MARYLAND GLOBAL INITIATIVES CORPORATION
AN AFFILIATE OF THE UNIVERSITY OF MARYLAND, BALTIMORE

MGIC Policies and Procedures – Information Technology

Board Approved September 2023

Contents

7 - INFORMATION TECHNOLOGY

Definitions

Capital asset: see *Equipment*
Confidential information: Non-public, proprietary, or sensitive information including processes, formulas, data, know-how, inventions, improvements, techniques, plans, strategies, forecasts, proposals, personal information, and health information (see **Sensitive data**).
Country director (CD): The lead manager of a country office. The CD position directly supervises senior management positions in an MGIC country office and reports to the designee of the MGIC President. In non-traditional MGIC structures (such as MGIC USA, small teams or embedded positions), the CD role is referred to as a Country Representative (CR).
Country office (CO): An MGIC branch office, corporate affiliate, field office, or program office established in a physical facility outside the United States, to conduct business in a country where UMB's research, education, and related programs are implemented.
Country office (CO) personnel: All employees working in an MGIC country office, whether on UMB payroll, MGIC payroll, or another UMB-authorized payroll, including staff, UMB faculty with CO positions, fellows, students, interns, and volunteers.
Critical business data: Essential information required for the country office to function smoothly and prevent operational and programmatic disruptions, as well as sensitive information that must be safeguarded, including all *sensitive data*.
Designated non-capital asset (DNCA): An asset valued at less than US$500 that merits additional stewardship because such assets are desirable, easily converted to personal use, and susceptible to theft.
Device: Any desktop computer, laptop, tablet, mobile phone, or other physical hardware or equipment that provides computing functions within a computing system.
Country representative (CR): The senior-most representative of MGIC based in a country or representing MGIC in that country remotely, as designated by the MGIC President. In countries where MGIC operates a full country office, the senior-most MGIC representative is the Country director (CD). In countries where MGIC is not legally registered, does not have a full country office, or has another operating model (e.g. embedded within a partner institution), the MGIC Country Representative role may be held by the AVP of International Operations, an MGIC consultant or employee hired through the MGIC under an Employer of Record (EOR) contract, or another position as designated by the MGIC President.
Director of finance and administration (DFA): The lead manager of the MGIC financial and accounting functions for an office or team, who may oversee and direct the office's administrative/operational functions as well, and whose title might be Director of Finance and Administration, Head of Finance, International Finance & Procurement Manager, or some other title indicating their leadership role in MGIC financial management.
Employer of Record (EOR): A professional employment firm that takes on the role of managing payroll, benefits, and risk management for a company's employees on its behalf, relieving the company of these responsibilities. **Duty station:** An employee's assigned place of work as documented in their employment agreement or as amended in writing.
Equipment: Any item that (1) is durable with an expected service life of one or more years; (2) has an acquisition cost (purchase value) of $5,000 or more; and (3) is complete in itself and does not lose its identity or become a component part of another article when put into use.
Exploitation: Constitutes the abuse of a person where some form of remuneration is involved or whereby the perpetrators benefit in some manner. Represents a form of coercion and violence that is detrimental to the person's physical or mental health, development, education, or well-being.
Field Operations Manual (FOM): The country office's compilation of country-specific procedures for administrative and operational functions including but not limited to, legal affairs, facilities

management, insurance, property management, travel, fleet management, communications, confidentiality and data security, and record retention.
Field sub-office: Any office besides the country office's main office, typically located in a region of the country where MGIC has significant program operations, sometimes referred to as a regional office.
Harassment: Unwelcome conduct that is based on gender, marital status, pregnancy, race, ethnicity, tribe, color, religion, age, ancestry, national origin, sex, gender identity or expression, sexual orientation, or physical or mental disability, and that interferes with an individual's work performance or creates an intimidating, hostile, humiliating, demeaning, or sexually offensive working environment.
Human resources (HR) lead: The lead specialist with responsibilities related to MGIC human resources management, which could in some cases be the DFA or a project manager.
Intellectual property: A work or invention that is a product of the human intellect, to which one has ownership rights, copyrights, patents, patent applications, trade secrecy rights, trademarks, service marks, trade names, know-how, data, technology, or other rights.
IT resources: Resources related to IT operations, including computerized information, computing facilities, computer networks, hardware, software, systems, programs, and devices.
IT support lead: The lead specialist within a country office, or contracted as a service provider, with responsibilities related to IT systems, policies, procedures, and support.
MDM: Mobile Device Management, a tool used to apply organizational policies to, and manage, mobile devices (laptops, phones)
MGIC Office: A unit, team, or designated representative within MGIC who maintain a physical presence in a country (such as a Country Office), or operate remotely when there is no physical office in country (such as MGIC USA).
MGIC Office Leadership: The CD or designated Country Representative, director of finance and administration (DFA), and other senior managers whom the CD supervises and who are collectively accountable for office or team management, operations, and programs.
MGIC Personnel: All employees working in an MGIC position, whether on UMB payroll, MGIC payroll, or another UMB-authorized payroll, including staff, UMB faculty with MGIC positions, fellows, students, interns, and other temporary workers, and individuals formally seconded to MGIC under professional services agreements with MGIC.
MGIC USA: The operational structure of MGIC procedures and services provided to UMB Funding Units outside of an MGIC country office. MGIC USA's services include procurement, financial transactions, recruitment and employment, and facilitation of legal services in countries where MGIC is not registered or operational. MGIC USA is an MGIC Office and is subject to the MGIC policies and procedures.
Non-capital asset (NCA): Physical assets with an acquisition cost of US$500 or more, but less than US$5,000 per unit, and with a useful life of greater than one year.
Partner: A civil society organization (CSO), including local and international non-governmental organizations (NGOs), or a governmental (state) actor with which the country office has an alliance that supports UMB research and programmatic aims.
Personally identifiable information (PII): Data that could potentially identify a specific individual, such as full name, date of birth, government ID number, and passport number.
Procurement lead: The staff member designated to manage the country office's procurement function and ensure MGIC procurement standards are met.
Project: A distinct programmatic or research activity funded by a sponsor or by UMB/MGIC lightly restricted funds that has specified expected results, timeframe, and budget.
Property lead: The staff member designated to oversee CO property management and ensure MGIC property management standards and procedures are met.
Property management: Management of equipment, which is also referred to as *personal property* and includes IT systems and excludes land and other *real property*.

