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

MGIC Policies and Procedures – Safety and Security

Board Approved September 2023

Contents

8. SAFETY AND SECURITY

Definitions

About "Designees"

These 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 the 5-4 Signature Authorities and with appropriate internal controls in place.

Capital asset: see *Equipment*
Country director (CD): The lead manager of a country office. This position directly supervises senior management positions in an MGIC country office and reports to the designee of the MGIC President.
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. 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 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. **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*.
Device: Any desktop computer, laptop, tablet, mobile phone, or other physical hardware or equipment that provides computing functions within a computing system.
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 country 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.
Duty of care: Responsibility to provide all employees with a reasonably safe work environment, free from recognized hazards, and to warn of any reasonably foreseeable risks.
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.
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 US$5,000 or more; and (3) is complete in itself and does not lose its identify or become a component part of another article when put into use.
Human resources (HR) lead: The lead specialist in an MGIC office with responsibilities related to human resources management, which could in some cases be the DFA or a project manager.
IT resources: Resources related to IT operations, including computerized information, computing facilities, computer networks, hardware, software, systems, programs, and devices.
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: Individuals engaged under MGIC Employment Contracts or by a third-party Employer of Record (EOR) retained by MGIC. MGIC Personnel may live and work in a country regardless of whether MGIC has an established country office or not.
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.
Property lead: The staff member designated to oversee office property management and ensure MGIC property management standards and procedures are met.
Safety and security focal point (SFP): The person holding chief responsibility for implementing, administering, monitoring, and evaluating the safety and security policies, procedures, and plans of the country office.
Sensitive data: Any personal, confidential, and legally protected information, including personally identifiable information (PII) associated with patient and study participant data.

UMB Central Administration: The offices and departments of UMB that oversee university-wide systems, policies, procedures and standards. These offices are designated by the MGIC Board to support the governance, compliance, and administration of MGIC. They include, among others, International Operations, Sponsored Program Administration, Sponsored Program Accounting and Compliance, Human Resources, the Office of the Controller, the Office of Accountability and Compliance, and the Office of Legal Counsel.
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.

8-1 Overview of Safety and Security Policies and Procedures

Policy principles

MGIC has both a legal and a moral obligation to fulfill its duty of care, which involves operating in a reasonable manner to reduce the risk of foreseeable injury and other harm to those working for MGIC. These Safety and Security Policies and Procedures direct and guide personnel regarding the appropriate support and mitigation measures they should have in place to fulfill that duty.

Primacy of Life over Assets: It is the Policy of the University of Maryland, Baltimore (UMB) and Maryland Global Initiatives Corporation (MGIC) that the safety and security of MGIC staff always take precedence over all other factors. This means management and personnel must give higher priority to the health, safety, and security of people over protection of operations/programs, facilities, equipment, or reputation. MGIC's commitment includes:

- Understanding and assessing threats, vulnerabilities, and risks
- Planning for and mitigating risks to personnel and assets under the country office's control
- Clearly communicating about risks
- Preparing personnel to minimize the probability and impact of a threat or an incident
- Ensuring incident management includes post-incident care for personnel

Duty of Care: MGIC leadership is committed to creating a culture of effective and pragmatic safety and security risk management across all operations that meets our duty of care responsibilities to all personnel. MGIC seeks to create this culture by establishing reasonable, sustainable measures to mitigate recognized risks; by integrating safety and security risk-management principles into research and program design and delivery; by empowering our personnel to take responsible decisions through a better understanding of the complex environments in which we operate; and, by investing resources to develop innovative tools and systems that enable program management to minimize safety and security risks to personnel while maximizing the impact of our research and other programs.

Right to Withdraw: MGIC upholds the right to modify or suspend operations, and to withdraw personnel from an area, zone, or country at any time as safety and security conditions warrant. Refusal by personnel to abide by MGIC directives may result in their dismissal. Regardless of the reason, personnel and their dependents refusing an evacuation or relocation order must acknowledge in writing that they are remaining at their risk and that MGIC will not accept further responsibility for their safety.

MGIC upholds the right of all personnel to withdraw from a situation that they feel poses an unreasonable level of risk, without suffering disciplinary action. No manager or other personnel may force, intimidate, or otherwise coerce another employee into doing something which that employee feels represents an unreasonable risk.

- Personnel who feel uncomfortable with the level of danger and risk imposed on them by their work should report that discomfort to their supervisor, the country director or country representative (CD/CR), or another member of senior management or through the Ethics Hotline
- Personnel who receive any instructions they consider threatening to themselves or those around them are obliged to report the issue to their supervisor, the CD/CR, or another member of senior management or through the Ethics Hotline.

Security vs. Safety

Security is primarily concerned with **intentional** acts of violence and other harm, while **safety** is primarily concerned with **unintentional** or **accidental** acts or events.

A supervisor receiving these types of reports is obliged to communicate the issue to the CD/CR or another member of senior management. MGIC office management is responsible for undertaking a review of any such report and determining and implementing an appropriate course of action.

Terminology related to safety and security

The following definitions explain terminology as related to safety and security and associated CO management duties.

A ***crisis*** is defined as: 1) a negative event that was unanticipated and for which plans had not been formulated, 2) a negative event that had been planned for, but has happened at a rate or pace unanticipated, or 3) a confluence of negative events anticipated and planned for individually, but not in combination.

Duty of care is the duty that an employer has to operate in a reasonable manner to avoid the risk of foreseeable injury and other harm to its employees. "Reasonable" is measured in comparison to industry standards in a particular operating environment. "Foreseeable" risks are those that can be identified, mitigated against, and educated about.

Hazards are natural, technological, or human-caused sources or causes of harm or difficulty.

