Microsoft Global Security Corporate Investigation Procedures

California State Bill 553

Purpose:

The purpose of this document is to capture Microsoft's Global Security Investigations (GSI) Americas Workplace Violence Prevention Plan in accordance with California State Bill 553. On September 30, 2023, California Governor Newsom signed CA SB 553, which, among other things, requires covered employers to develop and implement a Workplace Violence Prevention Plan by the law's July 1, 2024 effective date.

Workplace Violence Prevention Plan

Responsible Party:

The Microsoft Global Security Director of Security/Investigations (Americas region), and/or their designee, shall be responsible for the Workplace Violence Prevention Plan.

GSI is a team within the larger Microsoft Global Security (MSGS) organization that delivers a host of workplace violence prevention, support and security-safety response services to the company. 'Life Safety' is the highest core priority for MSGS.

The framework of stakeholders who may provide support to the GSI Threat Managment program at Microsoft may include – based on case related circumstances - representatives from the following groups: CELA Employment Law Attorney, Human Resources (HR), Global Employee Relations (GER), Benefits Business Partner, Global Security Operations, Global Security Operations Center (GSOC), Business and Regulatory Investigations (BRI), Executive Protection Services (EPS), Executive Threat Management (ETM), Executive Threat Intelligence (ETI), Real Estate & Facilities (RE&F), Public Relations, Workplace Investigations Team (WIT), Risk Management, and Business Unit managers/leaders.

Microsoft collaborates with local, state and federal law enforcement agencies as necessary and consults with operational and forensic psychologists/psychiatrists on some cases.

GSI investigators are active members of the Association of Threat Assessment Professionals (ATAP) and some GSI investigators are Certified Threat Managers (CTM) through ATAP.

GSI investigators are trained in using behavioral based Structured Professional Judgement (SPJ) tools to assist with risk assessments, including the Workplace Assessment for Violence Risk (WAVR-21), Communications Threat Assessment Protocol 25 (CTAP-25) and Stalking Risk Profile (SRP).

Internal program review-assessment and process improvements are conducted on an ongoing basis.

GSI maintains a Business Continuity Plan (BCP) that is updated annually.

Annual Training

Responsible Party: Responsibility for employee training at Microsoft is shared across several HR business groups, including Learning & Org Capability and the Microsoft Office of Health and Safety (OHS). The Global Director of OHS & Research is responsible for workplace safety training.

California Labor Code Section 6401.9(e) becomes operative on July 1, 2024. Microsoft will be required to provide most California-based employees with workplace violence prevention training. The training must be provided to California-based employees who work in the office. This would include employees who are hybrid. However, California employees who "telework" from a location of the employee's choice, which is not under the control of the employer" (i.e., remote employees) are not required to receive the training.

Execution: Beginning on July 1, 2024, and annually thereafter, Microsoft will provide workplace safety training to all required employees located in California. The training will compile Microsoft resources related to workplace safety, workplace violence prevention, and workplace violence hazards and details about where to obtain a copy of Microsoft's Workplace Violence Prevention Plan, report incidents, and obtain more information. Employees receiving the training will be required to confirm that they have read and understood the materials.

Reporting Channels and MS Response

There are several channels available to employees and vendor staff to report an incident and/or workplace security-safety concern:

- For emergencies notify the local police for a response by calling 911.
- For urgent matters notify the Global Security Operations Center (GSOC). The GSOC is operated 24 x 7 and can be reached by phone (+1425-706-0000) or email (msgsoc).
    - The GSOC will triage a concern and may initiate law enforcement response, security response and notification to the GSI on-call investigator (24x7).
- For less urgent issues, submit a ReportItNow (RIN) report for either physical security or digital security online reporting (one business day response time).
- Internal stakeholders (CELA, WIT, GER, HR) who partner regularly with GSI are also familiar with the GSI team inbox for reporting, alias 'secinv' (one business day response time).

