AAMVA

American Association of
Motor Vehicle Administrators

Employee Safety and Security
Best Practices Guide

August 2026

MVA OPERATIONS AND CUSTOMER EXPERIENCE COMMITTEE

EMPLOYEE SAFETY AND SECURITY WORKING GROUP

Contents

Introduction: Building a Culture of Safety and Security

Motor vehicle agencies across North America occupy a unique and critical space at the intersection of public service and public safety. Every day, our employees engage with a complete cross-section of society, managing transactions that are fundamental to modern life. This role carries a dual mandate: to provide accessible, efficient service to the public while simultaneously protecting our people, our facilities, and the vast repositories of sensitive data entrusted to our care.

For decades, the approach to security in many service-oriented government agencies has been largely reactive, often consisting of a collection of policies and physical measures implemented in response to past events. Although these elements are important, they may no longer be sufficient to meet the dynamic and evolving threats of the modern world.

This best practice guide is built on a fundamentally different premise. It advocates for a proactive, holistic, and sustainable approach to safety and security that is rooted in a simple but powerful idea: the most effective measure any agency can implement is a deeply embedded culture of safety. This guide recommends considering organizational readiness, including staffing, to handle complex safety or security incidents and any new responsibilities involved.

A culture of safety is not a line item in a budget or a chapter in a manual; rather, it needs to be a shared belief, visible at all levels of an organization, that the safety and security of employees and the public is a core, non-negotiable value. It transforms safety and security from a set of rules to be followed into a collective responsibility to be embraced. The detailed strategies, procedures, and tactics outlined in the following chapters are the tools to build and sustain this culture. Your culture will only be effective if it is built on a solid foundation of intentional leadership and organization-wide commitment.

The Cornerstone: Intentional Leadership and Unwavering Commitment

A true culture of safety does not emerge on its own; it is intentionally designed, championed, and sustained from the very top of the organization. As leaders within your jurisdictions, your role is a critical factor in the success of all safety and security programs. This commitment is expected to be both visible and tangible, demonstrated through consistent action:

- **Visibly Champion the Program:** Leadership is encouraged to articulate a clear and firm policy toward workplace violence and communicate that the safety of every employee is a paramount priority.
- **Allocate Necessary Resources:** A commitment to safety should be supported to implement the program effectively. This includes funding for training, physical security upgrades, and the personnel needed to manage the program.
- **Establish Absolute Accountability:** Leaders are responsible for ensuring that all managers and supervisors are implementing and maintaining safety policies within their teams. Likewise, a clear, nonpunitive system ought to exist for employees to report concerns without fear of retaliation.

The Foundation: Empowering Employees as Active Partners

A culture of safety is built and maintained by the people who live it every day. Your frontline employees are not passive recipients of security policy; they are your most valuable asset and your first line of defense. They possess an unparalleled, ground-level understanding of the daily risks and the practical realities of the service environment.

By empowering your staff in the active and meaningful participation of your employees, you foster a sense of shared ownership and collective vigilance. This guide will repeatedly emphasize the importance of:

- **Training for Empowerment:** moving beyond compliance-based training to provide employees with the practical skills they need to feel confident and capable, especially in high-stress situations
- **Creating Clear Reporting Channels:** establishing simple, trusted, and well-publicized methods for employees to report hazards, suspicious activity, and security concerns
- **Fostering a "See Something, Say Something" Mindset:** actively promoting a culture where every employee feels responsible for their environment and is encouraged to speak up when something doesn't seem right

How to Use This Guide

The principles outlined in this introduction serve as the philosophical bedrock for the best practice guide. The subsequent chapters are structured to provide a practical, actionable roadmap for jurisdictions to build and mature their safety and security programs. We have organized this guide around the six-phase incident response lifecycle—**preparation, identification, containment, resolution, recovery, and lessons learned**—a framework recognized by federal agencies such as the National Institute of Standards and Technology (NIST) and Cybersecurity and Infrastructure Security Agency (CISA). It is important to note that progression through the security lifecycle is not determined by time intervals but rather by the immediacy and nature of the threat. A jurisdiction may move from *preparation* directly to the *containment* section within seconds or may cycle between phases multiple times during a single incident depending on the evolving situation.

This structure is intentional. It frames security not as a static end-state but as a continuous, cyclical process of improvement. Each chapter will provide your jurisdiction with the tools, strategies, and guidance needed to navigate that phase of the lifecycle.

Ultimately, this guide is more than a set of recommendations. It is a call to action for every motor vehicle administrator to make a deliberate and sustained investment in your people, your mission, and the public's trust. By fostering a genuine culture of safety and security, you create a resilient organization.

Chapter 1 Preparation

Preparation: Planning, Training, and Hardening

The preparation phase is the foundational stage of the security lifecycle. It encompasses everything a jurisdiction does before an incident occurs, mitigate its potential impact, and ensures an effective response when the incident does occur. Preparation, the guide's main focus, involves moving from reactive enforcement to proactive safety.

The goal of this phase is not to instill fear in the workforce but to empower staff with confidence, knowledge, and tools so they can respond calmly and effectively under stress. By establishing a comprehensive framework, agencies can build a *Culture of Safety* where security is viewed as a core component of customer service and employee well-being. For the purposes of this guide, preparation is defined as the proactive and continuous process of planning, training, and equipping jurisdictions and employees to recognize and respond to safety and security incidents.

The Security Management System and Threat Assessment Teams

Modern security requires moving beyond sporadic checklists to a cyclical, programmatic approach known as a Security Management System (SeMS). Adopting a SeMS is essential for shifting physical security from a reactive stance to a proactive, systematic discipline. Unlike traditional models that often wait for an incident to trigger a response, SeMS integrates security into the daily fabric of agency operations, establishing it as a regular and systemic part of agency culture rather than a static checklist. This methodology ensures that vulnerabilities are identified and mitigated prior to an incident through a proactive and continuous process of planning and assessment.

The SeMS methodology is widely accepted in large customer service operations and aligns with standards used in high-stakes environments such as aviation and public transit, as well as federal frameworks. By mirroring the principles of the National Incident Management System (NIMS) utilized by the Federal Emergency Management Agency, motor vehicle agencies (MVAs) adopt a common language for all emergency responders, facilitating seamless cooperation with law enforcement and fire services during a crisis.

A central pillar of SeMS is the establishment of a Threat Assessment Team (TAT), which is a multidisciplinary group of trained staff responsible for identifying, evaluating, and responding to behaviors or situations that may pose a risk to employees, customers, or facilities. Unlike reactive security models, the TAT operates proactively: gathering information, assessing the level of concern, and coordinating an appropriate organizational response before a situation escalates. In doing so, the TAT moves ownership of safety out of a single department and embeds it across agency leadership.

Effective TATs draw representation from diverse functional areas, typically management, human resources, workplace safety professionals, legal, and agency security or law enforcement partners. This cross-functional composition is intentional. Potential threats rarely announce themselves through one channel; warning signs often surface across departments, and no single function has the full picture. The TAT's role is to assemble that picture; determine whether a situation warrants action, monitoring, or no response at the

moment; and establishes clear procedures for sharing information in a timely and confidential manner. Balancing privacy obligations with the duty to protect staff safety is not a secondary consideration, but it is built into how the team operates.

Internal Threat Mitigation: Although much focus is placed on external dangers, agencies are responsible for preparing for internal threats. A robust SeMS includes policies to mitigate risks from within the workforce. This begins with rigorous pre-employment screening and background checks for all personnel. Furthermore, agencies should consider, whenever possible, policies regarding the presence of weapons on the premises, including specific regulations addressing weapons stored in employees' personal vehicles parked on state property. It is recommended that policy development in this area be conducted with your agency's legal counsel. All employees should be fully aware of all weapons related regulations and policies at all locations where MVA offices are established. Requirements may vary between MVA locations depending on leased facilities versus owned locations versus locations with specific restrictions such as college campuses and the like. It is also important for all agency third parties to report threats to the TAT. Third parties are defined as anyone who conducts business on the agency's behalf. This could be a county location partner or privately procured entity.

Ensure reporting mechanisms enable the TAT to identify employees showing signs of extreme volatility or violent behavior before incidents occur.

Warning signs may include:

- Extreme volatility or sudden behavioral changes
- Direct or veiled threats of violence
- Obsessive behavior toward coworkers, supervisors, or customers
- Marked decline in work performance coupled with withdrawal
- Extreme expressions of grievance or persecution
- Inappropriate interest in workplace security measures or previous violent incidents

The TAT should establish a confidential and expedient reporting pathway that allows supervisors and coworkers to share concerns without fear of retaliation. When the TAT identifies an employee of concern, they may provide direction to management, who are encouraged to work closely with internal partners to ensure that any monitoring or disciplinary action complies with employment law and collective bargaining agreements while prioritizing workplace safety. For high-risk terminations, such as employees who have made threats or exhibited volatile behavior, agencies should develop specialized protocols that may include:

- Coordination with internal security or law enforcement for the termination meeting
- Immediate revocation of building access and information technology (IT) credentials
- Escort from the premises
- Notification to security personnel and the TAT
- Follow-up monitoring for a defined period
- Consider if broader internal notification is appropriate

The Emergency Action Plan

Every agency is encouraged to develop and communicate a clear, written Emergency Action Plan (EAP) that covers plausible scenarios, with emphasis on those that are most likely to occur and those that have the most acute impact on customers, employees, or the jurisdiction. EAPs ensure that every employee understands their role during an incident. Your plan must be distributed effectively and stored electronically to make sure every employee knows where to find it and can access it remotely.