Incident refers to an occurrence, event, accident, or change in a particular set of circumstances that poses a negative impact on or exposure to MGIC/UMB in terms of safety, security, or reputation.

Mitigation refers to activities intended to reduce harm to people, property, and institutional reputation by avoiding, preventing, or stopping incidents or events with potentially negative impact.

Risks exist as the potential for an unwanted outcome resulting from an incident or occurrence, as determined by its likelihood and the associated consequence.

Threats are hazards that are primarily focused on adversarial human-caused incidents.

Vulnerabilities are physical features or operational attributes that render an entity or an individual susceptible to a given hazard.

Safety and security risk management approaches

MGIC employs a three-pronged strategy to mitigate risk and safeguard operational security, seeking a balance among these approaches:

- **The acceptance approach** to program and security management is founded on effective relationships with, and cultivating and maintaining consent from, various stakeholders in an operational area as a means of reducing or removing potential threats. The aim of these effective relationships is to access vulnerable populations and undertake MGIC activities.
- **The protection approach** aims to reduce risk through protective devices for people, property, and premises (e.g., bars on the office windows, MGIC ID badges that personnel wear, facemasks, and hand sanitizer).
- **The deterrence approach** aims to reduce risk by containing a threat (e.g., suspending activities, using armed guards).

The acceptance approach is important and requires country offices to work creatively and persistently to maintain a public perception of the organization as impartial and independent. Among other things, acceptance is heavily influenced by actions of personnel, engagement with the

community, design and implementation of research and programs, and development of partnerships and relationships.
The acceptance approach alone is not sufficient, and country offices should always consider the full gamut of safety and security risk management approaches when deciding how to respond as threats in the operating environment shift, rise, and fall.

In addition to the above-mentioned prevention measures, personnel should give regular attention to preparedness of contingency plans for critical incident response (see 8-3 Critical Incident Management), equipment maintenance, and security trainings/briefings and other communication to maintain awareness and preparedness.

Organization of the policies and procedures for safety and security

Safety and Security
are everyone's business!

This portion of MGIC Policies and Procedures covers the safety and security functions that personnel must carry out to protect and safeguard personnel (duty of care), equipment, and facilities. It sets standards and provides guidance for managing safety and security in a way that fulfills duty of care and related obligations while implementing UMB's research and programming to improve the human condition.

The most important tools – and hence MGIC's core safety and security requirements – are:

1. An up-to-date **Country or Project Safety and Security Plan** that responds to the most common risks in MGIC's areas of operation and includes strategies to manage and mitigate risks, and is known by and readily accessible to all CO personnel
2. A designated **safety and security focal point** (SFP) who has formalized safety and security duties
3. A **safety and security briefing procedure** for all new employees and visitors and a mandated **training course** attended on at least an annual basis
4. **Critical incident management processes and procedures**

In addition to these tools, this section presents key personnel's duties and lays out MGIC Policies on use of guards and/or armed protection, suspension of operations, relocation and evacuation of personnel, security training, and timely and complete reporting of security risks and deficiencies.

The MGIC Safety and Security Policies and Procedures are complementary to other UMB and MGIC Policies and Procedures, notably:

- 2-Ethics and Conduct, which dictates the parameters of a workplace that CO personnel experience as safe
- 3-Administration and Operations on safety and security related to facilities, insurance, and transportation
- 4-10 Working Conditions on a safe and secure workplace
- Cash and staff security in 5-11 Bank Accounts
- 7-Information Technology related to security for IT equipment and other IT resources
- The Office of Emergency Management

The MGIC Safety and Security Policies and Procedures provide a framework within which country-specific rules, procedures, and guidelines must fall and which are documented in Country or Project Safety and Security Plans. The policies align with relevant MGIC and UMB policies and reflect applicable laws and regulations of the United States government (USG).

Country offices should adapt these policies and procedures to reflect local laws and regulations where applicable. Additional guidance should be issued as required to respond appropriately to safety and security in the country office's current and evolving operational environment. For example, operation in an unstable and insecure environment might require guidelines on in-depth and frequent trainings and briefings, processes for locking down facilities and sheltering in place, procedures for use of handheld radios and other specialized equipment, and/or strict restrictions on travel and other activity.

Use of armed protection

Whether to use armed protection is one of the trickiest questions that arises in the sphere of safety and security for international field operations. MGIC leadership may want to consider use of armed protection because of a high level of insecurity and taking into account the importance of balancing the acceptance, protection, and deterrence approaches to security management. Consultation with sponsors may be appropriate in some cases.

If MGIC leadership judges that armed protection would be appropriate in the context and that the associated risks and procedures are manageable, the CD/CR must obtain MGIC President approval to contract armed security services. To start the process, personnel should inquire with local guard companies as to what types of firearms, who may carry one, and under what circumstances the firearm may be used, and document these findings in a proposal. The proposal should be submitted to the UMB Funding Unit department administrator and the UMB International Safety and Security Manager (a member of the International Operations department) for review and escalation to MGIC President or designee.

While in some cases the use of armed protection is sufficient deterrence, in other cases MGIC may choose instead to modify operations or suspend MGIC activities in highly insecure locales or in the country as a whole (see 8-4 Modification, Suspension, and Closure of MGIC Operations).

CD/CR safety and security duties

The CD/CR is ultimately responsible for ensuring that MGIC fulfills its duty of care and protects equipment and facilities. Of highest importance is organizing operations and resources to implement the **Country or Project Safety and Security Plan**. The CD/CR is responsible for setting a tone at the top that emphasizes the importance of staff safety and security and establishes a culture in which all personnel take responsibility for understanding and mitigating safety and security risks to oneself and others.