Regional IT support lead: The person in MGIC who provides IT-related guidance and support to country offices and promotes compliance as relates to IT systems, policies, and procedures.
Report: A report in these procedures is a report of a known or reasonably suspected, serious violation of law or policy.
Requestor: The individual whose department or team requires procurement of goods or services and who initiates the procurement through submission of a purchase requisition.
Sensitive data: Any personal, confidential, and legally protected information, including personally identifiable information (PII) associated with patient and study participant data.
Sponsor: A funder of a sponsored project; an awarding agency or institutional donor; a funding source; an institution that funds activity that is separately budgeted and accounted for according to the terms the institution lays out in an award agreement.
UMB/MGIC IT resources: IT resources owned, leased, or used by UMB, MGIC, and the country office, including computerized information, computing facilities, computer networks, hardware, software, systems, programs, and devices.
UMB department administrator: The person in a UMB Funding Unit who typically serves as chief financial and operating officer for the UMB unit and is responsible for the planning and execution of compliance, financial, personnel, and other administrative affairs for the department's programs. When multiple UMB Funding Units engage the same MGIC office, the MGIC President designates one individual to serve as the UMB department administrator for that MGIC office's approvals and oversight purposes.
UMB department operations lead: The person in a UMB Funding Unit with responsibilities related to program operations, human resources management, and administration. When multiple UMB Funding Units engage the same MGIC office, the MGIC President designates one individual to serve as the UMB department operations lead for that MGIC office's approvals and oversight purposes.
UMB department program lead: The person in a UMB Funding Unit who directs the program. This role is often performed by the Principal Investigator or equivalent program director named in UMB's award agreement. This role may directly supervise MGIC technical leads in collaboration with the CD/CR.**UMB Funding Unit:** A UMB school, department, institute, center, or other structure that manages international program awards and engages and funds MGIC to implement those programs.
Users: CO personnel, students, faculty visitors and guests of MGIC who use UMB/MGIC IT resources in the course of CO employment, educational activities, or other purposes related to their MGIC affiliation; also, any other persons authorized to use UMB/MGIC IT resources; any person who receives a password from UMB/MGIC or who uses an email address that ends in "mgic.umaryland.edu."

7-1 Overview of the IT Policies and Procedures

Policy statement

Two categories of individuals may access and use MGIC information technology (IT) resources:

- MGIC personnel: MGIC employees become authorized users when they receive a fully executed employee contract from MGIC or through an MGIC Employer of Record (EOR) service, login credentials, and a UMB/MGIC email address.
- Other users authorized by the MGIC President or designee. No non-MGIC personnel may access or use MGIC IT resources without this authorization in writing.

About "Designees"
MGIC Policies and Procedures assign authorities and responsibilities to certain leadership positions. However, directors and managers may designate or delegate those authorities and responsibilities to colleagues, unless otherwise indicated and in accordance with 5-4 Signature Authorities and with appropriate internal controls in place.

All authorized users must follow MGIC IT Policies and Procedures. Use of UMB/MGIC IT resources is a privilege and subject to compliance with these Policies and Procedures.

Organization of the IT Policies and Procedures

This section of the Maryland Global Initiatives Corporation (MGIC) Policies and Procedures directs and guides all aspects of information technology. It covers everything from procurement of hardware and software using MGIC standards, through authorizing use and protecting assets, to equipment disposition. It specifies the role of the IT support lead and relationship to the regional IT support lead, and it provides MGIC's Acceptable Use Policy. Data and systems security, including protection of sensitive data, is highlighted in one portion as well as throughout the Policies and Procedures.

These IT policies and procedures are complementary to 2-Ethics and Conduct and 3-Administation and Operations, which provide confidentiality, asset management, and data retention guidance for MGIC personnel, as well as 4-Human Resources, 5-Financial Affairs, and 8-Safety and Security, which include information on procuring and protecting IT equipment. They align with relevant MGIC and UMB policies and reflect applicable laws and regulations of the United States government (USG).

MGIC office IT duties

The country director (CD) or country representative (CR) is ultimately responsible for the establishment and maintenance of IT systems that enable the MGIC office to fulfill programmatic and research-related objectives. Further, the CD/CR ensures there is a designated employee or service provider, known as the IT support lead, to lead this function for a full country office or a different MGIC team structure. This person may report to the CD/CR, to the director of finance and administration (DFA), or to some other senior manager and is responsible for working closely with the regional IT support lead, the UMB IT department, as well as any service providers engaged by MGIC to support IT requirements.

While offices will have distinct IT structures and staffing, the duties of the IT support lead are consistent, and the core responsibilities are:

- Ensure IT systems and standards are consistent with UMB, MGIC, and sponsor policies and standards and local standards and regulations
- Ensure adherence to MGIC hardware and software standards
- Maintain and support an effective IT environment that enables productive working conditions for MGIC personnel to fulfill their duties
- Maintain an accurate and detailed inventory of IT equipment in conjunction with the MGIC property lead
- Protect and securely store IT equipment and ensure MGIC personnel understand their obligation to protect and secure equipment in their possession
- Establish, promote, and adhere to MGIC standards that ensure data and systems security
- Maintain a regular schedule for onsite and offsite back-up and secure storage of data and systems
- Ensure all IT-related service providers have appropriate agreements to support MGIC needs and are accountable for providing high-quality and timely service
- Ensure MGIC personnel understand acceptable use of UMB/MGIC IT resources, and monitor for compliance
- Assist in creating, supporting, and terminating IT accounts including access to corporate email and IT-related systems

- Maintain an up-to-date list of all authorized users of UMB/MGIC IT resources
- Lead IT-related orientation and training for MGIC personnel
- Support IT-related transfer or separation actions for departing personnel
- Conduct IT systems audits on at least an annual basis
- Engage the UMB IT department as a cooperative partner to MGIC (through MGIC's regional IT lead, the International Operations IT Manager, and others as appropriate)

User responsibilities

MGIC personnel are responsible for protecting and caring for any IT equipment assigned to them, including its contents and any peripheral devices or accessories associated with the equipment. The equipment must be used strictly for work-related purposes and not personal matters. See 7-3 Protection of IT Assets for details.

MGIC personnel are responsible for adhering to IT privacy and other security policies, and otherwise using UMB/MGIC IT resources in a manner consistent with the MGIC Code of Ethics and Professional Conduct (the Code, found in 2-Ethics and Conduct.) See 7-4 Data and Systems Security and 7-5 Acceptable Use for detailed responsibilities.

MGIC Regional and UMB IT support

MGIC offices should first turn to their IT support lead to address IT needs and provide technical support to personnel and, as appropriate, partner organizations. When support needs cannot be met locally or when UMB must provide specific IT help, the IT support lead should reach out to MGIC's regional IT support lead as the first point of contact.

Broadly speaking, the regional IT support lead is responsible for providing IT-related guidance and support and for promoting compliance as relates to IT systems, policies, and procedures. However, the regional IT support lead is also responsible for specific tasks that are critical to MGIC and UMB data security, such as:

- Establishing official UMB/MGIC accounts and access, including email addresses, for new employees
- Terminating accounts and access for separating employees
- Resetting email passwords
- Providing IT support for UMB systems

The regional IT support lead will refer issues to various points of UMB IT support, which may include creating help tickets in these systems, depending on the nature of the issue:

- UMB School of Medicine (SOM) IT Support (help@SOM.Umaryland.edu)
- UMB Center for Information Technical Services (CITS) IT Helpdesk (help@Umaryland.edu)

Checklist for CDs/CRs

A tool for managing policy implementation and conducting compliance monitoring

- ☐ Assign a designated employee or service provider to be the IT support lead
- ☐ Ensure the IT support lead/team closely follows core responsibilities

- Ensure MGIC personnel records are consistently and accurately updated to trigger termination of access to equipment, systems and networks, including UMB's Community System, for former employees, and ensure no unauthorized users are on MGIC's rolls.
- Educate MGIC personnel regarding their user responsibilities such as protecting IT equipment assigned to them and using equipment for strictly for work-related purposes
- Reach out to the regional IT support lead for guidance and support needs

Key references

- 2-2 MGIC Code of Ethics and Professional Conduct
- 2-Ethics and Conduct
- 3-Administration and Operations
- 4-Human Resources
- 5-Financial Affairs
- 5-4 Signature Authorities
- 7-3 Protection of IT Assets
- 7-4 Data and Systems Security
- 7-5 Acceptable Use
- 8-Safety and Security

7-2 Hardware and Software Standards

Policy statement

Standardization of MGIC IT assets that adhere to minimum requirements enable a more efficient IT environment and support system. MGIC personnel should review MGIC IT standards and update office-specific IT standards on at least an annual basis, consulting the regional IT support lead for guidance or when significant changes are considered.