Developing and Validating the Plan: Creating a robust EAP is not a solitary task; it requires a collaborative approach that gathers input from a

diverse set of stakeholders. Internally, the planning team should include representation from executive leadership, human resources (HR), legal counsel, internal security, and frontline management.

Externally, agencies are responsible to coordinate with local law enforcement, fire departments, and emergency medical services during the design process. Sharing site plans and floor plans with local emergency responders ensures that the EAP is compatible with first responder protocols. These public safety partners should be invited to evaluate the plan, ensuring that the agency's internal procedures (such as evacuation routes or lockdown triggers) align with the tactical operations of arriving emergency units.

Scope of Awareness – Employees, Partners, and Contractors: The "scope of awareness" for the EAP needs to extend beyond direct government employees. It is critical that on-site contractors—specifically, other on-site workers such as security guards and janitorial staff—are fully versed in the plan. Janitorial staff are frequently the only personnel present after hours and may be the first to detect hazards such as leaking pipes or suspicious items. Similarly, co-located agencies or businesses within the same facility need to have access to relevant protocols to ensure a unified response to shared threats.

Essential Elements of the Plan: To be truly comprehensive, the EAP ought to go beyond general safety guidelines and detail specific response protocols. The plan should include distinct procedures for high-risk scenarios such as active shooter incidents, bomb threats, severe weather, medical emergencies, and hazardous materials exposure. Structurally, the EAP should clearly define:

- **Command and Control:** designating who has the authority to make critical decisions, such as triggering an evacuation or lockdown
- **Roles and Responsibilities:** specifying the duties of each employee type during an emergency to minimize confusion
- **Communication Strategies:** outlining how alerts will be disseminated to staff, customers, and external partners
- **Logistics:** including evacuation maps, shelter-in-place locations, and procedures for securing the building during off hours
- **Emergency Contact Lists:** comprehensive rosters, including TAT contacts, immediate response team members, local law enforcement liaisons, and emergency services coordination contacts

After-Hours and Radius Protocols: Security does not end when the doors close. The plan ought to include procedures, policies, and protocols for after-hours access control and monitoring. These procedures should identify how to handle emergencies that occur after hours. This includes a mechanism, such as a phone tree or automated mass notification system, to contact employees at home and inform them not to report to work if the facility is compromised. Furthermore, the agency must define the radius of concern. This geographic boundary determines when external incidents trigger protective protocols such as a lockout. Leadership is encouraged to decide in advance what proximity and what types of incidents warrant action.

For example:

- Does an active law enforcement pursuit within three blocks trigger a lockout?
- Does a bank robbery within a two-block radius automatically require a perimeter lockdown?
- What about civil disturbance or protest activity approaching the facility?

The radius of concern should be determined in consultation with local law enforcement and be based on the facility's urban or rural context, foot traffic patterns, and proximity to high-risk areas. Documenting these decision boundaries in advance removes hesitation during a crisis and ensures consistent application across shifts and leadership changes.

Continuous Evaluation and Improvement: The plan should be routinely subjected to annual or more frequent evaluation and revision. Agencies should conduct an after-action review following any drill or real-world incident to assess performance and modify training or procedures based on lessons learned. To prevent organizational blindness, agencies should consider inviting someone from an outside agency or another MVA site to observe drills and provide objective feedback on the plan's effectiveness.

Standardizing Terminology: Locks, Lights, and Perimeters

A critical failure point in many emergency responses is confusion over terminology. To ensure a cohesive response, the EAP is responsible for clearly defining and distinguishing between different protective postures. Although MVAs can offer direction in such scenarios, each individual ultimately has the freedom to decide how to ensure their own safety.

A **lockdown** is a protocol reserved strictly for internal threats, such as an active shooter or an individual wielding a weapon inside the facility. The mnemonic for this protocol is "Locks, Lights, Out of Sight". During a lockdown, all interior movement ceases, and staff and customers barricade themselves in secure rooms.

A **lockout (or secure)** acts as a countermeasure for external threats. This protocol is triggered by events such as civil disturbance, police activity in the immediate vicinity, or a threat outside the building. In a lockout, the exterior doors are locked to secure the perimeter, but business may often continue inside the facility.

Shelter in place is distinct from security threats and is used primarily for environmental hazards. This includes severe weather events such as tornadoes or external hazardous material (hazmat) clouds. In these instances, the protocol directs staff and the public to move to designated interior safe rooms, basements, or hardened spaces away from windows. These locations must be clearly identified and communicated in advance.

Comprehensive Scenario Planning

The EAP needs to be a living document that addresses a wide spectrum of risks. Beyond the active threat scenarios, the plan should detail responses for medical emergencies, bomb threats, and suspicious packages. It is expected to also account for infrastructure failures, such as power outages, gas leaks, or proximity incidents that could block access to the facility.

Communication is the lifeline of the EAP. Agencies ought to determine how they will be notified of external threats, whether through city or county emergency notification systems, social media, or direct observation. Internally, the plan is encouraged to strengthen and test communication systems, including panic buttons, intercoms, chat groups, phone trees, and desktop emergency notifications. It is essential that staff understand exactly what panic buttons do, when to activate them, who is notified upon activation, what to do while the response is still in progress, and what the expected response time is.

The 911 Protocol: A common failure during emergencies is the bystander effect, in which employees assume someone else has called for help. The EAP needs to explicitly state that *any* employee who witnesses a life-threatening emergency is authorized and expected to move to a safe location and call 911 immediately. The protocol is responsible for training staff to provide specific details to dispatchers. The plan ought to detail when and how to notify employees and customers who may otherwise be unaware of an unfolding event. This quick action can maximize safety and well-being.

Telecommunication During Emergencies: CISA has a program for you to connect to the Government Emergency Telecommunications Service (GETS). This allows you to have priority status to phone lines

during an emergency when the telecommunication system is at capacity for local and long-distance calls: www.cisa.gov/gets.

Rally Points and Accountability: The EAP needs to designate specific rally points—locations at a safe distance from the building where staff congregate for a headcount. These points need to be far enough away to ensure safety from potential hazards. Agencies should designate both a primary and a secondary rally point. The secondary location serves as an alternate gathering site if the primary rally point becomes unsafe because of environmental factors, proximity to an active threat, or other evolving conditions. Rally points should be reviewed periodically to ensure they remain valid over time. To facilitate clear communication during chaotic moments, agencies should establish and drill plain language protocols, code words, or distinct alarm tones that signal specific actions.

Physical Hardening and Crime Prevention Through Environmental Design

The physical environment should be designed to deter crime and facilitate safety through the principles of Crime Prevention Through Environmental Design (CPTED). This approach uses the designed environment to influence behavior and reduce the opportunity for crime.

Access and Visibility: Natural surveillance is a key CPTED principle. Office furniture and workstations should be arranged to maintain clear lines of sight, especially from supervisors or team-lead offices, which should have visibility of the lobby or main entry point.

Access controls are expected to be strictly enforced, with clear distinctions between public zones and "employee only" areas, secured by badge access or keycards. To prevent unauthorized entry through tailgating, when unauthorized individuals follow authorized personnel through secure doors without proper credentials, agencies should ensure separate employee and customer entry and exit points are available. The information desk should be positioned near the primary public entrance to ensure all visitors are seen and directed appropriately on arrival. Staff should be trained to interact with tailgaters and direct them to the correct public entry.

Visual Deterrence and Surveillance

Physical security relies heavily on the psychological perception of control. A "hardened" target is one where potential aggressors perceive a high risk of detection and intervention. This begins with clear, authoritative signage. Signage serves as the first layer of verbal de-escalation by setting behavioral expectations before a customer ever reaches a service counter. Perimeter signage indicating "Restricted Access," "Video Surveillance in Use," or notices of customer conduct expectations removes the excuse of ignorance and legally positions the agency to take enforcement action if policies are violated.

Inside the facility, signage should clearly identify "employee only" zones, reinforcing the territorial boundaries established by the office layout. Agencies should also post notices regarding recording policies in public areas. Signage should inform customers that video surveillance is in use for security purposes and that the facility is a public space. Where state law requires two-party consent for audio recording, signage needs to clearly indicate whether audio is being captured.

Beyond static signs, the strategic placement of security assets creates a dynamic deterrent. If security personnel or uniformed law enforcement are present, they should not be relegated to a back office or a low-visibility corner. Instead, they should be positioned in high-traffic areas to establish an immediate presence of authority. Similarly, video surveillance cameras should be positioned overtly rather than covertly. Although cameras serve an investigative function for gathering evidence, their primary role in the preparation phase is deterrence. Cameras should be visibly installed in lobbies, interaction zones, and parking areas to signal to the public that the environment is actively

monitored. The use of "public-view monitors"—screens facing the public where customers can see themselves being recorded—is a proven tactic to increase self-awareness and reduce aggressive behavior.

Exterior and Site Security

The security of the facility extends to the perimeter. Landscaping should be maintained to support safety; trees should be trimmed to maintain sightlines, and low-growing vegetation should be used near windows to eliminate hiding spots.

Lighting is equally critical for both during and after-hours safety. Parking lots and pathways should be illuminated with consistent lighting to eliminate shadows and deter criminal activity. Agencies should consider motion-activated or photocell-controlled lighting systems that automatically adjust to changing daylight hours and increase illumination when human activity is detected in specific zones.

To protect against vehicle-borne threats, agencies should install crash-rated bollards or hardened planters at building frontages and high-traffic pedestrian areas. These physical barriers prevent vehicle ramming attacks while maintaining a welcoming appearance.