Other key responsibilities are:

- Include discussion of ***safety and security*** matters whenever the leadership team meets (as a standing agenda item)
- Work with the UMB department operations lead to ensure necessary ***financial resources*** are available to put appropriate safety and security measures in place
- Ensure that at all times, the office has a designated employee or service provider to actively and continuously lead this function, known as the ***safety and security focal point***

By default, the SFP is the HR lead, but the CD/CR may designate another individual for this role, or in cases of a very small team, may also act as the safety and security focal point. .

The CD/CR is additionally responsible for:

- Ensuring that new personnel receive a timely introduction to the Country or Project Safety and Security Plan during their initial orientation period, and communicates to all personnel any changes to the plan
- Ensuring security briefings and trainings are provided as per protocol to personnel and visitors
- Developing plans to prevent and manage incidents and crises, ensuring that the country office has incident management procedures in place, and holding practice sessions
- Notifying the UMB International Safety and Security Manager of any critical incident in which a person is harmed or property is damaged as soon as possible, and compelling MGIC personnel to submit an Incident Report Form within 24 hours (see examples under Critical incidents in 8-3 Critical Incident Management)
- Ensuring use of critical incident management procedures, from reporting through post-incident follow-up actions
- Ensuring that the office or team develops and regularly reviews continuity-of-operations plans to minimize impact on staff and organizational objectives
- Modifying, suspending, or closing operations in consultation with UMB as circumstances require

Safety and security focal point (SFP) duties

Regardless of whether MGIC's presence is on a project or country office basis, the CD/CR should designate a Safety and Security Focal Point (SFP.) By default, the SFP is the HR lead, but the CD/CR may designate another individual for this role, or in cases of a very small team, may also act as the safety and security focal point.

The SFP generally serves in an advisory and supportive capacity. While offices and teams will have distinct structures and staffing, SFP duties are consistent, and the core responsibilities are:

- Collect and share safety and security information through participation in relevant external meetings, subscriptions to listservs, engagement with online platforms, and other means
- Perform assessments of threats and vulnerabilities on at least a quarterly basis and recommend modifications to processes and procedures to mitigate risk
- Develop and maintain an up-to-date Country Safety and Security Plan, where there is a country office, or a Project Safety and Security Plan if there is not a country office.
- Assist with orientation of new personnel and provision of security information to personnel and visitors
- Support MGIC leadership in conducting contingency planning and exercises for potential disruptions to operations
- Encourage the reporting of safety and security risks and incidents and support implementing and documenting subsequent mitigation efforts
- Liaise with personnel responsible for compliance and risk management
- Be familiar with and support compliance with governmental occupational health and safety requirements as they apply to offices, laboratories, and other facilities

Individual responsibilities

Individuals have a duty of compliance to act in accordance with MGIC Safety and Security Policies and Procedures and to support risk management efforts. Individuals are responsible for using their best judgment to minimize their own safety and security risk, keeping in mind that their actions and behaviors can have a harmful impact on other colleagues and the institution as a whole.

MGIC personnel working remotely (where there is no physical country office) should take reasonable measures to ensure that their personal work environment is safe and secure. If they have questions or concerns regarding the security environment in their assigned duty station, they should engage with UMB's International Safety and Security Manager. In most circumstances, UMB will only be able to provide advice or guidance to remote staff in their country of origin.

All personnel must accept this duty and respect that they can put themselves and others at risk if they fail in their responsibilities. Actions that violate MGIC Safety and Security Policies and local procedures and plans may lead to disciplinary action, up to and including termination of employment, as appropriate.

MGIC offices with portfolios funded by more than one UMB Funding Unit

As noted elsewhere in these Policies, MGIC offices and personnel may at times implement programs funded by more than one UMB Funding Unit, and may also be requested to facilitate international activities by UMB Funding Units when there is no physical country office. In such cases, personnel will find themselves servicing multiple UMB "clients" with varying program needs, internal management processes, and expectations of MGIC.

At an operational level, the CD/CR is responsible to uphold MGIC policies and procedures while maintaining effective partnerships with the relevant UMB leads of each program. In complex security environments and critical incident situations, the management of diverse internal stakeholders and their respective needs becomes even more challenging. This responsibility calls for exceptional judgment, decision-making, communication, and management skills to fulfill MGIC's duty of care obligations and to promote the safety and security of personnel and assets.

At an institutional level the MGIC Board of Directors is responsible to ensure effective coordination and coherence in how UMB's schools engage MGIC, and may be called upon to broker or resolve differences that increase organizational risk. When necessary to facilitate sound oversight and efficient decision-making when more than one Funding Unit is implementing programs through the same MGIC office, the MGIC President will designate a UMB employee to fill the roles of UMB Department Administrator and UMB Department Operations Lead for purposes of fulfilling the responsibilities described in these policies and procedures.