- Safety concerns are also reported by emailing globalohs@microsoft.com

While the primary methods for reporting physical security related matters are listed above, Microsoft offers additional reporting channels and reporting training via the Microsoft Runs on Trust landing page. Herein, various reporting topics are provided:

"You strengthen trust for Microsoft when you speak up. When you share a concern or ask a question, you can expect it to be taken seriously, reviewed fairly, and kept as confidential as possible. Your concern matters, which is why Microsoft has multiple teams—each designed to handle the specific needs of any situation."

- ReportItNow
- MS Integrity Portal (anonymous reporting)
- AskHR (workplace security/safety concerns are often reported to HR or a manager and then escalated to GSI)
- Workplace Investigations Team

Once GSI receives a potential workplace violence concern via a channel listed above, the team operates with a 24-hour service level agreement to respond to the reporting party, gather critical information/details, and formulate an initial response. Often, a response to a complainant occurs within minutes or hours on a business day. GSI staffs a primary and a secondary on-call investigator 24x7 to respond quickly to reports received by the GSOC after hours, weekends and holidays.

Once a report is received/assigned to an investigator, the matter is triaged for initial details and exigency and a strategic process of information gathering and response begins. The investigative framework utilized is based on industry best standards (ATAP, ASIS) and has been evaluated over time with our legal partners and other key stakeholders. Information gathering commences (reporting party and key witnesses contacted, internal data resources leveraged, open-source public records checked, etc) and partners/stakeholders are engaged. A continuous loop of information updates, risk assessment, consulting with partners, delivering mitigation steps and documentation takes place throughout an issue's life cycle.

Microsoft prohibits retaliation against individuals who report workplace concerns or who participate in an internal investigation process. The no retaliation policy is communicated by the assigned investigator to the subject(s) of an investigation and/or key participants in the investigation.

The Microsoft Office of Health and Safety provides SafetyHUB on Viva Connections where employees can submit safety concerns or observations. Employees are encouraged to report any observations of unsafe conditions to SafetyHUB on Viva connections or by emailing globalohs@microsoft.com. Similar to REF, OHS maintains a website 'SafetyHUB SafetyHub | Global - Home (sharepoint.com) with information about reporting, emergency response and how to maintain a safe and healthy workplace.

Microsoft Global Security Corporate Investigation Procedures

Threat Management at Microsoft

Life Safety is the core priority for MSGS. GSI's primary mission is to **reduce Microsoft risk via identification, intervention, and mitigation of physical threats to persons and facilities.** In line with this mission, GSI maintains a robust threat management program where behavioral assessment, mitigation and partnering with stakeholders establish its foundation.

Microsoft has a Workplace Violence Policy (WVP) that can be accessed here: Workplace violence policy (sharepoint.com). The policy also includes a no retaliation provision.

To accomplish its mission, GSI established a Threat Management Program Methodology to identify, assess, and manage individuals or groups who may pose a risk of committing targeted acts of violence against Microsoft employees, contingent staff, guests, and facilities. GSI utilizes a structured, risk-based approach rooted in contemporary science and best practices of threat management.

The Microsoft Threat Management Methodology incorporates the following principles:

- The Threat Management Program must be defensible, consistent, and humane.
- It must be defensible, reflecting compliance with all applicable laws, regulations and policies governing Microsoft's global footprint to protect our company, stakeholders, and partners.
- It must be consistent in its application to protect the integrity of our investigations, reduce potential bias, and prevent negative outcomes.
- Lastly, it must be humane, treating the victims and subjects of threat investigations with dignity and respect to engender trust and reduce the potential for violent behavior.

The Threat Management Methodology is reviewed and updated on an ongoing basis to ensure industry best practice is reflected.

Microsoft Global Security hosts a website (Global Security - Home (sharepoint.com)) available to all staff with corpnet connection. The site offers a wide array of information surrounding security resources, reporting, physical safety tip/planning, trainings, security videos, online safety information, travel advisories, access related, country specific and security awareness information.

GSI leverages a 'toolbox' of capabilities designed to coach and empower staff who have reported a security-safety concern and to enhance security, as needed, at Microsoft sites. These tools include but are not limited to:

- Customized briefings to include security resources and safety planning tips to concerned parties (including sharing awareness documents that cover available security resources, safety planning tips, home safety information and online safety tips).
- Security escorts to/from a vehicle (at sites where available).
- Parking arrangements.
- Office door lock.
- Security Alert (shared with building lobby hosts and the security framework).
- Enhanced security presence and patrols (uniform, plainclothes).
- Badge trace and security response.
- Office move/directory removal.
- Armed security/protective assignments.
- Residential and non-work considerations.