Interior Defensive Design

Beyond the lobby, and where possible, the interior workspace should be designed with defensive capabilities. A secure help room should be designated in restricted areas where staff can retreat if a threat breaches the counter line. This room requires a reinforced door with a deadbolt that cannot be breached from the outside. The secure help room should be in an employee-only area, ideally positioned to allow quick access from customer service stations while remaining invisible to the public. For larger facilities with multiple service areas or floors, agencies should consider designating multiple secure rooms to ensure staff are never more than a short distance from safety. Inside this room, agencies should install a hardline landline phone to ensure communication remains possible even if the building's VoIP or web-based systems fail because of power or network outages. The room should also contain a copy of the EAP, a first aid kit, and emergency contact information.

Furniture selection is also a component of safety. In high-interaction zones, agencies should prioritize heavy, sturdy furniture that is anchored or difficult to lift, preventing chairs or tables from being used as projectiles during a violent outburst.

Daily Security Protocols: Physical security relies on daily discipline. The EAP should mandate a "closing sweep" protocol when designated staff inspect the entire facility, including restrooms, storage closets, and corners, at the end of every business day to ensure no unauthorized persons remain in the building.

Additionally, fire safety protocols needs to be strictly enforced regarding personal appliances; policies should explicitly regulate or ban the use of space heaters and candles, which serve as common ignition sources. Encourage staff to use a buddy system or have a process in place if an employee leaves the site alone.

Training and Exercises

Training is the engine of preparedness. A plan is only as effective as the staff's ability to execute it under stress. This section outlines the training cadence, curriculum requirements, and evaluation protocols necessary to build competence and confidence across the workforce.

De-escalation Training

All customer-facing staff should receive comprehensive training in verbal de-escalation. Although AAMVA does not endorse a specific de-escalation training program, options that may fit your jurisdiction's needs are widely available. Effective training emphasizes active listening and empathy; maintaining a calm tone and nonthreatening body language; offering choices and collaborative problem solving; and critically, recognizing

when to disengage and seek assistance. Safety always takes precedence over transaction completion.

Emergency Action Plan Training

Your EAP is expected to be practiced ensuring effectiveness. Table-top exercises, scenario discussions, and running active drills provide opportunities for staff to learn through action and better prepare them for an active incident.

Safety Awareness Training

Formal "If You See Something, Say Something®" programs encourage staff to report suspicious behavior without fear of overreacting. Basic training should cover how to use the reporting system, when to report, and what information should go into the report. Include data and information gathered from your jurisdiction to help reinforce the importance of reporting safety and security risks.

Life-Safety Training

The curriculum ought to expand beyond safety and security threats to include life-safety skills. Agencies should consider providing training in cardiopulmonary resuscitation (CPR), first aid, and use of naloxone (ex. Narcan) and automated external defibrillators (AEDs).

Training Cadence: To ensure consistency, safety orientation ought to be a mandatory component of onboarding for every new hire. However, memory fades over time; therefore, the agency is responsible for instituting a minimum annual refresher training for all staff to review emergency codes, evacuation routes, and lockdown procedures.

Training builds the muscle memory required to act when the brain is under stress. Agencies are encouraged to train staff on all emergency protocols, with a specific focus on the "Run, Hide, Fight" model recommended by the U.S. Department of Homeland Security (DHS).

This training should not be static; it requires role-playing and scenario-based discussions to help staff understand how to use verbal techniques and de-escalation training to defuse volatile situations before they become physical. If this fails, employees need to understand when to evacuate (run), when to barricade (hide), and when to incapacitate an attacker as a last resort (fight).

Drills and Evaluation: Agencies should conduct emergency drills yearly as a minimum; quarterly is recommended given turnover rates. Exercises are expected to be diverse, and the content should rotate through various scenarios, including severe weather sheltering, medical emergencies, bomb threats, and family reunification procedures. Active shooter drills should be scheduled similarly and with the same regularity as fire or tornado drills, ensuring knowledge is refreshed frequently.

These exercises should test not only the lockdown mechanics but also the communication systems, accountability procedures, coordination with external responders, and follow-up activities. Drills provide the opportunity to identify and improve weaknesses in the plan.

Following every drill or real incident, an after-action review needs to be conducted to assess performance. This review identifies flaws or gaps in the procedure and allows the agency to modify training or protocols accordingly. To prevent organizational blindness, agencies should consider bringing in observers from outside agencies or other MVA sites to provide objective feedback that internal teams might miss.

This continuous cycle of planning, training, drilling, and revision forms the core of the SeMS. By committing to this iterative improvement process, MVAs can build a culture of preparedness that ensures the safety of both their public servants and the communities they serve.

Chapter 2 Identification (Detection and Analysis)

The identification phase is the process of observing, recognizing, and reporting warning signs of a potential security incident or escalating situation. This phase is critical to effective incident management at MVA facilities. Early detection allows staff to respond appropriately, potentially de-escalating situations before they become critical.

Effective identification requires trained and observant staff, clear recognition of warning signs, and established reporting protocols. This chapter provides MVA administrators with best practices for developing robust identification capabilities across their organizations.

Recognizing Early Warning Signs

Behavioral Indicators of Potential Violence

Staff should be trained to recognize behavioral warning signs that may indicate a potential security incident. Agitation and escalating anger often manifest through using a raised voice, aggressive posture, pacing, clenched fists, or rapid breathing. Verbal threats, whether direct or implied, represent clear warning signs requiring immediate attention. Drastic behavioral changes, such as sudden shifts from calm to aggressiveness, can signal an individual approaching a critical threshold.

Other concerning behaviors include obsessive focus on a single grievance despite staff attempts at resolution, intimidation tactics such as invading personal space or blocking exits, and signs of intoxication or impairment that may indicate unpredictable behavior and reduced impulse control.

The Pathway to Violence

Violence is often a process rather than a spontaneous event. The pathway typically involves observable stages: grievance development, when an individual perceives a wrong; ideation, when thoughts of violence emerge as a solution, planning, and preparation, including research and acquisition of means; and finally implementation of the violent act. Staff trained to recognize these stages can intervene early, often preventing escalation through appropriate responses and referral to supervisors or security personnel. Violence rarely appears without warning; observable precursors provide opportunities for protective interventions.

Identifying Specific Service Disrupters

First Amendment Auditors

Individuals may exercise their rights to free speech and freedom of the press by recording and documenting interactions within public spaces. Such individuals frequently visit government buildings to assess permissible activities and establish boundaries. Your legal team will help you in drafting a policy specific to your jurisdiction for recording in MVA spaces. This policy ought to be shared with all staff and procedures implemented when identifying this type of interaction.

Pseudo-Legal Ideology Groups

MVA employees frequently encounter individuals affiliated with anti-government, pseudo-legal, and other extremist organizations. These individuals operate under complex and contradictory interpretations of legal and historical texts, asserting independence from government jurisdiction. They fundamentally reject government authority, including

licensing and registration requirements, relying on obscure legal arguments that sound sophisticated but lack actual legal foundation.

Recognizing Pseudo-Legal Documents

At a high level, these obscure legal arguments are more magic than law. When presented with unusual documentation, staff should be able to identify potential pseudo-legal materials. The document may involve a legitimate MVA transaction that can be processed, but many requests from pseudo-legal ideology groups do not involve legitimate MVA transactions.

These documents typically exhibit distinctive hallmarks. References to individuals as "vessels" appear frequently, based on misapplication of admiralty law. Inappropriate use of legal terminology from copyright law, secured party status, or the Uniform Commercial Code demonstrates fundamental misunderstanding. The formatting itself is often distinctive: names written in all capital letters or with unusual symbols, use of specific ink colors (particularly red) or biological materials such as blood or hair, and postage stamps placed in unusual locations.

Certain phrases serve as immediate identifiers, including "without prejudice" or "without recourse," references to laws or court cases from the 1800s or earlier, citations from religious texts used as legal authority, and assertions that silence equals consent. An example document is provided in the Appendix with reference to number in the text.

Best Practices for Handling Pseudo-Legal Documents

When receiving a pseudo-legal document, accept it while maintaining professional courtesy. Avoid arguing legal interpretations with the customer. Document receipt by scanning the document into the records management system with notation of date and time received. In most cases, take no further action because most pseudo-legal requests do not involve legitimate MVA transactions. If uncertain, route materials to legal or supervisory personnel for review. Accepting a document does not obligate the MVA to act based on its contents. If a legitimate MVA transaction is embedded within pseudo-legal materials—such as a valid title transfer accompanied by pseudo-legal documents - the agency may conduct that legitimate transaction while disregarding the invalid documentation.

Operational Prevention: Reducing Friction Points

Security begins with operations. Before a customer becomes a threat, they most likely are seeking service. A sophisticated identification strategy includes proactive assessment of operational factors that may contribute to escalation.

Identifying Friction Points

Friction points are moments in the customer experience that induce stress, confusion, or anger, often serving as the genesis of escalation. Common friction points include unclear queueing systems that cause customers to wait in wrong lines ; lack of transparency around wait times, creating anxiety; confusing signage or processes, leading to repeated visits; document confusion; inadequate staffing during peak times; inconsistent information from different staff members; and limited-service channels, forcing all customers through identical processes regardless of transaction complexity.

Operational Strategies to Minimize Escalation

Greeter stations quickly guide customers to the right service lines and direct upset individuals to experienced staff. Transparency through displayed wait times, clear pre-arrival information about required documentation, and multi-channel communication creates realistic expectations. The physical environment significantly impacts customer stress; comfortable seating, clear signage, adequate climate control and lighting, access to restrooms and water, and effective noise management all prevent escalation before it begins.

Regularly surveying customers and staff to identify emerging friction points, combined with analysis of complaint data and incident reports, reveals systemic issues addressable through operational changes, training, or facility improvements.