In countries where there is a Country Director but other MGIC projects organized outside of the Country Office's remit, the Program/Project Lead should collaborate with the Country Director on matters of safety and security, and elicit the support from the HO safety/security team on safety/security matters affecting either the CO or the project. ----------

Checklist for CDs/CRs

A tool for managing policy implementation and conducting compliance monitoring

- ☐ Set a tone at the top that emphasizes the importance of staff safety and security, and ensure MGIC fulfills its duty of care responsibilities to personnel
- ☐ Ensure there is an up-to-date Country or Project Safety and Security Plan which is readily accessible to all personnel

- Have at all times a designated employee or service provider to fulfill the SFP role
- Ensure the office is providing a safety and security briefing to all new employees and visitors and monitor to ensure compliance; provide/require ongoing training
- Give priority to planning for and managing critical incidents and crises in a systematic way in accordance with MGIC requirements
- Obtain the MGIC President's authorization prior to contracting armed security services or permitting firearms on MGIC premises or in MGIC vehicles
- Ensure safety and security is regularly discussed with and by office leadership
- Ensure necessary financial resources are available to put appropriate safety and security measures in place

Work with the SFP to establish a culture in which all personnel take responsibility for understanding and mitigating safety and security risks to oneself and others

Key references

- Ethics Hotline (https://www.umaryland.edu/mgic/ethics-hotline)
- 2-Ethics and Conduct
- 3-Administration and Operations
- 4-10 Working Conditions
- 5-11 Bank Accounts
- 7-Information Technology
- 8-3 Critical Incident Management
- 8-4 Modification, Suspension, and Closure of MGIC Operations

8-2 Country/Project Safety and Security Plan

Policy statement

Country offices or individual programs/projects are obligated to have a Country or Project Safety and Security Plan that is approved by the UMB department operations lead. It must be updated at least annually and more often in higher-risk environments and as the safety and security landscape changes.

The Country/Project Safety and Security Plan must be available to all personnel assigned to or working with that office or team, and may be translated as needed. All personnel must receive a briefing on the Country/Project Safety and Security Plan upon hire and whenever significant updates are issued. This briefing must cover the procedures for reporting safety and security risks and deficiencies as well as safety and security incidents.

Contents of the Country/Project Safety and Security Plan

The Country/Project Safety and Security Plan provides guidance for all personnel as they carry out their responsibilities. The plan should cover, at a minimum, the following topics as described elsewhere in this section:

- Roles and responsibilities – see safety and security duties, Safety and security focal point (SFP) duties, Individual responsibilities, and the Incident Management Team
- Threat, vulnerability, and risk assessments
- CO/Project operating procedures
- Communications plans, including emergency contacts and phone tree

- Contingency plans including for Modification, suspension, and closure of activities, hibernation, and evacuation
- Emergency evacuation plans
- Security trainings and briefings
- Reporting security risks and deficiencies
- Annexes to the plan

Threat, vulnerability, and risk assessments

All MGIC operating contexts have notable threats, and these evolve over time, as do country offices' vulnerabilities and risks. With a constantly changing environment and dynamic activity, the office must continuously monitor the situation and assess the potential impact changes and shifts might have on risk to MGIC personnel and property. The responsibility for monitoring the security environment lies primarily with the CD/CR and SFP, but other personnel should engage in this as well, so as to provide the office with a fuller view of the security environment.

While the SFP holds the ultimate responsibility for conducting threat, vulnerability, and risk assessments, they should also collaborate with security professionals, be they a part of UMB's security team, private vendors, or members of local security support groups to inform the basis of their assessment. Any assessments should be shared with the UMB security team prior to their inclusion in the CSSP and should also be reassessed on a quarterly basis or more frequently in unstable or rapidly changing operating environments. The results should be communicated to MGIC personnel to enhance their judgment on how best to minimize their own safety and security risk. The results should also be shared with UMB Funding Units and the UMB International Safety and Security Manager to provide them with up-to-date contextual information for making decisions.

In conducting the periodic assessments, the SFP will take into account:

1. External analysis of the local and regional context, including analysis of history and culture, state and non-state actors, demographics, and vulnerabilities associated with gender, sexual orientation, age, race/ethnicity, and other identities, and examination of conflict, crime, and vulnerability to natural disasters and public health emergencies
2. Known or identified threats to MGIC, personnel, and projects
3. Potential impact of known or identified threats and vulnerabilities
4. Options to mitigate or minimize the risks presented by these threats

MGIC operating procedures

The Country/Project Safety and Security Plan includes standard operating procedures (SOPs) for areas particularly critical to mitigating risks to people, equipment, and facilities. The SOPs should draw upon relevant MGIC Policies and Procedures, including:

- Maintaining safe and secure facilities – see 3-5 Facilities Management
- Safety and security while traveling – see 3-8 Travel
- Vehicle safety and security measures – see 3-9 Vehicle Use and Fleet Management
- Cash and staff security – see 5-11 Bank Accounts

Special consideration for transporting non-MGIC/UMB personnel: On occasion, MGIC may transport partner or community representatives in addition to MGIC and UMB personnel. The practice is strongly discouraged but permitted so long as the transportation has a clear business

purpose. In such cases, the office may want to ask each guest passenger to sign a Passenger Release Form, regardless of how comprehensive the country office's vehicle insurance coverage is. Guest passengers must be at least 18 years old; children may not be transported.

Communications plans

MGIC offices should establish and maintain an effective, secure **communications plan** for all sites. This includes:

- The roles and responsibilities that leadership holds on a day-to-day basis as well as in responding to incidents and crises
- The responsibilities of the communications point person
- The communication channels that will be used to provide accurate, coordinated, and timely information to personnel, subrecipient organizations, and other external stakeholders before, during, and after an emergency or crisis
- Who will serve as spokesperson for public inquiries and the media (see 3-11 Communications)
- Who will carry out other communications activities such as rumor control and brand protection
- Emergency notification procedure, specifically, who is authorized to send alert and warning messages to personnel and external recipients and what communication modes will be used

Communication tree: Unless otherwise designated by the CD/CR, the SFP holds the responsibility for maintaining an up-to-date electronic and hard-copy list of personnel's contact information and a "communication tree" for use in case of emergency.

Communications technology: The MGIC office should use appropriate communications technologies that ensure the security of confidential and sensitive information and that enable maintaining contact with personnel and sub-offices on a day-to-day basis and in extreme situations.