MGIC teams implementing highly specialized program scopes may require a higher level of technology or unique software that facilitates carrying out specific tasks. MGIC personnel should provide a documented justification for any request to use hardware or software that is outside of the set standards. Any deviation from the standards requires IT support lead approval and, for procurements valued at or above US$5,000, the written approval of the CD and UMB department program lead.

Procurements of hardware, software, and IT support services should be made in coordination with the IT support lead and within budgetary requirements.

It is prohibited to have unlicensed software on MGIC IT assets.

MGIC personnel who use a personal IT device to complete MGIC-related activities are subject to MGIC IT requirements and must strictly observe policies and procedures to protect privacy and confidentiality (see 7-4 Data and Systems Security).

Hardware and software standards

The IT support lead, in coordination with a service provider if needed, maintains hardware specifications that standardize MGIC equipment and meet operational needs within the IT support lead's assigned office or team, as well as industry and MGIC standards. Furthermore, the IT support

lead maintains a list of approved software and documents any deviation as per Deviation from hardware and software standards below.

The MGIC office's hardware and software standards should be reviewed and updated on at least an annual basis. (See IT systems audits in 7-4 Data and Systems Security for details.) A sample of standards as of August 2023 include:

- Operating system: Current, industry-standard versions of Windows, Mac OS
- Office productivity: Microsoft365 Suite (available through UMB's license)
- UNIT4 Enterprise Resource Planning (ERP) for Finance and HR operations
- Vulnerability Management: Rapid7 InsightVM (available through UMB's license)
- Endpoint Privilege Management and Application Control: Cyberark EPM (available through UMB's license)
- Endpoint Configuration: Microsoft Endpoint Manager (InTune) (available through UMB's license)
- Laptops: Dell Latitude, Apple MacBook
- Desktop: Dell, Apple iMac
- Servers: Dell PowerEdge
- Firewall: FortiGate
- In-house storage: NetApp
- Cloud Storage: OneDrive, SharePoint, Microsoft Teams, Box
- AccessPoints: Ubiquiti Unifi
- Phones: Samsung
- Browser: Google Chrome, Internet Explorer, Microsoft Edge, Firefox 10, or Safari
- Email: Microsoft Outlook
- Calendar: Microsoft Outlook
- Antivirus: Microsoft Defender for Endpoint (available through UMB license)
- Video conferencing: Zoom, Microsoft Teams, Cisco Webex
- Secure file transfer: Microsoft Office 365, Secure File Transfer Protocol (SFTP)

All software must be officially licensed and registered by MGIC or UMB. Licenses are maintained for the full duration of use and securely stored in the MGIC office or with a contracted service provider. See 7-3 Protection of IT Assets.

Procurement of hardware and software

When MGIC offices purchase hardware or software, the process must adhere to MGIC's Procurement Policy (see 5-15 Procurement). New acquisitions should be immediately added to the office's Inventory Register, as per the guidance under Inventory management below.

Of special note is requirement to comply with U.S. export controls and sanctions law that restrict the export, transfer, and disclosure of certain technical and scientific data, software, and tangible items. In some cases, MGIC may be required to obtain an export license or other USG approval. Any questions or concerns relating to U.S. export controls and sanctions should be promptly referred to the UMB department administrator.

Further, MGIC offices implementing programs with USG funding from UMB must comply with Section 889 of the U.S. National Defense Authorization Act which restricts the purchase or use of any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

The UMB Funding Unit responsible for a USG award to which Section 899 complies may be able to seek a waiver from the sponsor. MGIC personnel requesting, procuring, and providing IT support for IT equipment, systems or services must coordinate with the UMB department administrator and UMB department program lead to confirm Section 889 applicability prior to any purchase of covered technology. MGIC personnel should promptly refer policy interpretation and compliance questions to the UMB Department of International Operations (IO) IT Manager.

Deviation from hardware and software standards

Requestors are responsible for following MGIC's hardware and software standards. If desiring to deviate from those standards, the requestor must seek prior approval using the following process:

1. The requestor presents a written rationale to the IT support lead.
2. The IT support lead consults with the regional IT support lead as appropriate and provides written approval.
3. If the value of the procurement is greater than or equal to US$5,000, the IT support lead seeks written approval from the CD and UMB department program lead.
4. The IT support lead provides the requestor and the DFA with the approval(s).

As part of the DFA's role in approving procurements, the DFA is responsible for monitoring compliance with this process.

Hardware and software maintenance

Hardware and software maintenance on IT assets must be carried out by an IT professional. Requests for maintenance should be first directed to the IT support lead to coordinate the repair or update. All software licenses should be documented and tracked as part of software inventory management. Should an MGIC office wish to establish a more detailed process, this should be made available to office personnel and the regional IT lea to ensure consistent use of procedures.

For support that leverages a service provider, see maintenance and support contracts in 7-3 Protection of IT Assets.

Hardware replacement cycle

MGIC offices and teams should establish a replacement cycle for computers and other hardware, taking into account as one factor the period of the manufacturer's hardware warranty. The replacement cycle defines the period after which a computer may be considered for replacement, allowing exceptions for equipment that can no longer be supported.

Using a strategic approach to replacement, the cycle should seek the optimal balance between the cost of replacing equipment and the benefits gained through enhanced employee and organizational performance. Establishment and management of the cycle should be coordinated between the IT support lead and procurement lead, to determine together when new equipment shall be purchased.

The decommissioning of IT equipment should be carried out by entities that can provide certification that intellectual and sensitive data stored on hard drives will be properly destroyed. Any proposal to decommission an IT server used by the country office shall be initiated by the IT support lead and authorized by the CD/CR. The proposal should present a comprehensive plan for server

replacement, for migration of services, and for how downtime will be minimized to an acceptable level. Servers shall be decommissioned once the hardware warranty period has elapsed.

Use of personal IT devices

While MGIC should minimize the need, on occasion personnel may use their own personal device to complete MGIC activities. As outlined in 7-4 Data and Systems Security and 2-2 MGIC Code of Ethics and Professional Conduct, MGIC files and documents must never be stored on personal IT devices.

If MGIC personnel use personal devices, such as a laptop or mobile phone, to access UMB/MGIC email or other systems, MGIC security requirements must be strictly followed – see 7-4 Data and Systems Security for details regarding passwords/PINs, antivirus programs, remote wiping, and more. MGIC personnel should be advised that use of their personal devices while connected to the local office network must also adhere to the 7-5 Acceptable Use Policy.