Recognizing Channel-Specific Escalation

Escalation occurs across multiple channels with distinct indicators. In-person escalation manifests through physical aggression indicators, voice volume and tone changes, and visible emotional dysregulation. Telephone escalation includes increasingly aggressive or profane language, repeated calling, and threats directed at staff or facility. Written communication through email, mail, or social media can escalate with threatening or obsessive language, excessive correspondence on the same issue, and publication of staff names or facility information with negative intent. Staff should recognize escalation patterns specific to each channel and understand that threats made by phone or email are no less serious than those made in person.

Reporting and Communication Protocols

Internal Reporting Systems: Establish clear, simple mechanisms for staff to report concerning behaviors or incidents. For immediate threats, protocols should emphasize calling 911 and then urgent direct supervisor notification and security contact. For non-urgent concerns, an incident reporting system with designated review personnel, including TAT, allows tracking and pattern recognition. Anonymous reporting options serve situations when staff may be uncomfortable with direct reporting.

Information Sharing: Develop protocols for sharing concerning information quickly and accurately across your agency. This will better assist you in identifying potential areas of risk.

Documentation Standards: All observations and reports should include date, time, and location of the incident, detailed descriptions of behavior or documentation observed, names and descriptions of individuals involved, actions taken by staff, and any witnesses.

Thorough documentation supports pattern recognition across multiple encounters, provides legal defensibility, and enables continuous improvement of security protocols. **Key Principles for Effective Identification:** Several overarching principles should guide MVA organizations. First, recognize that anyone is capable of concerning behavior; challenging situations can arise from any demographic group or transaction type. Second, early intervention is key; the earlier a concerning situation is identified, the more options exist for resolution. Third, trust staff instincts. Frontline staff often detect concerning patterns before they can be formally categorized. Fourth, context matters profoundly.

Consider operational factors that may be contributing to customer frustration rather than viewing every agitated customer as a security threat divorced from circumstances.

Finally, identification skills degrade without regular reinforcement. Continuous training is essential because threat recognition requires ongoing exposure to scenarios and regular refresher training to maintain effectiveness. By building robust identification capabilities grounded in these principles, MVA organizations create the foundation for effective incident management and a safer environment for both staff and the public they serve.

Chapter 3 Containment Through Activation of Emergency Action Plans

After an incident is identified, the immediate goal is to prevent it from spreading or worsening. Containment focuses on limiting the incident's impact through rapid, appropriate response. The nature of containment varies significantly based on the type and severity of the incident.

Effective containment requires pre-established protocols, trained staff who understand their roles during emergencies, and clear communication systems. The containment phase bridges identification and recovery, determining whether an incident remains a manageable disruption or escalates into an active incident. Although this chapter outlines the principles and frameworks for containment, detailed incident-specific protocols are provided in the appendices for quick reference during actual emergencies.

The Containment Continuum: Matching Response to Threat Level

Containment exists along a continuum from minimal intervention to maximum response. Understanding where a situation falls on this continuum allows staff to deploy appropriate containment measures without underresponding to serious threats or overresponding to situations that can be managed with less intensive interventions.

At the lowest level of the continuum, verbal de-escalation represents the most desirable form of containment when circumstances permit its use. Moving up the continuum, situations may require management intervention, temporary service suspension to specific individuals, or redirection of customer flow to isolate problems. At higher levels, containment may involve activating panic alarms, calling law enforcement, or implementing facility lockdown procedures. At the highest level, active threat situations require immediate evacuation or shelter-in-place responses that prioritize survival over all other considerations.

The key to effective containment is accurate assessment of threat level combined with swift deployment of the appropriate response. Staff trained in both identification and containment can make these critical decisions rapidly, understanding that the goal is always to use the minimum necessary force while ensuring safety.

De-escalation as Verbal Containment

The application of de-escalation techniques represents a form of verbal containment designed to stop a conflict from escalating. When staff identify early warning signs of escalation as described in Chapter 1, immediate deployment of de-escalation skills can contain the situation before it requires more intensive interventions. De-escalation should always be the first response when the situation permits because it resolves conflicts while maintaining dignity for all parties and preserving the customer relationship.

Critically, staff should be able to recognize when de-escalation is not appropriate for the situation or when the threat is considered immediate. If a customer exhibits signs of imminent violence, if the customer is significantly impaired by substances, or if the situation is deteriorating despite de-escalation attempts, staff should disengage immediately and activate emergency protocols. The transition from verbal containment to emergency response needs to be swift and decisive.

Emergency Response Activation

When de-escalation is unsuccessful or when facing immediate threats, staff must know how to effectively activate emergency services. Calling 911 represents a critical containment action that brings professional emergency responders to manage situations beyond staff capacity. Beyond the external 911 call, follow your EAP on additional notifications to management, staff, and customers.

Active Threat Response: Run, Hide, Fight

"Run, Hide, Fight" is the recommended action in an active threat situation, specifically when active shooter, armed intruder, or other imminent violence is occurring. This protocol allows individuals to make rapid decisions based on their specific circumstances until law enforcement is able to intervene. See the index or appendix for the Run, Hide, Fight protocol.

When Law Enforcement Arrives

When law enforcement personnel arrive, staff needs to understand that officers' first task is to end the incident and defuse the situation appropriately. Staff should always keep their hands visible and empty when encountering law enforcement, raising them immediately when officers appear and following commands without delay or discussion. Officers responding to active threats operate under extreme stress and cannot always distinguish between victims and threats without clear behavioral signals. Following law enforcement instructions precisely and evacuating in the direction indicated ensures safety for staff, customers, and first responders.

Operational Disruptions

Not all containment situations involve direct threats to people. Operational disruptions including power outages, facility damage, and IT system failures require different containment approaches focused on maintaining essential services while managing the disruption. Protocols for managing service disruptions include containment actions such as closing specific service areas, redirecting customer flow to isolate problems, or temporarily suspending non-essential functions to maintain core services.

During operational disruptions, clear communication with customers becomes critical. Transparent communication reduces frustration and allows customers to make informed decisions about whether to wait, use alternative channels, or reschedule. Internal communication ensures staff understand their modified roles during disruptions and know how to direct customers appropriately.

Detailed protocols for specific operational disruptions, including power outages, facility loss, and IT system failures, are provided in Appendix B.

Incident-Specific Protocols: A Reference Framework

Although the principles outlined in previous sections apply across incident types, specific incidents require tailored responses. MVA facilities may encounter robbery attempts; medical emergencies, including drug overdoses; physical attacks; bomb threats; fires or explosions; suspicious packages; situations involving restraining or trespassing orders; and various other security incidents. Each incident type has distinctive characteristics requiring specific response protocols.

Rather than attempting to memorize detailed protocols for every possible incident, staff should understand the general framework: assess the immediate threat level, ensure personal safety first, activate appropriate emergency response through 911 or internal protocols, contain the situation by limiting its spread or impact, document and preserve digital evidence thoroughly after the incident is resolved, and provide appropriate notifications to supervisors and incident response teams.

Detailed incident-specific protocols are provided in Appendix A, organized alphabetically for quick reference during actual incidents. These protocols provide guidance for what actions to take until first responders assume responsibility.

Communication During Containment

Communication during incidents operates on multiple levels simultaneously: immediate tactical communication among staff responding to the incident, notification communication activating TATs and emergency services, internal communication informing all facility staff of the situation and appropriate actions, and external communication managing public information and media inquiries.

Immediate tactical communication during incidents should be clear, brief, and specific. Staff should use plain language rather than acronyms that may be misunderstood under stress. Panic alarms and emergency notification systems supplement verbal communication, ensuring messages reach all staff even in noisy environments or when verbal communication is impossible.

Designated communication officers manage media inquiries, public notifications, and external stakeholder updates. Only designated spokespersons should communicate with media to ensure message consistency and accuracy. All other staff should politely redirect media inquiries to official spokespersons. Appendix D includes communication plan templates for various incident types.

Specialized Situations and Delivering Services Offsite

Certain situations require specialized consideration beyond standard incident protocols. Staff who work alone at single-person facilities or during mobile outreach events may face difficulty immediately calling for help or cannot rely on other staff for assistance. Protocols for working alone should include regular check-in with supervisors, panic alarm systems that function in remote locations, and situational awareness training. Detailed guidance for working alone and mobile operations is provided in Appendix C. When serving homebound individuals, it is advisable for two employees to visit the residence accompanied by security or local law enforcement. In most areas, a physician's or healthcare professional's note is required to provide home services. It is important for all employees to run through emergency situations and have a safety plan before deploying services offsite.

Conclusion

Through the principles outlined in this chapter—matching response to threat level, prioritizing life safety, communicating clearly during an incident, and taking informed, decisive action apply across all incident types—MVA organizations can ensure that when incidents occur, containment actions are swift, appropriate, and effective in protecting both staff and the public they serve. The transition from containment to recovery begins when incidents no longer pose an active threat.

Chapter 4 Resolution

After the incident is contained, resolution begins with managing the immediate aftermath. This phase may be led by law enforcement or emergency services, with employees supporting professional responders and preserving critical information.

Resolution marks the transition from active emergency response to stabilization. This chapter clarifies the essential but supporting role MVA employees play during resolution: cooperating with law enforcement, preserving evidence, providing accurate information, and preparing for recovery.

The Resolution Framework

Resolution involves several key activities that distinguish it from both containment and recovery. It is possible that the threat is contained before law enforcement arrives on scene and MVA staff will begin the resolution phase. After law enforcement or emergency services arrives and assumes command of the scene, they will direct all activities.