Leadership During a Crisis

- Give top priority to providing **all** personnel with regular, clear, and timely information.
- Keep in mind that they may be confused and worried.
- Help them understand what they can expect in this abnormal and unstable environment.

Contingency plans

MGIC offices should develop contingency plans relevant to assessed threats, vulnerabilities, and risks that might negatively affect MGIC operations, programming, and research in that context. These plans should identify procedures that will ensure MGIC can respond quickly to emergency events and critical incidents. They should also include business continuity plans, to ensure critical functions continue (as possible) despite the occurrence of such events.

Contingency plans should seek to identify and address operational gaps and needs that could hinder an emergency response and might include:

- Identifying "critical business data," which is essential information required for the office to function smoothly and prevent operational and programmatic disruptions, as well as sensitive information that must be safeguarded, including all *sensitive data* (see Definitions)

- Setting up mechanisms to allow uninterrupted access to critical business data and other documentation as well as to MGIC IT systems and other IT resources
- Provisioning personnel with equipment such as mobile Wi-Fi, mobile airtime, and laptops that would support their working remotely or otherwise outside the office
- Developing risk-mitigation procedures to protect personnel in the face of a pandemic or other public health emergency
- Developing IT disaster recovery procedures
- Documenting procedures for emergency procurement
- Establishing protocols for handling critical incidents such as hostage taking, sexual violence and assault, gunfire, and carjacking – see 8-3 Critical Incident Management
- Establishing policies and procedures for moving staff – see Hibernation, relocation, and evacuation in 8-4 Modification, Suspension, and Closure of MGIC Operations

Earthquakes? Floods? Riots? Pandemic?

- If an area is prone to earthquakes, the office should have a contingency plan that defines procedures to implement in the event of an earthquake.
- If an area is prone to floods, there should be a plan in the event of flooding.
- If an area is prone to civil unrest, there should be a plan in the event of riots.
- The office should have a contingency plan that addresses the impact a pandemic might have on operations.

MGIC leadership should seek broad engagement by personnel when developing contingency plans. Their range of experience and knowledge will help ensure the plan is relevant and thorough, and their participation will make staff buy-in and adherence more likely.

Contingency plans should be validated through trainings and exercises.

Emergency evacuation plans

Emergency evacuation is one of several immediate response options available in the face of a rapid-onset crisis such as civil unrest, airborne hazards, or weather emergencies. This option limits the potential exposure of persons to hazards that may be present in the environment. The Country/Project Safety and Security Plan should specify who is authorized to order an emergency evacuation, who will notify affected parties and through what communication channels, what transportation may be arranged, and what evacuation routes might be best in a time of crisis. In developing emergency evacuation plans, MGIC leadership should engage the UMB International Safety and Security Manager and/or other security professionals with this experience.

The Country Safety and Security Plan should also state under what very limited circumstances MGIC might move personnel (and possibly their families) to a safer location in the face of a severe threat. See Hibernation, relocation, and evacuation for details.

Security training and briefings

New personnel: The SFP is responsible for ensuring that newly hired personnel receive a full **briefing** on the Country/Project Safety and Security Plan and their responsibilities in relation to it. The briefing should take place within one week of the person's date of hire. In addition, newly hired personnel must complete an MGIC-approved **training course** on personal safety and security. Evidence that new personnel received the briefing and completed the required training course should be placed in their personnel files. Contact the UMB department operations lead or UMB International Safety & Security Manager to access approved training courses.

Every new member of the MGIC team should know about the incident reporting procedure – what to report, when to report, and how to report. Depending on the imminence and severity of threats in the operating environment, participation in safety and security training sessions may also be warranted. Training sessions are valuable for building practical skills that mitigate risk and for increasing compliance with incident reporting and other safety and security requirements.

Visitors to MGIC offices: All visitors from outside the country office's operating context should receive a safety and security briefing upon arrival. Topics to cover include transportation safety, health risks, cultural norms and threats specific to gender and sexual orientation, and other identified threats such as crime and civil unrest. UMB also offers pre-departure briefings to UMB business travelers.

Ongoing safety and security training: MGIC should require that personnel take an MGIC-approved training course on personal safety and security on an annual basis.
Ongoing security briefings: The SFP should keep office leadership well-informed about the security landscape. Even in more stable and lower-threat environments, frequently communicating with personnel about safety and security issues can help mitigate risk and reduce safety and security incidents.

The SFP or any other manager who becomes aware of a significant change in the security landscape should advise MGIC leadership within 24 hours, and should inform the UMB department operations lead and UMB's International Safety & Security Manager.

Reporting security risks and deficiencies

MGIC office leadership should encourage all personnel to **be vigilant for security risks and deficiencies and to report any possible or known threats** – even ones that are dealt with easily and quickly – to the CD/CR or SFP. This includes anything related to safety and security, from rumors of civil unrest, to threats against foreigners or healthcare workers, to personnel not complying with seatbelt usage requirements.

MGIC does not permit retaliation against any person who reports security risks or deficiencies. For further information, see the 2-2 MGIC Code of Ethics and Professional Conduct.

Annexes to the plan

The Country/Project Safety and Security Plan may include annexes as appropriate to support or expand upon information provided therein. Examples include contact information, maps, and evacuation procedures.

Review and approval process for the Project Safety and Security Plan

Legal review: If the Country/Project Safety and Security Plan addresses matters that are pertinent to local labor law or compliance, the country office should consult with local legal counsel when developing the plan.

UMB approval: Once completed, the MGIC office submits their Country/Project Safety and Security Plan to the UMB department operations lead, who in turn coordinates review by other UMB colleagues, seeks approval by UMB'S International Safety and Security Manager,, and communicates approval back to the office.