Checklist for CDs/CRs

- ☐ Maintain standards for hardware and software and update them on at least an annual basis
- ☐ Only use software that is officially licensed and registered by MGIC or UMB
- ☐ Ensure MGIC complies with applicable USG export controls, sanctions laws, and prohibitions against use of covered technology, through close coordination with UMB Funding Units implementing awards subject to these requirements.
- ☐ Enforce adherence to the standards and require written rationales for and approval of any deviation
- ☐ Establish a replacement cycle for computers and other hardware and ensure that intellectual and sensitive data is destroyed when IT equipment is decommissioned
- ☐ If allowing MGIC personnel to use personal devices to access UMB/MGIC email or other systems, ensure MGIC security and acceptable use requirements are followed

Key references

- Inventory Register
- 2-2 MGIC Code of Ethics and Professional Conduct
- 5-15 Procurement
- 7-3 Protection of IT Assets
- 7-4 Data and Systems Security
- 7-5 Acceptable Use Policy

7-3 Protection of IT Assets

Policy statement

Depending on the scale and operations of an MGIC office or team, IT service providers may be contracted to provide IT-related support and guidance.

MGIC offices must follow an inventory management system for IT assets that includes registration of new equipment and accessories, annual and periodic checks of all IT assets, and responsible disposition of equipment, in accordance with 3-7 Property Management.

MGIC offices must ensure the safety and security of all technology assets, maintaining restricted access to licenses and servers and other equipment. Employees are responsible for technology assets assigned to them, must immediately report any loss, damage, or theft, and must return them in good condition and working order.

Maintenance and support contracts

To ensure that effective IT infrastructure and systems are in place to support MGIC operational needs, the office may establish service-level agreements (SLAs) with reputable vendors for hardware, software, and network support. See on procurement and engagement of vendors. Agreements with service providers should be reviewed and renewed on at least an annual basis to ensure they are meeting the office's changing needs, they provide the appropriate levels of service, and they continue to offer value for money.

The IT support lead is the manager of all IT-related SLAs and should serve as the internal focal point for MGIC personnel before contacting service providers directly. Typically, external service providers are called upon only for complicated issues that MGIC has been unable to resolve in-house. It is recommended that MGIC offices have SLAs with specific vendors for specific IT services and maintain consistency and clarity about which vendor to engage for what types of IT support.

Inventory management of IT assets

MGIC should maintain an inventory management system that ensures adequate receiving and accounting for IT equipment, including periodic inventory checks. All device equipment and accessories, including software licenses, must be properly accounted for by the MGIC office property lead in the Inventory Register.

IT assets on the Inventory Register include **capital assets** with a value of US$5,000 or greater, **non-capital assets** with a value of US$500-US$4,999.99, and **designated non-capital assets** (DCNAs) which have a value less than US$500, but are desirable, easily converted to personal use, and susceptible to theft. Typically, DCNAs are not fixed to a permanent structure and can be easily removed or carried – such as laptops, tablets, smartphones, external hard drives, or audio/visual equipment – thus requiring additional stewardship. See 3-7 Property Management and 5-15 Procurement.

Storage and regulated access to IT assets

All original software disks, licenses, and rescue disks as well as IT assets not in regular use by MGIC personnel should be kept in a locked storage area in the office. Access should be strictly regulated.

If located within an MGIC office, all servers should be enclosed in a locked server cabinet, and kept in a secure, low-traffic area of the office that is monitored by closed-circuit television (CCTV) cameras and is temperature-controlled. If servers are located offsite with a vendor, then the service agreement should stipulate location in a secure, temperature-controlled area with regulated access.

To regulate access to individually used IT assets, supervisors should complete and sign a New Hire IT Equipment & Access Request Form for each new employee. Upon receipt of the form, the IT support lead provides the new employee with the specified IT equipment and access.

MGIC offices should specify responsibilities and processes for storage, access, issuance, and return of IT assets. A recommended approach to division of responsibilities and segregation of duties is as follows:

- The property lead (or designee) stores and controls access to IT assets.
- The property lead manages the inventory for those assets, while the IT support lead keeps a list for purposes of efficient assignment of assets.
- The property lead issues IT assets to MGIC personnel at the behest of the IT support lead.
- The IT support lead sets up and configures equipment for users.

This arrangement requires the IT support lead and property lead to collaborate closely in executing their duties.

Use and care of IT assets

MGIC requires that personnel take reasonable precautions in protecting and caring for any IT equipment assigned by MGIC, including its contents and any peripheral devices or accessories associated with the equipment. Equipment should only be assigned to an individual who is an employee of UMB or MGIC (including MGIC employees hired under an MGIC Employer of Record service). Upon receiving certain equipment, such as a laptop, the IT support lead has the recipient sign an Employee Equipment Acknowledgement Form (EEAF) and shares a copy with the Human Resources (HR) lead to place in the employee's personnel file.

All MGIC-provided IT equipment shall be used strictly for work-related purposes and not personal matters. See 4-10 Working Conditions.

MGIC mandates that personnel in possession of IT assets immediately report any loss, damage, or theft to their supervisor and the IT support lead. In cases of suspected theft, the police must be notified by the person, or their supervisor and a copy of the police report requested. Moreover, the person whose device was stolen must complete an Incident Report Form and attach the police report and/or other relevant documentation. See Reporting property loss, damage, or theft in 3-7 Property Management.

Any damage caused to MGIC property due to negligence is the employee's responsibility and MGIC may require the employee to reimburse the organization for the fair market value of the equipment.

MGIC personnel are responsible for promptly returning IT equipment and accessories in satisfactory condition after it is no longer needed or when the individual transfers or separates from the organization. See 4-20 Separation from Employment.

MGIC has the right to visually inspect equipment at any time. Inspection may include access to data on the equipment and analysis of the use of the equipment.

Checklist for CDs/CRs

- ☐ Ensure the office inventory management system for IT assets includes registration, periodic checks, and responsible disposition
- ☐ Review and renew agreements with service providers on at least an annual basis

- ☐ Maintain a locked storage area for IT assets, with temperature control and regulated access for servers and individually assigned equipment
- ☐ Foster a work environment where MGIC personnel take reasonable precautions and protections in caring for IT equipment, immediately report loss or damage, and return equipment promptly

Key references

- Employee Equipment Acknowledgement Form (EEAF)
- Incident Report Form
- Inventory Register
- New Hire IT Equipment & Access Request Form
- 3-7 Property Management
- 4-10 Working Conditions
- 4-20 Separation of Employment
- 5-Financial Affairs
- 5-15 Procurement

7-4 Data and Systems Security

Policy statement

Due to the nature of UMB's programs and research, MGIC and country offices possess sensitive data, defined as any personal, confidential, and legally protected information, including personally identifiable information (PII), and manage information systems that must be proactively protected. UMB and MGIC recognize and respect the need for privacy of sensitive information and aim to establish and maintain IT systems and processes that protect this information and comply with UMB, MGIC, and sponsor requirements and local laws and regulations.