Emergency medical services triage and treat injured persons. The scene is secured to preserve evidence. All personnel are accounted for. Initial damage assessment begins. Finally, the transition to recovery operations commences as responders complete immediate work and begin releasing portions of facilities. Understanding these activities helps staff recognize what is happening during this overwhelming period and helps them cooperate effectively. In the event of a natural disaster or emergency, local law enforcement or other first responders may not be activated or available. Therefore, MVA leadership may be tasked with some of these responsibilities. The detailed Resolution Action Plan in Appendix F provides step-by-step guidance for various incident types, recognizing that not all steps apply to every situation.

Providing Critical Information

When officers indicate readiness for information, provide intelligence that helps assess the current environment.

Deliver information in brief, factual statements. Avoid lengthy narratives, speculation, or emotional reactions during active response. As situations stabilize, officers will collect detailed witness statements. Preserve observations mentally, noting exact sequences, specific words, precise actions, and evidence locations. Write notes if materials are available because memory fades rapidly after an incident occurs.

Understanding Law Enforcement Priorities

Law enforcement priorities follow a clear hierarchy. The first priority is always stopping active threats. Officers will bypass injured people and ignore property damage to reach and neutralize threats. This prevents additional casualties. After threats are neutralized, priorities shift to emergency medical care, scene security, personnel accountability, witness interviews, and finally releasing uninvolved persons. Do not interpret focus on threat neutralization as indifference. Officers are minimizing total harm.

When Fight Response Successfully Neutralizes a Threat

Cease the use of force immediately after the threat has been disabled. Contact emergency services (911) if this has not already been done and provide a clear statement indicating that the threat has been

neutralized but remains present. Do not move or handle any threats or weapons unless necessary to maintain safety. Because employees might not be comfortable handling weapons, it's important to have clear expectations and a plan for their roles in these situations. Maintain the integrity of the scene and carefully preserve your recollection of events because you will be required to deliver a comprehensive account of the incident. If capable, administer first aid. Please note that individual circumstances may differ, and this guidance does not replace live training with qualified law enforcement professionals. It is important to understand your jurisdiction's sovereign or good Samaritan laws for these situations.

Scene Security and Evidence Preservation

When the incident is over, securing and preserving the scene become the priorities. Law enforcement may lead this activity.

Employee Responsibilities

Respect perimeters established by law enforcement or MVA leadership. Do not attempt to retrieve personal belongings, check on facilities, or satisfy curiosity. Items inside perimeters will be returned when the investigation permits. Do not touch, move, or alter anything within secured areas unless specifically directed by law enforcement or MVA leadership. Items that seem insignificant may provide critical evidence, including fingerprints, DNA, ballistics, video recordings, documents, and physical traces. If you notice evidence could be lost, contact law enforcement instead of trying to preserve it yourself. Leave immediately if the site is damaged or unsafe. Do not attempt to assess damage or secure evidence if safety is a concern. Preserve your own clothing and personal effects if you had contact with threats, were injured, or may have transferred evidence.

Financial Assets and Sensitive Materials

Cash, inventory, and customer records within incident scenes cannot be removed for safekeeping. Management should work with law enforcement to develop protocols for securing these materials while maintaining scene integrity.

Accountability and Witness Management

Accounting for all personnel ensures no one remains in danger, identifies potential witnesses, helps law enforcement rule out additional threats, and allows organizations to support affected employees and notify family members.

Accountability Process

Facility managers or designated coordinators work with law enforcement using sign-in logs, appointment schedules, and employee rosters. However, these systems may be incomplete. Physical facility searches, emergency contact calls, and careful documentation contribute to complete accountability. Immediately respond to calls or texts from supervisors confirming your safety and location. If unable to respond because of being with law enforcement or emergency services, respond as soon as possible.

Employees who evacuated or were offsite should also confirm their status.

Witness Management

Law enforcement will interview witnesses before releasing them from scenes unless medical treatment is required. This timing preserves memories because crucial details may be lost within hours.

Cooperate fully, providing truthful and complete information. Say "I don't know" or "I don't remember" rather than guessing. Do not discuss incidents with other witnesses before providing statements because this contaminates independent memories.

Coordination Between Leadership and Public Safety

Liaison Functions

Your EAP will identify who will serve as law enforcement liaisons. Facilitate law enforcement access to information systems, video surveillance, access logs, and other organizational resources. Advocate for organizational needs, including operational timelines and employee welfare. Manage information flow between public safety officials and organizational leadership.

Media Management

Whereas law enforcement typically leads media communications regarding criminal investigations, organizational communications officers handle operational information. Coordinate to ensure parallel communication efforts do not contradict each other or release confidential information. Direct all media inquiries to designated communications officers who coordinate with law enforcement before releasing information.

Initial Damage and Impact Assessment

As facilities are released from law enforcement control, initial assessment informs immediate transition to recovery operations.

Assessment Areas

Physical Damage: Document structural damage, equipment damage, inventory damage, and environmental contamination. Determine if facilities are safe for occupancy and identify immediate risks requiring mitigation.

IT and Data Systems: Determine if systems are functional, if data have been compromised or lost, if security has been breached, and if systems can be safely reactivated or require forensic analysis.

Financial Impact: Assess lost revenue during closure, emergency response costs, immediate security enhancements needed, and preliminary insurance notifications.

Employee Impact: Identify employees directly involved, those requiring immediate medical or psychological care, those whose work locations are inaccessible, and those needing modified assignments.

Customer Impact: Identify customers present during incidents, those with affected appointments or deadlines, and those whose transactions were interrupted.

Document all assessment information systematically and share with MVA response teams to inform decision-making processes. Initial assessments will be refined during the recovery phase as more complete information becomes available.

Transition to Recovery Operations

Resolution concludes when law enforcement releases scenes, all personnel are accounted for, witnesses have provided initial statements, threats are fully neutralized, and damage assessment provides sufficient information to begin planning recovery. The transition is gradual, with different aspects released at different times.

Formal Transition

Law enforcement incident commanders officially release scene control to MVA leadership. This may be partial or complete. Check with law enforcement before occupying facilities or resuming operations.

Immediate Actions Upon Scene Release

If facilities were evacuated, manage re-entry carefully with initial entry by security or facilities staff to assess conditions and identify hazards. Communicate facility status, return-to-work procedures, and available support services and implemented changes to

employees. Inform the public about service availability, procedural changes, and contact information. Implement temporary security enhancements if incidents revealed vulnerabilities. Arrange environmental remediation if biological hazards exist. Conduct preliminary debriefings with response teams and TAT if applicable. Compile and organize documentation of all resolution-phase activities.

The transition represents a shift from emergency response led by law enforcement to restoration led by the organization. Understanding this shift helps organizations transition effectively, neither rushing back to operations prematurely nor prolonging emergency response unnecessarily.

Legal and Administrative Considerations

The resolution phase involves numerous legal and administrative considerations requiring careful attention.

Evidence Preservation: Organizations have obligations to preserve evidence for law enforcement investigations, civil litigation, insurance claims, regulatory inquiries, and internal investigations. Formal evidence preservation policies should be activated immediately and maintained throughout resolution and into recovery. Follow your internal counsel's direction.

Employee Rights: Employees have rights to legal representation and fair treatment.

Workers' Compensation: Injuries sustained during workplace incidents are generally compensable. Suggest that injured employees receive appropriate care. All parties are aware of their respective responsibilities and obligations, and everyone involved has been informed.

Insurance Notifications: Most insurance policies require prompt incident notification. Notify insurance carriers during resolution, providing preliminary information about what occurred and resulting damages or injuries.

Regulatory Reporting: Certain incidents may trigger mandatory reporting to federal, state, or local agencies. Consult legal counsel to identify applicable obligations and ensure compliance with required timelines.

Conclusion

Resolution represents the critical bridge between emergency response and return to normal operations. Employees play an essential supporting role, cooperating with law enforcement, preserving evidence, providing accurate statements, and maintaining accountability.

The duration and complexity of resolution vary dramatically. As resolution concludes and facilities can be reoccupied, the focus shifts to recovery, which will address restoration of normal operations, comprehensive employee support, facility repair and enhancement, financial recovery, lessons learned processes, and policy updates.

The detailed Resolution Action Plan in Appendix F provides step-by-step guidance that jurisdictions can customize for their specific needs, ensuring that when resolution becomes necessary, employees understand their critical supporting role and can execute it effectively.

Chapter 5 Recovery

Immediate Recovery

Recovery typically begins after first responders have released control of the scene or local leaders have given the signal that recovery efforts can begin. This phase of the incident cycle may coincide with the resolution phase. Leadership must establish clear command and communication by designating a point person or team of people to oversee decision making for MVA options. Instructions should be communicated using clear, calm, and direct language, and only verified information should be shared to prevent misinformation or panic.

Customer and Community Recovery

Following an event, organizations should prioritize clear, timely communication with customers and the broader community about service disruptions, facility closures, and safety protocols being implemented to protect the public. All external communications should be consistent with established agency policies and approved communication procedures. Messaging should be transparent, empathetic, and focused on what the public can expect during the recovery period. When appropriate, coordinate with local authorities, partners, and community leaders to ensure consistent and accurate information. Ongoing communication throughout the recovery process supports public confidence, reinforces accountability, and demonstrates a continued commitment to community safety and well-being.

Leadership Responsibilities During the First One to Five Days

The period immediately following an active incident plays a critical role in shaping employee recovery, organizational stability, and trust in leadership. On the first day, leaders should focus on stabilization of physical assets and the support of people. Leadership should issue a clear and compassionate statement acknowledging the incident and reaffirming the organization's commitment to safety and security. Activate employee assistance programs and mental health resources early and promptly review facility assets to assess operational readiness.