Revisions: The office should update and revise the Country/Project Safety and Security Plan according to changes in the situation and as learned through regular monitoring and evaluation of threats, vulnerabilities, and risks. In most contexts, annual review of the plan suffices; however, more frequent assessments May be necessary in unstable or rapidly changing operating environments.

Dissemination of the Country/Project Safety and Security Plan

Agreement Statement: Each new employee receives, upon hire, the Country/Project Safety and Security Plan and any revision memoranda or critical security notices released since the plan was last updated. New employees sign the statement acknowledging receipt of the Country/Project Safety and Security Plan (template may be found in the Plan itself) to signify their understanding of what is required and their commitment to adhering to the procedures described therein. When disseminating substantive revisions to the Country/Project Safety and Security Plan, the office collects newly signed acknowledgement statements from all employees. Employees' signed statements are placed in their personnel files.

Access to the Country/Project Safety and Security Plan: The Country/Project Safety and Security Plan should be readily accessible to all employees for application of the procedures in their day-to-day work. This includes accessibility to both hard copies and the digital version. Translation of key portions or of the entire plan into another language may be warranted.

Checklist for CDs/CRs

- ☐ Ensure the office regularly monitors and evaluates threats, vulnerabilities, and risks and adjusts safety and security procedures in response
- ☐ Oversee annual or more frequent updates to the Country/Project Safety and Security Plan, obtain UMB approval for revisions, and ensure all personnel have ready access to it
- ☐ Bring leadership to initiatives that mitigate risk using the acceptance approach and balance it with the protection and deterrence approaches
- ☐ Ensure that the required safety and security trainings and briefings are arranged, and that personnel and visitors participate in them as mandated
- ☐ Support ongoing safety and security trainings and drills, as well as regular security briefings for personnel and leadership
- ☐ Encourage all personnel to be vigilant and report any possible or known threats

Require that upon hire, all new employees receive and sign acknowledgement of receipt of the Country/Project Safety and Security Plan and any revisions since the last update

Key references

- Passenger Release Form
- Ethics Hotline
- 2-2 MGIC Code of Ethics and Professional Conduct
- 3-5 Facilities Management
- 3-8 Travel
- 3-9 Vehicle Use and Fleet Management
- 3-10 Communications
- 5-11 Bank Accounts
- 8-1 Overview of Safety and Security Policies and Procedures

8-3 Critical Incident Management

Policy statement

Personnel must immediately report to their supervisor safety and security incidents that involve the MGIC office or personnel, including minor incidents. The responsible personnel shall complete and submit an Incident Report Form to the DFA, CD/CR, and SFP within 24 hours.

If considered a crisis or a critical incident, the first part of the Incident Report Form must be completed and submitted to the CD/CR and SFP, and to UMB's International Safety and Security Manager, within **24 hours** of the incident. Furthermore, offices are required to document post-incident decisions and other actions taken to mitigate future likelihood and impact.

Of special note:

- Immediate reporting of a ***vehicular crash (accident)*** is required even if the damage to the country office's vehicle or another vehicle is deemed minimal. See Safety and security while traveling in 3-8 Travel.
- If a capital asset or non-capital asset (NCA) is stolen or damaged through criminal activity, the property lead or other responsible CO personnel shall submit an Incident Report Form to the DFA, CD, and SFP and seek a police report.
- Certain exposures to deadly pathogens or poisons are considered safety incidents and, accordingly, should be reported to the same UMB points noted above, as well as to UMB's Institutional Review Board (typically through the UMB program lead).

In the event of a crisis, the CD/CR is responsible for leading the response, mobilizing the Incident Management Team and collaborating with UMB entities as appropriate.

Critical incidents

Critical incidents, which as per the above Policy must be reported to UMB within 24 hours, are usually ***sudden and unexpected*** and/or ***create a significant risk of substantial or serious harm***. Some rise to the level of a crisis (see Terminology related to safety and security). They include, but are not limited to a major vehicular crash, arrest/detention, assault/sexual assault, carjacking, explosion/bomb, kidnapping/abduction, shooting, death, serious threat/intimidation, major riots/protests, and outbreak of violent conflict.

Encouraging Incident Reporting

Leadership should highly encourage managers and individuals to submit reports for any small incident, even if it is dealt with easily and quickly.

Incident Management Team

In countries where MGIC has a large physical presence, the CD/CR should appoint a permanent Incident Management Team, regardless of the current threat level in the operation environment. Its

membership, informed by the Country/Project Safety and Security Plan, should include technical and operations leadership as well as the SFP and communications lead. In countries where MGIC does not have an office or the team is small, the UMB International Safety and Security Manager will engage UMB's institutional Incident Management Team as appropriate to support MGIC's response to critical incidents.

The role of an Incident Management Team includes establishing a response structure, co-opting additional staff members as determined by the nature of the incident, defining roles and responsibilities, determining a response strategy, and formulating and coordinating crisis communications in the face of a critical incident, such as a local, regional, or national outbreak of violence, a sudden-onset natural disaster, or another type of humanitarian crisis.

The CD/CR is expected to immediately notify the UMB department operations lead and UMB International Safety & Security Manager as soon as practical about an emerging crisis, even if all the facts and considerations are not yet known. Subsequent communications should cover the processes and actions of the Incident Management Team. The CD/CR is responsible for ensuring ongoing consultation with UMB and effective coordination between local and university-level Incident Management Teams, specifically regarding crisis communications and especially if the situation may bring high exposure and potential impact on MGIC/UMB operations and/or reputation.

Procedures for responding to critical incidents

An Incident Report Form should be completed and submitted to the CD or CR and security focal point for any incident affecting the safety and security of people and/or property, **within 24 hours**. Reporting through an Incident Report Form is required even if the damage to MGIC's vehicle or another vehicle is deemed minimal.