GSI periodically meets with key stakeholder (CELA, WIT, GER, HR) teams to provide an overview of the threat management program and refresh on process, partnering, identifying behavioral concerns, and reporting considerations.

GSI has established formal reporting and response elements to support Security Assisted Terminations, Security Assisted Meetings and Reductions in Force. The process emphasizes early reporting to GSI, formal risk assessment, security process coaching and planning mechanisms to deliver capable and appropriate security support. The situation is assessed again post meeting for any ongoing concerns that may necessitate a threat management case assignment to an investigator.

Microsoft has a Domestic Violence provision on its Human Resources handbook (Domestic violence and crime victims (sharepoint.com)) site which outlines and offers support options. GSI partners with stakeholders on potential domestic violence matters to assess and mitigate workplace risk, offer Benefits support, and resource information. GSI collaborates with a police legal advocate on some cases as well. The legal advocate is versed in outside of work safety planning, court orders and domestic violence resources. The legal advocate can discuss with a concerned party as an option at the concerned party's discretion.

Record Keeping

Microsoft Global Security Corporate Investigation Procedures

Case Management System:

GSI documents investigative records in our case management system (CMS) called Perspective (PPM), which includes log entries listing relevant case information, updates and actions taken, and acts as a repository for relevant case documents/attachments.

Investigative Categories relevant to CA SB 553 exist within PPM's Life Safety classifications.

GSI's PPM documentation procedure requires Investigators to select from the below Categories when documenting a Life Safety incident. GSI Life Safety documentation is retained indefinitely in accordance with MS Data Retention policy (*GSEC2000-21-MSFT*). The Occupational Health and Safety group maintains Cal/OSHA Form 300 for 5 years.

The GSI Threat Management Methodology lists case management and case closure guidelines.

GSI Life Safety Categories include the following taxonomy:

911 Call	ETM - Inappropriate Communication	Life Safety - Other	Security Assisted Termination
Assault	Extortion	Medical	Stalking\Unwanted Pursuit
Bomb	Fire	Missing Person	Suicidal
Civil Unrest - Demonstration	Harassment	Natural Disaster	Threat
Death	Hazard	Robbery	Trespass
Domestic Violence	Hazardous Materials	Safety Issue	Weapons Violation
Duress	Kidnap	Security Assisted Meeting	Welfare Check

Annual Audit

This plan will be formally reviewed by the GSI Director of Investigations (Americas region), and/or their designee, on an annual basis. Program review and refinements will occur on an ongoing basis as our team culture emphasizes continual process improvement. Program review will include input and considerations brought forth by partners/stakeholders in the process, including staff who

have been involved/impacted (complainant, subject, witness, etc). Any deficiencies observed or learnings following an incident will be highly prioritized for reformation.

Microsoft has several avenues for identifying, reporting, and responding to unsafe workplace conditions. Site specific facilities contacts with our Real Estate & Facilities (RE&F) organization are onsite and typically well known to the employees at each site. They are primary contacts to monitor for concerns, schedule periodic inspections and/or receive reports of potentially unsafe conditions. RE&F also operates a website 'REFWeb (REFWeb - Home (sharepoint.com)) that offers robust services, reporting and facilities related information and request forms.

Microsoft's Occupational Health and Safety group has a process for periodic workplace inspections to identify unsafe conditions. They investigate all incidents or unsafe conditions reported by employees to determine root cause(s) and identify opportunities for improvement. The frequency of the inspections varies from monthly to annually based on the type of location and associated risks.

Some sites are staffed with physical security responders whose role is to observe and report any security or safety related concerns. Our Global Security Operations Center (GSOC) is also available (24x7) to receive, review and forward security-safety related concerns to the appropriate teams for response.

Document History

Change Description	Alias	Date
Document creation, review, and sign-off	Jpotts, eberb, kasigafo	TBD