During days two and three, leadership should maintain transparency through regular updates, even when information is limited. An assessment of operational disruptions should be continued, and planning for a phased return to normal operations should begin when feasible. Check your EAP to see whether you need to activate backup locations, alternative customer delivery methods, or additional staffing. Managers are encouraged to check in with employees individually or in small groups to listen to concerns and assess emotional well-being.

By days four and five, the focus should shift toward recovery and rebuilding trust. Leaders should support emotional recovery by normalizing discussions around stress, grief, or fear and offering flexibility such as temporary remote work or adjusted schedules.

Communication regarding enhanced safety and security measures is essential to reassure employees that lessons have been learned. Leadership should also recognize and acknowledge the resilience and cooperation demonstrated by employees during the incident. This should occur alongside essential facility repairs.

Guiding Principles for Leadership

Effective leadership during response and recovery following a traumatic event is grounded in

compassion, transparency, and visibility. Leaders should prioritize people over productivity, recognizing that employee well-being is foundational to long-term recovery. The decision to reopen an office following a necessary closure should be made carefully and with great care for customers and staff affected. In some cases, not reopening a location may be in the greater interest.

Clear and honest communication should take precedence over perfect messaging, with leaders openly acknowledging what is known and unknown. Visible and approachable leadership fosters trust and reassurance, and continuous learning from the incident strengthens future preparedness and organizational resilience. Consider each employee as a whole person and understand that they have loved ones with concerns, too.

Recovery Process and Long-Term Support

Recovery is an ongoing process that involves restoring services while continuing to support employees and customers. Immediate recovery efforts should focus on reunification and safety, access to support services, and recognition that individuals respond differently to traumatic events. Organizations should promote resilience through sustained mental health support, including employee assistance programs, peer mentoring, and resilience-building initiatives.

Long-term recovery strategies may need to be considered based on advice from internal partners or external experts. Leadership should monitor for warning signs of unresolved trauma, such as frequent absences, sleeping at work, or substance use, and intervene with appropriate support when necessary.

Conclusion

Resolution and recovery are both operational and human-centered processes. By integrating structured emergency planning with compassionate, consistent leadership, organizations can restore services while fostering resiliency, trust, and long-term well-being among employees.

Chapter 6 Lessons Learned—Turning Recovery Into Readiness

Lessons learned complete the incident lifecycle and close the continuous improvement cycle at the heart of the SeMS approach. Rather than filing after-action reports and moving on, effective lessons learned processes translate insights directly into updated emergency plans, revised training, facility modifications, and enhanced security protocols—providing data-driven justification for targeted investments in staffing, technology, environmental design, and training. Leadership needs to do more than resolve incidents; they ought to gather insights to prevent future ones and strengthen response strategies.

The Continuous Improvement Cycle

By mirroring NIMS principles, MVAs adopt a common framework that facilitates coordination with law enforcement and emergency services while supporting structured organizational learning. Plans that appear effective on paper may function differently under the fear, confusion, and time pressure of actual events. Post-incident learning closes that gap.

The review process should unfold in three stages: a preliminary debrief immediately after the incident to capture fresh observations; a comprehensive after-action review 30 to 60 days after the incident, after recovery has stabilized and staff have had time to process their experiences; and a follow-up review 6 to 12 months later to assess whether implemented improvements are working and identify any issues not initially apparent.

The purpose is not to assign blame but to understand how people, decisions, tools, and systems performed under stress. Effective reviews identify what worked and should be reinforced, what failed and requires correction, what assumptions proved wrong, what training or resources were missing, what environmental factors influenced outcomes, and what insights could benefit peer jurisdictions.

Conducting After-Action Reviews

The Department of Homeland Security's Homeland Security Exercise and Evaluation Program (HSEEP) provides widely used guidance for collecting observations, identifying strengths and gaps, and translating findings into corrective actions. Combined with CPTED concepts and DHS SAFE principles, this framework extends the review beyond operational response to include how environmental design, access control, and visibility shape behavior and outcomes. CISA offers facility security assessment assistance at cisa.gov.

Psychological safety is essential. Ground rules ought to focus on learning rather than blame so employees share what actually happened, not what they think leadership wants to hear. Leaders are expected to model receptiveness to difficult feedback and demonstrate that reported concerns lead to genuine improvement.

Comprehensive reviews draw on multiple data collection methods: facilitated group debriefs; individual interviews for those reluctant to speak in groups; anonymous surveys to surface honest feedback on leadership or culture; voluntary written statements; detailed timeline reconstruction; document review (incident reports, surveillance footage, communication logs, access control records); and quantitative analysis of response times, staffing levels, and service disruption. No single method captures the full picture; combining approaches does.

Ensure diverse participation including frontline employees, supervisors, leadership, support functions (HR, IT, facilities, legal), external partners (law enforcement, emergency services), and TAT members. Capturing all perspectives—not just those of leadership or just frontline—is what makes lessons learned genuinely useful.

Analyzing People and Resources Separately

To avoid missing critical gaps, analyze people and resources as distinct categories. Leaders may incorrectly assume preparation and response were adequate simply because no one was injured. Evaluating each phase of your EAP separately—and examining both human and physical factors—ensures nothing is overlooked.

People-focused analysis examines whether staff understood their roles, leaders had sufficient situational awareness to make timely decisions, communication was clear and

consistent throughout, and leadership presence reassured staff when needed. It also assesses whether employees recognized and responded to the incident promptly, felt empowered to act or escalate, and applied their training effectively and whether the organizational culture supported honest reporting and prioritized employee safety and well-being afterward.

Resource-focused analysis reviews whether emergency plans were available, current, and practical under real conditions—and whether staff knew how to locate and implement them. Physical security and environmental design should be evaluated using CPTED principles: access controls, barriers, lighting, safe rooms, building layout, and natural surveillance, with attention to any vulnerabilities in public-access areas. Technology assessment should determine whether communication tools, alarms, cameras, and IT systems functioned reliably and whether staff could operate them under pressure. Staffing and external partnerships should be reviewed for adequacy and timeliness, and any gaps in supplies, equipment, or system redundancy should be documented as improvement opportunities.

Documenting and Prioritizing Improvements

After-action reviews only create value when their findings are acted on. Each After-Action Report should include an executive summary, incident overview, description of the review methodology, analysis of what worked and what failed, and specific actionable recommendations organized by category (training, procedures, facilities, equipment, staffing) with clear ownership and timelines.

When resources are limited, prioritize improvements based on risk reduction impact (which changes address the most serious vulnerabilities), feasibility (balancing quick wins with longer-term investments), cost-effectiveness, stakeholder support, and interdependencies (sequencing improvements so foundational changes precede dependent ones).

Every identified improvement should be captured in an Improvement Plan that documents the specific gap, the corrective action, the accountable individual, required resources, implementation deadline, measurable success criteria, and a regular reporting mechanism. Improvements without deadlines, owners, or defined outcomes rarely get completed.

Integrating Lessons Into Organizational Systems

Lessons learned need to change how the organization actually operates. Key integration points include:

- **Emergency plans:** Revise evacuation and shelter-in-place procedures, clarify roles, remove outdated protocols, version-control all changes, notify staff, and test updates through exercises before the next incident.
- **Training:** Update curricula to reflect actual incidents, address identified skill gaps, and develop anonymized case studies for ongoing training. Real examples are far more effective than hypothetical scenarios.

- **Physical security:** Prioritize low-cost improvements (better lighting, repositioned workstations, improved signage) immediately while planning medium- and high-cost upgrades through capital budgeting. Post-incident findings are compelling justification for investment requests.
- **Policy:** Review and update policies on workplace violence prevention, employee authority, incident reporting, and post-incident support. Engage frontline staff in revisions to ensure practical applicability.
- **Communication:** Address common failures by clarifying chains of communication, implementing redundant systems, developing pre-drafted message templates, and testing protocols regularly under realistic conditions.

Validation and Monitoring

Leadership have an obligation to actively verify that corrective actions are completed. Establish a review cadence: monthly for status updates on active projects, quarterly for comprehensive progress assessment, and annually for strategic evaluation and plan reassessment. Assign executive-level ownership of the overall improvement plan. Plans should also be reviewed after facility renovations, major staffing changes, new threat identification, or significant changes in community context regardless of whether an incident has occurred.

Sharing Lessons Across the MVA Community

Your jurisdiction's experience has value beyond your organization. Share lessons learned internally across all facilities and departments, not just those directly involved—through staff meetings, training, and leadership communications. Reach out to neighboring jurisdictions and regional partners and establish formal information-sharing relationships when possible.

AAMVA offers several ways to share information widely, such as conferences, regional meetings, pop-up classroom events, and various publications. Additionally, AAMVA can provide consulting support and assist your MVA network with other jurisdictions. When sharing externally, provide sufficient operational detail to be useful while protecting sensitive information such as unresolved vulnerabilities, personal information, and details that could enable future harm.

Organizational transparency about failures and lessons learned is a mark of maturity and an ethical responsibility. Organizations that hide failures allow other jurisdictions to repeat them. By sharing openly, the MVA community builds collective resilience no single jurisdiction could achieve alone.

Measuring Learning Effectiveness

Effective lessons learned processes produce observable outcomes over time:

- **Declining incident severity:** Vulnerabilities are addressed, response improves, and serious harm is prevented or contained more quickly.
- **Faster, more effective response:** Staff apply learned procedures; decision-making processes and coordination improve.
- **Fewer repeat issues:** The same failures do not recur across multiple after-action reviews.
- **Higher employee confidence:** Staff trust that the organization takes safety seriously and will support them.
- **Increased reporting:** A culture of transparency produces more incident and near-miss reports as staff trust that observations lead to positive change.
- **Risk-aligned resource allocation:** Budget and capital decisions reflect lessons learned priorities rather than tradition or politics.