Any crash or other incident in which a person is harmed, or a vehicle is damaged must be reported **as soon as possible to the UMB International Safety and Security Manager**.

Once notified of an accident or other safety or security incident, the CD or CR is authorized and expected to take immediate measures to ensure medical care and wellness support, personal safety, and property safeguards as appropriate to the immediate situation.

The CD/CR or SFP must also obtain a police report when possible and necessary for potential future legal or insurance requirements.

The CD/CR, SFP and UMB International Safety and Security Manager shall jointly take the lead and coordinate closely with UMB operations leads, UMB program leads, and other relevant stakeholders on the following common procedures, which, depending on the nature of the incident, may include:

- Engaging the UMB operations lead in cases of property theft and damage, vendor and leaseholder negotiations, disciplinary hearings and internal investigations, and other operational matters
- Engaging the UMB program lead for IRB notification, sponsor reporting, and program management purposes as required
- Informing legal counsel for required filings and representation
- Submitting claims to local insurance providers, and documenting incidents for corporate and UMB insurance coverages
- Notifying the MGIC Board of Directors
- Responding to press

- Implementing enhanced security precautions and protections as required
- Conducting after-action reviews, and revising MGIC policies and procedures in response to lessons learned
- Initiating the UMB institutional Incident Management Team as warranted

If the person responsible for the crash or damage violated MGIC policies, procedures, or codes or local traffic law, that person will be held accountable and may be disciplined up to and including termination of employment.

Post-incident action (lessons learned)

The SFP typically collaborates with appropriate MGIC and UMB personnel to conduct an after-action review of each critical incident, consider lessons learned, and develop post-incident actions. This involves completing *Part II: Decisions and Actions Taken/Planned* in the Incident Report Form. Once finalized, incident reports with these follow-on actions should be shared among MGIC and UMB personnel, with the objective of learning and better preparing for future incidents.

Post-incident care

In addition to learning from incidents, MGIC is also committed to post-incident care options for its personnel. Supportive interventions by those trained in psychological support or counseling should start immediately after the critical or traumatic incident to lower stress and reduce negative effects. MGIC may facilitate specialized clinical care, if and as appropriate.

Checklist for CDs/CRs

- ☐ Foster a work environment where personnel immediately report all safety and security incidents, no matter how minor, using the Incident Report Form
- ☐ Ensure the MGIC office complies with the submission requirements for Incident Report Forms, including reporting critical incidents to UMB's International Safety and Security Manager within 24 hours
- ☐ Co-lead the response to critical incidents in partnership with the UMB International Safety and Security Manager
- ☐ Ensure decisions and actions taken in response to incidents are documented and shared with personnel so as to better prepare for and mitigate future incidents
- ☐ Ensure the office provides personnel with post-incident care

Key references

- Incident Report Form
- 3-8 Travel
- 8-1 Overview of Safety and Security Policies and Procedures

8-4 Modification, Suspension, and Closure of MGIC Operations

Policy statement

A rising threat level may require MGIC to modify, suspend, or close operations in a region of a country or in a country as a whole. Activation will be proportionate with the scope of the incident and the needs to perform operational functions.

The recommendation to modify, suspend, or close operations may come from either MGIC or UMB leadership. The CD/CR holds the authority to take immediate action and modify and indefinitely close operations in the face of a threat. If circumstances permit, the CD/CR should consult with the MGIC VP – Policy & Administration and UMB department operations lead prior to proceeding.

The UMB Funding Unit holds the responsibility for formally communicating with sponsors regarding the situation and for obtaining any required sponsor approvals. For information on decisions to close out MGIC operations, see 3-13 Closing MGIC Offices.

Modification of operations

In the face of a natural disaster, conflict, public health crisis, or other major threat or disruption, MGIC may consider making substantial modifications to operations while continuing to implement programming and research. Top considerations that leadership should keep in mind are as follows:

- MGIC must continue to comply with all sponsor requirements unless UMB obtains written approval from sponsors for exceptions or waivers.
- To the extent possible, typical financial record keeping and procurement tools should be used.
- If the office needs to reprioritize work and shift job duties, the supervisors should document the revised tasks and duties. Changes affecting personnel must be in line with local labor law, which in some cases may be quite restrictive and require that the affected employees document their consent to a shift in duties. Changes should be reflected in revised work plans and associated staffing plans, approved by the CD/CR, and submitted to the UMB department program lead for approval.

When considering adjustments to programming and research, MGIC should consider:

1. What are the **activities** that need to be canceled? What are the activities that may need to be ramped up to support an emergency response? What are the activities that may be added if sponsor support is available?
2. With a revised **work plan and scope**, what are the revised staffing needs? Are there staff who need to be re-tasked to other activities? Are there staff who will no longer have a scope of work that can be conducted during the emergency response period? Are there staff who will continue to execute their scope?
3. Given the proposed changes in activities and work plan and scope, are there **financial implications** that will require re-budgeting? Will there be extraordinary procurement expenses? Are there staffing or other expenses that will continue during potential "hold" periods?
4. How might the proposed changes impact **overall risk** to MGIC personnel, assets, and reputation? How best can these risks be mitigated?

Modification of operations might involve shifting personnel to alternate worksites or to working remotely (teleworking) because their duty station is unsafe. MGIC should document instances where they provide individuals with resources such as laptops and extra mobile airtime to make this possible and should confirm the suitability of internet security and data protection. (see Section 7 – Information Technology).