All MGIC personnel are required to use caution when retaining or transferring data, in all formats or media, that is considered confidential or sensitive as well as when accessing information systems that contain this data.

MGIC offices must protect MGIC and UMB data and systems against spam, phishing, and hacking attempts, including through efforts to raise awareness among MGIC personnel on common risks and protective measures. All MGIC offices and personnel should install and maintain UMB's license for Microsoft Defender for Endpoint virus protection program on all MGIC devices and servers. All MGIC devices and Wi-Fi access points must require a username and password to log on, and passwords must be changed every three months. Visitors shall be provided with guest Wi-Fi that is separate from the Wi-Fi network used by MGIC personnel. Furthermore, MGIC offices must endeavor to safeguard the digital workspace and keep it free from exploitation and harassment.

MGIC offices must maintain a regular schedule and secure storage of data and systems back-ups, with the specific back-up processes and responsible parties identified.

Different types of MGIC records have different record retention requirements. Please refer to the specific policy under each department for the specific retention period.

Any data storage device that contains sensitive data requires special handling when disposing of the IT asset to ensure the data has been made unrecoverable.

Before the commencement of any data-handling process for any project, the MGIC office must develop a Project Data Management Plan outlining all information security processes and safeguarding measures. This document must be approved by the IT support lead, in consultation with the regional IT support lead, and by the CD/CR.

Protecting privacy and confidentiality

Maintaining security of sensitive information is one of UMB and MGIC's most important responsibilities, as described in 3-11 Confidentiality and Data Security. MGIC IT personnel and service providers are accountable for safeguarding sensitive information and strive to do so by:

- Limiting access to sensitive information to individuals on a "need to know" or "least-privilege" basis and for the sole purpose of carrying out MGIC activities
- Emphasizing the importance of confidentiality and privacy through a combination of training, operating procedures that fulfill the requirements of this Policy, and systematically enforced IT security
- Strictly adhering to relevant local laws and regulations to protect sensitive information
- Continually updating and testing MGIC IT resources to improve protection of sensitive information

Given the risk associated with **external transfer** of sensitive data, any plan that entails external transfer requires prior approval by the UMB department program lead of the UMB Funding Unit.

File security

File security must be upheld in specific ways and while implementing specific tasks, as follows.

Storage: MGIC files and documents must be stored in MGIC offices, on MGIC- or UMB-owned IT equipment, and in MGIC or UMB online repositories. MGIC offices **should not** store files and documents:

- On thumb drives, memory sticks, flash memory cards, or similar media
- Using online and cloud services such as personal cloud storage services, personal emails, online file converters (pdf, CSV, jpg), and generally any other services that require uploading CO data to another server
- In employees' homes, on personal IT devices, or in other personal spaces, unless an exception has been granted for MGIC employees who have been assigned to work permanently from a home office. This exception may only be approved by the CD/CR or equivalent MGIC leadership position, and only upon verification by the IT support lead that MGIC and UMB data protection and security standards are met in the home office.

For additional information or if an exception is to be requested, see confidentiality in 2-2 MGIC Code of Ethics and Professional Conduct.

Sharing: MGIC personnel must use the UMB preferred secure file transfer platform, currently Microsoft365. Email is not a secure means of sending sensitive data and its use can put MGIC at risk of legal and compliance issues. Sending files via email is advised only for an occasional data-sharing need, in which case the email must be encrypted. Further, MGIC personnel should refrain from sharing sensitive data on peer-to-peer file sharing platforms.

MGIC personnel can use shared repositories in the servers within the office local area network (LAN) as a means to share files. Partners or UMB/MGIC affiliates shall share their data through secure file transfer protocol (FTP) services via a secure virtual private network tunnel (VPN) that is encrypted to ensure confidentiality of information. See IT security at partners' facilities and elsewhere for more information.

Safeguarding protected information: MGIC offices must strive to reasonably safeguard protected information from intentional or unintentional disclosure by implementing a mechanism to encrypt information and implementing procedures that verify that a person or entity seeking access is properly authenticated.

Encrypting Email

If using a Microsoft Office 365 email account, the user can encrypt an email message by adding [secure] anywhere in an email's subject line.

Office 365 will encrypt the email and all attachments before sending the email to recipients. Recipients can reply to the encrypted email and their reply plus any added attachments will also be encrypted.

For further information, see the UMB webpage on Sending Secure Encrypted Emails.

Database with PII: If a database is hosted on any UMB-administered infrastructure and contains PII such as names, phone numbers, GPS coordinates, or dates of birth, MGIC personnel must implement data encryption on all PII fields. A de-identified dataset should be utilized for program management and improvement, and all unique identifiers should be removed from this dataset. Each MGIC office should restrict the number of individuals who have access to the code to permit re-identification if needed.

Email security: UMB/MGIC email accounts should be used exclusively for MGIC-related business. MGIC personnel should not use their personal email accounts for MGIC-related business and understand that sharing of MGIC sensitive data via personal email accounts is particularly risky. All email shall have two-factor authentication configured.

Mobile device security: Mobile device management (MDM) enables the complete remote "wipe" of the mobile device and renders the data unrecoverable, in the event of theft or loss, as soon as the device is reconnected to the internet. UMB's current license for Microsoft InTune provides MDM capabilities and should be used on all mobile devices used to conduct MGIC business.

If a mobile device is used to collect sensitive data, the device storage must be encrypted, and access to the operating system password-protected. For devices used to collect data in a field activity such as survey or site visits:

- The operating system should lock the device for at least 30 seconds after five failed attempts to unlock it (incorrect password entries).
- The data erasure process should be triggered after a maximum of 15 failed attempts to unlock the device (again, incorrect password entries).

When it is necessary to access sensitive data, MGIC personnel must safeguard the information and never leave it unattended.

Data breaches: Individuals who become aware that sensitive data has been shared or otherwise divulged contrary to confidentiality obligations in the MGIC Code of Ethics and Professional Conduct should immediately notify their supervisor and the CD/CR, preferably in writing, and/or report the data breach through the Ethics Hotline which provides a confidential and anonymous reporting mechanism.

See also 3-11 Confidentiality and Data Security and 3-12 Record Retention and Access.

Remote access to MGIC office IT network

MGIC personnel may require access to MGIC networked resources and information to carry out work outside of the office, such as on a field visit or when working remotely. While networked access can increase productivity, there are also associated risks and threats that need to be minimized.

The process of accessing the IT network remotely must meet the same security standards as those that apply to accessing the network in-office. Remote access must be through VPN and strictly controlled through authentication and authorization measures.

Similarly, acceptable use and security policies that apply to in-office devices also apply to devices connecting to the IT network remotely. Logon information may not be shared with others. IT devices owned by personnel that are used to access MGIC systems remotely must have updated and active antivirus protection software.

The IT support lead must pre-approve remote access to networked resources and information, and the approval must be documented in writing. Requirements shall include:

- Compliance with endpoint protection requirements
- Encryption used for data transmission between remotely situated workstations and the network
- Configuration to drop inactive connections after 30 minutes, whenever possible
- MDM software (e.g., Microsoft InTune) on mobile devices to enable remote wiping of the device
- Prior and explicit approval by MGIC's Regional IT Lead or UMB's IT department for any use of third-party products or services that establish remote access or bypass institutionally approved VPN connections (e.g., PCAnywhere, GoToMyPC)

Only approved remote access software shall be used by IT personnel while providing IT support remotely.