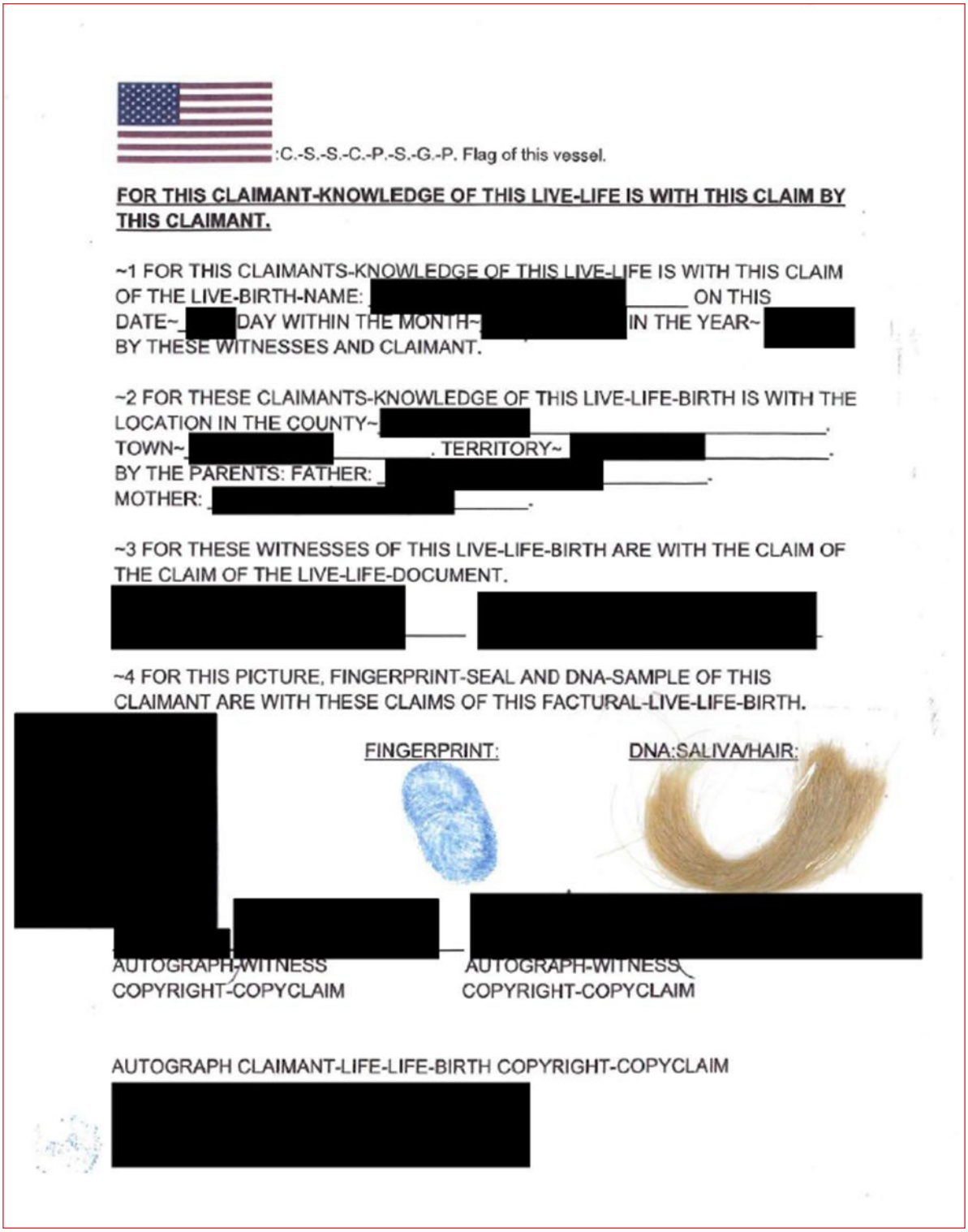
Conclusion: Completing the Cycle

Lessons learned closes the continuous improvement loop. Without systematic learning, organizations repeat failures and fail their fundamental responsibility to protect employees and customers. Every incident—regardless of severity—offers insight: medical emergencies expose facility design issues, customer conflicts reveal training gaps, and near-misses surface vulnerabilities before harm occurs.

Security is not a destination. Instead, it is a continuous cycle of preparation, response, recovery, and learning. Organizations that commit to this cycle, honestly assess their vulnerabilities, and systematically address them build the resilience needed to protect their people and fulfill their mission of public service—even in the most challenging circumstances.

This guide is a working document. Use it. Train from it. Test against it. Update your plans based on it. Contribute your experience to improve it for others. Together, the MVA community becomes safer, stronger, and more resilient with every lesson learned and every improvement made.

Appendix A Incident-Specific Response Protocols



:C.-S.-S.-C.-P.-S.-G.-P. Flag of this vessel.

FOR THIS CLAIMANT-KNOWLEDGE OF THIS LIVE-LIFE IS WITH THIS CLAIM BY THIS CLAIMANT.

~1 FOR THIS CLAIMANTS-KNOWLEDGE OF THIS LIVE-LIFE IS WITH THIS CLAIM OF THE LIVE-BIRTH-NAME: _____ ON THIS DATE~_ DAY WITHIN THE MONTH~ IN THE YEAR~ BY THESE WITNESSES AND CLAIMANT.

~2 FOR THESE CLAIMANTS-KNOWLEDGE OF THIS LIVE-LIFE-BIRTH IS WITH THE LOCATION IN THE COUNTY~_____.
TOWN~_____. TERRITORY~_____.
BY THE PARENTS: FATHER: _____.
MOTHER: _____.

~3 FOR THESE WITNESSES OF THIS LIVE-LIFE-BIRTH ARE WITH THE CLAIM OF THE CLAIM OF THE LIVE-LIFE-DOCUMENT.

_____ _____

~4 FOR THIS PICTURE, FINGERPRINT-SEAL AND DNA-SAMPLE OF THIS CLAIMANT ARE WITH THESE CLAIMS OF THIS FACTURAL-LIVE-LIFE-BIRTH.

FINGERPRINT:

DNA:SALIVA/HAIR:

_____ _____

AUTOGRAPH-WITNESS
COPYRIGHT-COPYCLAIM

AUTOGRAPH-WITNESS
COPYRIGHT-COPYCLAIM

AUTOGRAPH CLAIMANT-LIFE-LIFE-BIRTH COPYRIGHT-COPYCLAIM

_____

1. The "Silence Equals Consent" Fallacy

This concept rests on a fundamental misapplication of contract law principles, placing a positive obligation on recipients to reject offers or be deemed to have accepted them. It appears as unilateral declarations of "opting out" of laws, "fee schedules" that recipients allegedly accept by not rejecting, and debt elimination schemes in which failure to provide certain evidence negates legitimate obligations.

2. Misquoted Legal Precedent: *Thompson v. State*

A frequently cited case involves a carefully selected partial quote from *Thompson v. State,* 154 S.E. 579 (Va. 1930), suggesting an absolute right to drive without a license. However, the very next paragraph in that decision states: "The exercise of such a common right the city may, under its police power, regulate in the interest of the public safety and welfare; but it may not arbitrarily or unreasonably prohibit or restrict it."

The Virginia Supreme Court was not saying people have a right to drive without a license. It confirmed that government could regulate that right provided it did not do so arbitrarily or unreasonably. Similarly, *Shuttlesworth v. Birmingham,* 394 U.S. 147 (1969), is sometimes cited to negate licensing requirements, but that case concerned parade permits and First Amendment rights, not driver licensing.

3. Run: Evacuate When Possible

If a safe escape route exists, immediate evacuation is the priority response. Getting away from the threat is always preferable to remaining in the facility when escape is possible. Staff should leave belongings behind and move quickly toward exits, understanding that personal items can be replaced but lives cannot. Although facilities maintain posted evacuation routes, staff need to recognize that these routes may be compromised depending on the specific circumstances of the incident. If the primary evacuation route is blocked or leads toward the threat, staff should use alternative exits, including windows if they are on the ground floor, or emergency exits in any direction that provides safety.

When evacuating, staff should help others escape when possible but not place themselves at risk to do so. Warning others not to enter the area prevents additional people from encountering the threat. If able to do so safely without slowing evacuation, staff should activate panic buttons to alert authorities. Staff should not attempt to move injured persons unless they are in immediate danger of further harm such as fire or ongoing violence; emergency responders are trained and equipped for medical evacuation and can provide care that untrained individuals cannot.

When they are clear of the facility, staff should move to a safe distance and call 911 if emergency services have not already been contacted. Staff should provide their location, describe what they witnessed, and follow dispatcher instructions. Evacuated staff should remain available to law enforcement for information but should move to designated assembly areas away from the facility to avoid interfering with emergency response operations.

Jurisdictions should consider accessibility issues when developing evacuation protocols. Some employees and customers may have mobility limitations, visual or hearing impairments, or other conditions that affect their ability to evacuate quickly. Facilities should identify designated employees or supervisors responsible for facilitating evacuation for individuals requiring assistance. These personnel should be trained and aware of their responsibilities, understanding both how to assist and recognizing that their own safety comes first. If assisting another person creates unacceptable risk, the designated assistant should evacuate and immediately inform first responders about individuals who require assistance and their locations.