Suspension and closure of operations

When violence flares or other life-threatening factors present a direct threat to the safety and well-being of MGIC personnel, offices may need to suspend operations temporarily, indefinitely, or even permanently. The CD/CR should keep in close communication with the UMB department program and operations leads and UMB International Safety and Security Manager regarding the evolving context, severity of risk, and feasible security measures. Suspension may be the best choice in such circumstances. Suspension is also a reasonable response after a major incident to allow time for serious consideration of the security situation and what to do next.

Suspension of Research

The suspension and closure of MGIC operations usually goes hand-in-hand with the suspension of research, which must be reported to the UMB Institutional Review Board.

However, a situation might arise in which research is suspended but operations continue at a reduced level.

In another possible scenario, research might continue through partners when MGIC operations are suspended or closed out.

Any recommendation to suspend a portion or all operations in-country is presented to the MGIC President, who holds the authority to approve suspension of operations. If a CD/CR has unilaterally suspended operations in the face of a rapid-onset emergency, the CD/CR or MGIC VP – Policy & Administration must seek MGIC President approval to formalize and continue that suspension.

Suspension of operations requires implementing an action plan to fulfill duty of care for personnel, to secure sensitive data and files and arrange access to all critical business data, and to protect and secure property and premises. The CD/CR will lead the development and execution of the plan unless the responsibility is assumed by the UMB department operations lead and/or the UMB International Safety & Security Manager. UMB Funding Units will take the lead on communicating and consulting with sponsors, as appropriate.

In the unlikely case that a severe threat level precludes resumption of operations in any reasonable timeframe and/or security concerns make program implementation impossible for the foreseeable future, the MGIC Board may choose to close the office. UMB Funding Units and MGIC office personnel will take the lead on program and MGIC office operational close-out, while the UMB International Operations Department will manage the legal de-registration of the corporate business or conversion to business dormancy.

Hibernation, relocation, and evacuation

When the threat level is severe, MGIC has several operational options it might implement, all of which require very careful consideration. Modification or suspension of operations might include **hibernation**, with personnel sheltering in place; **relocation**, where personnel (and possibly their families and/or MGIC assets) are moved to a safer location within the country; and/or **evacuation**, where expatriate and TCN personnel are removed from the affected area and taken across an international border. These actions might also be taken in anticipation of rising insecurity, to avoid personnel being exposed to threats.

The Country/Project Safety and Security Plan should address planning for hibernation, relocation, and evacuation depending on the local context. It should indicate the authority levels for decision making, roles and responsibilities and delegation, criteria for who shall be moved and when, and the planned processes. The plans should take into account the varying levels of risk to personnel because of ethnicity, tribe, color, religion, ancestry, national origin, age, gender, and sexual orientation.

In a crisis, the country office/project should strive to protect all personnel as best possible.

- In the event of extreme threat, MGIC may evacuate international staff and accompanying dependents to a safe place in a neighboring country or to home of record.
- MGIC will endeavor to relocate national staff and their immediate family who were posted elsewhere in the country to a safer place within the country.
- MGIC will endeavor to assist in the relocation of any national staff and immediate family who are at risk directly as a consequence of their work, or because of their ethnic origin, or if they are exposed to an imminent or targeted threat.

Awareness of INGOs as targets

When a security situation deteriorates for whatever reason, local populations may determine or believe that (I)NGOs and their staff are in some way responsible. Not only does this increase MGIC's overall threat level, but MGIC may with other (I)NGOs be subject to restrictions and other sanctions imposed by government authorities or others wielding power in that context. Keeping informed and constantly aware is important.

If in this insecure context, personnel experience a medical crisis or assault or other trauma, the HR lead takes responsibility for handling these situations with guidance from the CD/CR and external professionals.

Re-opening and re-initiating operations

Following on plans for how hibernation, relocation, and evacuation will be handled, the MGIC office should have generic plans covering re-opening of offices and re-initiation of operations. In determining if safety and security conditions permit moving forward, leadership should assess, depending on the situation:

- Current and predicted government restrictions
- Prevalence and reliability of data regarding violence, disease, or other threats
- Mitigation and containment capacity
- Recent and predicted actions of communities, partners, donors, and other players
- Actions that international organizations and other entities similar to MGIC are taking

MGIC leadership should consider and address internal conditions when formulating plans to resume programming and operations. This would include:

- Level of risk MGIC and UMB is prepared to take with regard to staff health and safety
- Degree of programmatic necessity for personnel to return to the office or a post location
- Possibility of implementing a phased process, if important for reducing risk
- Adequacy of mitigation and containment measures in place to protect staff in their workspaces, including essential travel
- Clarity and completeness of policies and processes in place to support staff through the transition
- Strength of the internal communications procedure to prepare and inform personnel throughout the re-opening process

The office should engage the UMB department program and operations leads and MGIC VP – Policy & Administration in the planning process. Approval must be sought from the MGIC President to reverse suspension of operations and from the MGIC Board for reversing closure of a country office.

Checklist for CDs/CRs

- ☐ Maintain close communication with and consult the UMB International Safety & Security Manager and UMB department program and operations leads regarding threats that may compel the country office to modify, suspend, or close operations
- ☐ Collaborate with UMB Funding Units on communicating with sponsors in such situations, leaving formal UMB sponsor communications to the UMB department program lead
- ☐ Obtain approval by the MGIC President for partial suspension of operations and re-initiation thereof
- ☐ Ensure any security-related modifications to operations comply with sponsor requirements, unless UMB obtains exceptions or waivers from sponsors
- ☐ Ensure plans for hibernation, relocation, and evacuation account for risks to personnel due to ethnicity, tribe, color, religion, ancestry, national origin, age, gender, and sexual orientation

Key references

- 3-13 Closing MGIC Offices