Protecting against spam, phishing, and hacking attempts

Spam, phishing, and hacking attempts are common IT security challenges, and MGIC must leverage existing UMB tools and educate its personnel to help minimize these risks. Actions an office can take to help secure the network and sensitive information include:

- Limit use of personal accounts on networked devices
- Install and maintain UMB's endpoint protection tools, including Microsoft InTune and the other management tools listed above.
- Train all personnel at least once every year on security awareness and educate them on common attempts and how to avoid inadvertently providing access
- Ensure all systems have up-to-date antivirus software, including security patches and updates
- Password protect and encrypt sensitive data whenever there is a need to share the data

Individuals who are concerned that an MGIC IT asset or system may have been compromised through a phishing or hacking attempt should immediately notify their supervisor or the IT support lead.

Endpoint protection

MGIC-approved endpoint protection software must be installed, updated, and maintained in each MGIC device and server. The endpoint protection will ensure effective vulnerability management, allocation of local admin privileges, application whitelisting and control as well as antivirus protection. The software should be set to start up when the device itself starts up (boots) and should automatically conduct a daily check for updates from the manufacturer's website/portal.

The IT support lead, with support from a service provider if needed, implements a systematic, accountable, and documented process for managing exposure to vulnerabilities through timely deployment of endpoint protection software updates and patches.

Username and password security

All MGIC devices require a unique username and password for access, while all Wi-Fi connections require a unique Service Set Identifier (SSID) and security key for access. Each user of a device connected to the MGIC network has either a unique network account or is an authorized guest user.

Passwords are selected by the individual users or, in the case of office Wi-Fi access, by the IT support lead. A password must be "strong," i.e., carefully chosen by the user so that it is easy for the user to remember but difficult for anyone else to guess. At a minimum, passwords for email and UMID accounts must be changed every year, and passwords for administrator accounts must be changed every three months. All passwords must meet the following criteria:

- 12 characters
- One number
- One symbol
- An upper-case letter
- A lower-case letter

MGIC personnel are prohibited from sharing their user credentials or otherwise permitting another employee or unauthorized user to access sensitive information in UMB/MGIC IT systems.

MGIC personnel are encouraged to log out of their devices whenever they are left unattended. An office may mandate the use of a password-protected screensaver after a defined period of inactivity by a user, especially for devices that store or access sensitive data.

Data and systems back-ups

UMB/MGIC email accounts are kept securely backed up at the University level. For other data and systems, country offices are encouraged to use secure cloud back-up options, e.g., Microsoft OneDrive.

MGIC offices should conduct regularly scheduled data and systems back-ups. For individual devices, daily back-ups are automated to a local server, external hard drive, or some other UMB/MGIC-provided location. Where devices are not connected by an office network (i.e., stand-alone computers) in field sub-offices and partner facilities, it is recommended that the country office

implement automated back-ups. If automation is not possible, the IT support lead ensures staff back up all their data to an external hard drive or USB drive on at least a weekly basis.

It is recommended that financial data, servers, or systems be backed up **daily**, with other critical business data, servers, and systems backed up regularly and automatically on a set schedule. Back-ups must be securely stored in a different geographic location from that of the MGIC office.

Also recommended for servers and other critical IT equipment is the provision of an uninterruptible power supply (UPS) system with enough runtime to avoid downtime and prevent loss of data when utility power is interrupted or fluctuates outside safe levels.

IT systems audits

IT systems audits should be conducted on at least an annual basis. Such audits involve testing and assessing whether MGIC is successfully protecting data, software applications, and operating systems. IT systems audits focus on IT security and typically include a technical assessment of the IT infrastructure and an audit of physical and administrative controls. Steps may include:

- Review current security-related materials (e.g., written policies and procedures)
- Review the latest applicable UMB, MGIC, and sponsor requirements and local laws against MGIC data security and confidentiality policies
- Identify any policies or procedures that are either barriers to information sharing or sources of data security weaknesses
- Review any history of data security breaches or near-breaches, and associated lessons learned
- Assess physical security and define the secure area
- Confirm all software on MGIC computers is licensed
- Assess electronic security protections and methods of data transfer and storage
- Assess factors related to security of information in the field, as appropriate
- Assess training needs

IT systems audits should be fully documented. For further guidance, the IT support lead may consult with the regional IT support lead.

IT security at partners' facilities and elsewhere

MGIC should ensure that partners are aware of their IT-security-related responsibilities as required under the terms and conditions of the UMG/MGIC subaward, memorandum of understanding (MOU), or other partnership agreement. Capacity permitting, MGIC may provide general technical support to partners for proactive protection of information systems and sensitive data, including PII.

MGIC programming and research activity may include collaborating with partners on data collection from health facilities, households, and other sources. If the data will be transmitted to MGIC, the office should assist the partners with appropriate security measures. These include measures related to the **device** used for data collection and transmission:

- Encrypt the storage on the devices used to collect the data
- After submission/upload of the data, delete the data files from the device
- Protect the device with a strong password that is changed every three months
- Run the device with the latest recommended software, including antivirus software
- Set up MDM software on the device

They also include measures related to the **medium** of file transmission:

- Set up a File Transfer Protocol Secure (FTPS) server for the collection of files from facilities
- Make the FTPS server accessible only over a VPN connection
- Have at least two MGIC personnel authorize new users before setting up their access in the FTPS system
- Ensure each user has a personalized FTP account, a personalized folder for files submission allowing uploads only, and authentication with a strong password that must be changed every three months

What are data storage devices (media)?

Any piece of equipment that stores data, including:

- Desktop computers
- Laptops
- Network servers
- Mobile phones
- Multi-function printer/copiers
- Removable devices such as USB flash drives and external drives

If MGIC personnel are posted at a partner's facility, such as a district health office, or are assigned to work from an approved home office location, the IT support lead supports them in adhering to MGIC IT Policies and Procedures at their duty station.

Wherever possible, MGIC should leverage Microsoft365 tools when collaborating with partners, as a best practice.

Sanitizing IT equipment before disposition, reuse, or repurpose

When disposing of IT equipment, country offices follow MGIC asset disposition requirements (see 3-7 Property Management) and take additional precautions related to protecting sensitive data. This includes when returning rented equipment, such as a photocopier, to a vendor. Moreover, the same precautions must be taken if IT equipment is to be reused or repurposed at an MGIC office or elsewhere.

In such cases, data storage devices that contain sensitive data must be wiped or "sanitized" to render the data unrecoverable. Sanitization prevents information from being retrieved by data, disk, or file-recovery utilities. MGIC offices may reference the UMB Procedure for Disposal of Media Containing Sensitive Data for the latest guidance on the data sanitization process to use for each type of asset, as recommended by the USG National Institute of Standards and Technology (NIST).

What is media "sanitization"

A process that renders access to target data on the media infeasible for a given level of effort

Prior to sanitizing IT equipment, MGIC should follow record retention procedures as laid out in 3-12 Record Retention and Access.

