personnel.
- Unauthorized access to or use of confidential information will be reported promptly to the appropriate customer.

Exchange of Confidential Information

- MGIC maintains a Secure File Transfer System for delivery of confidential information electronically via the internet in encrypted format.
- MGIC encourages customers and other third parties to encrypt confidential information transmitted electronically over the internet to MGIC by using the Secure File Transfer System.
- Practices are in place to verify the identity of callers (*i.e.,* appropriate lender or borrower) before confidential information is disclosed over the phone.
- Document routing software is used to deliver faxes to the appropriate destination.
- Data received electronically from customers is archived in its original format.

Confidentiality Agreements and Policies

- MGIC's privacy policy is contained on its web sites.
- MGIC maintains a Code of Business Conduct (the "Code") and employee handbook which include requirements for employees to protect the confidentiality of information received from and prepared for customers, consumers, vendors, suppliers, contractors, as well as MGIC's proprietary information. Employees must acknowledge the handbook provisions and periodically are required to certify that they have complied with the Code.
- Employees must sign an agreement that includes provisions restricting the use and disclosure of confidential information consistent with MGIC's policies.
- Criminal background checks are performed on newly hired employees.
- Vendors and other third parties who handle or have access to confidential information are subject to a security risk assessment and monitoring by MGIC and must enter into confidentiality agreements restricting the use and disclosure of such information to the purposes for which it is provided.

Program Administration

MGIC has an ongoing security awareness program to train employees regarding certain aspects of the information security program. The security awareness program includes new hire orientation, a security awareness handbook, periodic newsletter articles and e-mail announcements, employee surveys and contests, and training programs.

MGIC employees are instructed to report unauthorized or fraudulent attempts to obtain confidential information to the IT security group or MGIC's General Counsel. Where appropriate, incidents are referred to the appropriate regulatory and law enforcement agencies.

MGIC monitors, evaluates and adjusts, as appropriate, the information security program in light of relevant changes in business arrangements, technology, the sensitivity of confidential information, and internal or external threats to the security, confidentiality and integrity of confidential information.

MGIC performs periodic tests of the security controls to confirm that they are reducing risks and achieving the objectives of the information security program. Tests are conducted, where appropriate, by independent third parties or staff independent of those who develop or maintain the program/controls.