Terminating access upon separation

To maintain security for data and IT systems, the separation process for MGIC personnel must include immediate termination of all accounts and access. See 7-6 Establishing and Terminating Accounts and Access and 4-20 Separation from Employment.

Checklist for CDs/CRs

- ☐ Have IT security systems in place and foster a work environment where MGIC personnel actively protect personally identifiable information in all forms and other sensitive information
- ☐ Require that MGIC files and documents be stored on MGIC or UMB devices and repositories and not on personal devices, others' servers, or other unapproved devices and locations unless an exception has been granted for employees assigned to a home office location.
- ☐ Take consistent measures to minimize risk of spam, phishing, and hacking through use of, but not limited to, filters, antivirus software, password protection, and training of MGIC personnel
- ☐ Require usernames and passwords for access to all devices, and SSIDs and security keys for Wi-Fi access, and mandate that passwords be changed every three months
- ☐ Give priority to monitoring and, as possible, automating back-ups of data and systems, especially those handling critical business data
- ☐ Conduct IT systems audits on at least an annual basis and document the process and results
- ☐ Ensure data storage devices with sensitive data are disposed of following the latest guidance on data sanitization
- ☐ Enforce the requirement that IT accounts for separated employees be terminated immediately

Key references

- 2-2 MGIC Code of Ethics and Professional Conduct
- 3-7 Property Management
- 3-11 Confidentiality and Data Security
- 3-12 Record Retention and Access
- 4-20 Separation from Employment
- 7-6 Establishing and Terminating Accounts and Access
- Ethics Hotline (https://www.umaryland.edu/mgic/ethics-hotline/)
- UMB webpage on Sending Secure Encrypted Emails
- X-99.08(A) UMB Policy on Disposal of Media Containing Sensitive Data

7-5 Acceptable Use

Policy statement

Acceptable use of UMB and MGIC IT resources is use in support of research, programs, education, service, and administrative activities of UMB and MGIC. All users must be held to account for responsible and professional use of IT resources. Misuse of IT resources poses tremendous risk to the operations, integrity, and reputation of UMB and MGIC, and may result in disciplinary action up to and including termination of employment.

UMB and MGIC monitor use of UMB/MGIC IT resources to ensure compliance with acceptable use. Authorized users should have no expectation of privacy as to information stored or transmitted using UMB/MGIC IT resources. Suspected violations of IT policies and misuse of UMB/MGIC IT resources should be reported immediately to an employee's supervisor, the IT support lead, or through the Ethics Hotline.

Acceptable use

Acceptable use means that authorized users:

- Are responsible for safeguarding their own identification (ID) codes and passwords
- Are responsible for using their ID codes and passwords only for their intended purposes
- Are responsible for using UMB/MGIC IT resources in a manner consistent with MGIC core values and adhering to the MGIC Code of Ethics and Professional Conduct
- Are responsible for all transactions made under the authorization of their ID
- Are responsible for any activity that involves UMB/MGIC IT resources and that originates from computing devices owned by or assigned to them
- May not represent or imply that personal electronic publications (e.g., web pages, social media content) or personal communications reflect the views or policies of UMB or MGIC
- May not state or imply that links provided from web pages hosted on UMB or MGIC IT resources constitute or imply a UMB or MGIC endorsement of those sites, their content, or products and services associated with those sites

Our Values

MGIC's core values are at the heart of our mission to improve the human condition and serve the public good through education, research, clinical care, and service. These core values guide our programs, operating philosophy, and commitment to our constituents, while supporting our dedication to global enhancement and social progress.

Respect and Integrity: We value each other and hold ourselves accountable for acting ethically and transparently using compassion and empathy.

Well-Being and Sustainability: We care about the welfare of our people, planet, communities, and University.

Equity and Justice: We embrace and are committed to diversity, and we value inclusive and just communities. We oppose racism and oppression in all its forms.

Innovation and Discovery: We imagine and explore new and improved ways to accomplish our mission through education, research, clinical care, and service.

Misuse

Misuse is use of UMB/MGIC IT resources in a manner not consistent with standards for acceptable use. Misuse includes, but is not limited to:

- Securing unauthorized access to or unauthorized use of UMB/MGIC IT resources, or facilitating such use or access by another person
- Accessing or attempting to access UMB/MGIC IT resources on or off MGIC premises without authority (which is also referred to as hacking)
- Any deliberate or reckless act that denies or interferes with the access and use of UMB/MGIC IT resources by others
- Use of UMB/MGIC IT resources in violation of the law or the policies of MGIC, including anti-discrimination or harassment policies
- Personal communication, or other personal use, that interferes with the use of UMB/MGIC IT resources by authorized users for official MGIC purposes and responsibilities, or that interferes with or indicates neglect of employment responsibilities (e.g., use of online retail sites, video streaming, internet gaming, or distracting or extensive personal messaging that interferes with job productivity)
- Software theft or piracy, data theft, copyright violations, and other actions that violate the intellectual property rights of others

- Inappropriate access, use, or disclosure of data including confidential personal identification numbers, birth dates, addresses, or other personally identifiable information; unauthorized sale or transfer of such information
- Altering system hardware configurations without authorization; installing or deleting system software without authorization; installing or removing system hardware without authorization
- Intercepting or monitoring communications, user dialog, or password input intended for another recipient, except when this is done as part of authorized IT resource management or if required by law
- Collecting or storing information about users of UMB/MGIC IT resources without user authorization, except as necessary for official MGIC activities and functions; or collection or storing of information which does not comply with local law
- Illegal activity or other misconduct, including the use of work time or UMB/MGIC IT resources to access pornography
- Business or commercial activity not carried out on behalf of UMB or MGIC
- Access to or use of electronic distribution lists and email accounts created by UMB or MGIC for purposes not authorized by UMB or MGIC; permitting others access to such distribution lists for unauthorized purposes
- Transmitting messages that are threatening, obscene, vulgar, derogatory or harassing; messages that attack another individual or group of individuals; or messages that violate the policies of MGIC including the MGIC Code of Ethics and Professional Conduct
- Anomalous (unusual or unexpected) computing activity that is illegal or wasteful of UMB/MGIC IT resources or that violates the terms of use of the licenses and agreements through which UMB or MGIC obtains or uses IT resources

Security and monitoring

The maintenance, operation, and security of UMB/MGIC IT resources may require monitoring, including logging activity and usage patterns, which is designed at the discretion of the IT support lead.

MGIC has the right to monitor use of IT resources, including email, file-sharing, and internet activity of specific individuals or systems. Users may be subject to monitoring without specific notification. Special monitoring of an individual may involve checking as to whether:

- A user may be violating any aspect of this Policy, work rules, or law
- A user has voluntarily made activity or account information available to the public, as by posting to an electronic list or web page
- A user is taking actions that compromise the security, integrity, or functionality of IT resources
- A user of UMB/MGIC IT resources or an account has business-related reasons for anomalous activity demonstrated by usage patterns
- A person using UMB/MGIC IT resources is doing so without authorization

Monitoring of the use of IT resources shall be for business purposes as permitted by law. If an MGIC office or team would like to initiate a new type of monitoring, the IT support lead should first consult the regional IT support lead and UMB department administrator for guidance and coordination.

Office Wi-Fi

MGIC offices should strive to have continuous and adequate Wi-Fi access for personnel and guests to complete MGIC-related activities. Offices must have separate internal and guest Wi-Fi access points and credentials to ensure security of internal data and systems. Passwords on the office Wi-Fi accounts must be changed every three months. In order to ensure adequate bandwidth for CMGIC related functions, the IT support lead, in coordination with the DFA and a service provider if needed, may restrict access entirely or at certain high-traffic times to websites that require high amounts of bandwidth, such as video streaming platforms.

Email use

UMB/MGIC email accounts must be used for all business-related communications. Occasional use of email for personal communications during the business day is acceptable. Users are advised, however, that they have no right of privacy in personal communications sent or received using UMB/MGIC email. Such messages are subject to monitoring and disclosure.

Copyright laws, license agreements, MGIC policies, and relevant local laws apply to email. Email sent with the intent of disrupting communication or other system services is not allowed. Use of email for sharing unsolicited commercial purposes or chain letters, for example, is not acceptable.

Broadcast email sent to a full list of users beyond an individual office or team is prohibited unless approved by the UMB department operations lead.

The IT support lead may carry out training or issue additional guidance for MGIC personnel on topics such as email etiquette, leveraging Microsoft Outlook productively and collaboratively, shared calendaring, or other topics that would benefit efficient and effective operations.

Web pages

MGIC personnel who create, maintain, or host a web page using UMB/MGIC IT resources are responsible for the integrity of the information contained in the page and for compliance with MGIC policies and local laws including those that govern copyright, obscenity, defamation, and software piracy.

Personal or commercial web pages may not be posted using UMB/MGIC IT resources unless expressly authorized by the CD/CR and then only if the web page is related to MGIC activities. Creating web content or maintaining web pages that are contrary to MGIC core values of accountability, civility, collaboration, diversity, excellence, knowledge, and leadership are not acceptable use of UMB/MGIC IT resources.

Reporting and investigating violations

Suspected violations of IT policies and misuse of UMB/MGIC IT resources should be reported immediately to an employee's supervisor, the IT support lead, or through the Ethics Hotline.

In close consultation with the HR lead and in a manner that is timely, respectful, and to the extent possible confidential, the IT support lead shall investigate thoroughly issues concerning use of UMB/MGIC IT resources. The IT support lead must provide a detailed report of the investigation to the CD/CR and cooperate in disciplinary proceedings as needed. an MGIC office may suspend an accused user's access to some or all UMB/MGIC IT resources until an investigation is complete and, if required, a formal discussion has been held to determine the validity of the allegations.

Users who commit serious or repeated violations of IT policies are subject to additional sanctions such as permanent termination of access to UMB/MGIC IT resources, use restrictions, or special monitoring. Further, violation of IT policies and misuse of UMB/MGIC IT resources may result in disciplinary action up to and including termination of employment.

Immediate action may be taken by the IT support lead in consultation with the HR lead in response to potential or ongoing threats to IT asset security, the health or safety of persons, the privacy rights of personnel and program or research participants, compliance with the law, or the security of sensitive information. The regional IT support lead should be notified without delay of actions taken in this regard. Further, the HR lead or CD/CR shall immediately report suspected criminal violations of law to the UMB department operations lead and MGIC President for further action.

Additional policies and guidelines on acceptable use

UMB Funding Units may provide MGIC offices with a Data Management Policy or other additional acceptable use guidelines relevant to their sponsors or funding sources. If these provide contradictory guidance or direction to MGIC Policies and Procedures or local law and regulations, the CD/CR should contact the IO Department's IT Manager to determine how to address the contradictions.

MGIC offices themselves may implement additional requirements for appropriate and acceptable use of IT resources. Such requirements shall be no less restrictive than this Policy and do not supplant this, Policy. IT support leads should contact the IO department's IT Manager for assistance with policy interpretation and compliance as needed.

Checklist for CDs/CRs

- ☐ Foster a work environment where MGIC personnel are aware of what constitutes the acceptable use of IT resources in support of MGIC programming and research and understand that misuse may result in discipline and possible termination of employment
- ☐ If choosing to initiate a new type of monitoring, consult with the regional IT support lead and UMB department administrator for guidance and coordination
- ☐ Follow all relevant laws, licensing agreements, and policies for email
- ☐ Ensure personnel managing MGIC web pages conform to the integrity and compliance requirements for the information posted online
- ☐ Encourage personnel to report suspected violations of IT policies and misuse
- ☐ Work in close consultation with the IT support lead and HR lead to investigate and take action on violations of IT policy
- ☐ Consult the IO department IT Manager for MGIC and UMB policy guidance as needed

Key references

- 2-2 MGIC Code of Ethics and Professional Conduct
- Ethics Hotline

7-6 Establishing and Terminating Accounts and Access

Policy statement

The MGIC office is responsible for planning and coordinating among IT, human resources, supervisors, and the regional IT support lead to ensure employees are provided with timely and

efficient access to UMB/MGIC email accounts and information systems, thus supporting them in effectively carrying out their MGIC-related activities. Similarly, coordination is needed for proper and timely termination of employee accounts and access, which helps ensure security of UMB/MGIC IT resources and data.

Procedures

The IT support lead, as well as the HR Lead, are responsible for maintaining an up-to-date list of all authorized users of IT resources and users assigned to the MGIC office. The list should document users' access to accounts, authorization level for each MGIC system, and status on awareness trainings related to information security of sensitive data, including the handling of PII.

MGIC offices must strive to have email and other system accounts accessible to new hires on the first day of employment to ensure productive on-boarding and orientation. Supervisors may request that the IT support lead provide basic training on standard IT resources. See 4-9 Orientation.

To establish a new UMB/MGIC email account, as well as network and systems access, the HR lead or other appropriate manager submits a request to the regional IT support lead in which the employee's full name, position title, and start and dates are provided. The regional IT support lead in turn seeks approval from the UMB department operations lead.

When an employee leaves MGIC for any reason, their access to MGIC devices and systems **must be revoked immediately**. The employee's supervisor is responsible for instructing the departing employee to maintain all UMB/MGIC files and data and ensuring that the data stored on the employee's device is archived, working with the IT support lead for technical support. Upon separation of employment, the IT support lead or other appropriate MGIC manager must contact the regional IT support lead at least two business days prior to departure of an employee to schedule the termination of accounts and access.

The Regional IT Support Lead is responsible for processing new hires and employee terminations in the UMB Community System, and is accountable for the accuracy of MGIC staff roles in the UMB system at all times. The source data for this vitally important responsibility are MGIC office Personnel Action Forms and timely, advance communications from the MGIC office's HR lead or other senior management regarding employee status changes. See 4-20 Separation of Employment.

Checklist for CDs/CRs

- ☐ Ensure personnel receive timely and efficient access to UMB/MGIC email and information system accounts
- ☐ Enforce the requirement that accounts for separated employees be terminated immediately

Key references

- 4-9 Orientation
- 4-20 Separation of Employment