4. Hide: Shelter in Place When Evacuation Is Not Possible

If evacuation is not feasible because of the location of the threat or lack of safe escape routes, staff should find secure hiding locations and remain out of sight. The immediate priority is getting out of the threat's view. Staff should seek hiding places that provide protection in case shots are fired in their direction. Designated shelter spaces identified during facility security planning provide optimal protection, but any room with a locking door can serve as temporary refuge. Hardened spaces with minimal windows, solid walls, and lockable doors offer the best protection.

When in a hiding location, staff should lock and barricade doors using furniture, filing cabinets, or any available materials. Heavy items pushed against doors prevent or delay entry even if locks are breached. Closing blinds prevents the threat from seeing into the space, and turning off lights makes rooms appear unoccupied. All electronic devices must be silenced completely; even vibration can reveal presence. If multiple people are hiding in the same general area, they should separate within the space or hide in different locations to make it more difficult for a threat to harm multiple individuals simultaneously.

Staff should activate panic buttons if able to do so without revealing their location. Calling 911 and leaving the line open provides emergency responders with real-time audio information about the situation without requiring conversation that might alert the threat. Staff should remain absolutely quiet and in their hiding places until law enforcement personnel specifically identify themselves and tell occupants it is safe to evacuate. Emerging too early can place individuals directly in the path of the threat or cause confusion with responding officers, who may be unable to distinguish between threats and victims in chaotic situations.

Facilities should consider whether lockdown, lock-in, or lockout protocols are appropriate and attainable for their specific configuration. A lockdown involves securing all interior spaces with staff and customers sheltering in place is appropriate when a threat is inside the facility. A lock-in secures the facility perimeter while allowing controlled movement inside, appropriate when the threat is primarily to specific individuals rather than everyone. A lockout secures the facility perimeter against an external threat while operations continue inside, which is appropriate when threats exist in the surrounding area but have not entered the facility. The appropriate protocol depends on the nature and location of the threat, and staff should be trained to recognize which protocol applies to different scenarios.

5. Fight: Defend as a Last Resort

If evacuation and hiding are not possible and an individual faces imminent danger with the threat immediately present, defending against the threat becomes necessary for survival. This is always a last resort when no other options exist. Fighting back violates natural instincts for many people, but survival requires overriding these instincts when facing active threats. Individuals are encouraged to commit fully to their defensive actions, understanding that half-measures will likely prove ineffective and may enrage attackers without stopping them.

Acting as aggressively as possible against the threat using any available objects as improvised weapons provides the best chance of survival. Throwing items to distract and disorient the threat creates opportunities for escape or disarmament. Heavy objects, hot liquids, cleaning chemicals, or any items that can cause pain or injury should be deployed without hesitation. Recruiting others to ambush the threat with makeshift weapons such as chairs, fire extinguishers, scissors, or books increases effectiveness through numbers and simultaneous action from multiple directions. Coordinated group action significantly improves survival odds compared with individual efforts.

Individuals may need to mentally adjust and be prepared psychologically for the reality that causing severe or lethal injury to the threat may be necessary to stop the attack. This is perhaps the most difficult aspect of the "fight" response because most people are deeply conditioned against violence. However, in active threat situations, the threat has already demonstrated intent to cause harm, and defending oneself and others is both legally justified and morally necessary. Training should address this psychological barrier honestly, helping staff understand that choosing to defend themselves does not make them violent people but rather survivors who took necessary action when all other options were exhausted.

Robbery Procedures

If you are approached and asked for money, whether at your workstation or while taking a deposit to the bank, cooperate and hand over money immediately. Do not resist or delay. Protect your own health and safety at all costs. Do not take any action that may affect the safety of staff or customers. Cooperate and follow the robber's instructions but do not do more than asked. Give the robber only money that can be readily seen. Do not dig out hidden money unless specifically instructed to do so.

If you must reach under your workstation with your hands for money or other documents, advise the robber at all times of what you are doing to prevent sudden movements from being misinterpreted as threats. Do not press the panic alarm button during the robbery if doing so might be noticed and escalate the situation.

Try to observe the robber as calmly and naturally as possible under the circumstances without obvious staring. The more you can remember, the more helpful it will be to police. Try to note the type and color of clothing worn; color of the hair, eyes, and skin; any distinguishing features such as scars or tattoos; approximate age; height and build; and any mannerisms, speech peculiarities, or accents. Observe if the robber touched anything where fingerprints may have been left.

If other staff members notice that a robbery is taking place at another workstation, they should press the panic alarm button only if certain they will not be observed doing so. If more than one robber is involved, study the nearest one rather than attempting to observe all suspects. After subjects have left the facility, try to get descriptions of vehicles used (if applicable), license plate numbers, direction of travel or flight, and other occupants. After the person has left the premises and you consider the situation safe, press the panic alarm button and notify your supervisor immediately. Call 911 directly as well.

Save any note that may have been used and do not handle it unnecessarily or allow others to handle it to preserve fingerprint evidence. Employees should not discuss the crime among themselves or with other witnesses until they have been interviewed by police. If there is a delay before police arrival, make written notes while details remain fresh.

Inform the director of the robbery. Refer all inquiries from media to the director. Do not discuss the losses with anyone.

Prevent anyone from going into areas or touching anything where the robber might have been. Lock doors if possible and allow no one in except police. Hold all witnesses until police arrive. After police have left, allow employees to phone their families if they wish.

Incident Response Team

- Emergency: 911
- Facility manager or supervisor
- Director of the service center
- Director of highway safety
- Registrar of motor vehicles
- HR

Medical Emergencies and First Aid

- All staff should receive first aid training. Post a list of all trained first aid employees in areas accessible to all staff.
- A staff member or customer may suddenly become ill while working at or visiting a facility. If you notice someone is unwell, ask if they need to call someone or require an ambulance. If possible, help them to a private area. Notify your manager or ask someone to do it for you.

For minor emergencies, report the illness or injury to your manager. Make use of first aid kits if required. Each facility should have names of staff trained in first aid posted by first aid kits.

For major illness or injury, call 911 immediately and provide emergency personnel with:

- Your name and location
- The type of emergency (fracture, bleeding, etc.)
- Stay on the line with dispatchers.

If you are helping the victim, do not move the person unless there is immediate danger such as fire or structural collapse. Keep others clear of the area. Stop bleeding if possible using available materials. Restore breathing and/or heartbeat with AED or CPR only if you are trained. Do not attempt these procedures without training.

Incident Response Team

- Emergency: 911
- Facility manager or supervisor
- Director of the service center

Drug Overdose Response

If someone is experiencing a medical emergency, call 911 immediately. Act right away. Overdose deaths are usually a relatively slow process, taking minutes to hours, meaning response during this window can prevent fatality.

Someone overdosing will be not breathing and not responsive. Additional signs include skin turning blue or gray, pinpoint pupils, and deep gurgling sounds.

Step 1: Stimulate them awake by yelling their name and administering a hard sternum rub to the chest plate.

Step 2: If naloxone (Narcan) is available and you are trained in its use, administer it. Give one dose every 2 to 3 minutes following these guidelines:

- Injectable: Draw up entire vial and inject into thigh muscle (must be intramuscular to work).
- Nasal: Insert the device fully into one nostril and click the plunger, ensuring full insertion so medication absorbs through sinuses.

Step 3: Call 911 and explain someone is not responsive and not breathing.

Step 4: Provide rescue breathing if trained:

- Get the person on their back.
- Tip their head back to straighten the airway.
- Pinch their nose.
- Put your mouth over theirs and form a seal.
- Give one breath every 5 seconds.

Step 5: When the person starts breathing regularly on their own, roll them into a recovery position on their side.

Step 6: Be gentle with them and yourself afterward. Both the victim and responders may need support following traumatic events.

Incident Response Team

- Emergency: 911
- Facility manager or supervisor
- Director of the service center
- Registrar of motor vehicles
- Director of highway safety

Physical Attack Response

Every precaution should be taken to prevent physical attacks. If a physical attack or hostage-taking incident is taking place in your work area, press the panic alarm button when appropriate and safe to do so. If you are attacked, make noise. Yell or scream as loud as possible. Try shouting specific words such as "STOP," "FIRE," or "HELP" to alert others and potentially deter attackers.

- If you approach a situation that feels threatening or has potential to become threatening, turn back or go to the nearest safe place and call for help.
- If you are being pulled along or dragged, fall to the ground and roll to make yourself more difficult to move.
- If someone grabs your purse, briefcase, deposit bag, or other belongings, do not resist. Throw the item several feet away from the thief and run in the opposite direction, yelling "HELP" or "FIRE." Do not chase the thief.
- Run to the nearest safe place such as an office or occupied business.
- Make note of the offender's description, including physical characteristics and clothing while details remain fresh.
- Call police immediately after the incident. Any physical attack, however slight, warrants a police report. Inform your manager.
- If an injury occurred to an employee requiring medical attention or time lost from work, complete workers' compensation reporting. If injury occurred but did not require doctor visit or time loss, file departmental non-medical aid reports.

Incident Response Team

- Emergency: 911
- Facility manager or supervisor
- Director of the service center

Bomb Threat Procedures

Bomb Threat by Telephone

If a bomb threat is telephoned to your facility, remain calm and courteous. Do not interrupt the caller. Without alerting the caller, indicate to a coworker through written note that you are receiving a bomb threat. They should notify the manager who should call 911.

Keep the caller on the line. Try to note exactly what the caller says, making notes during the conversation. Attempt to persuade the caller to tell you:

- When will the bomb explode?
- Where is the bomb now?
- What does it look like?
- What will cause it to go off?
- Did they place the bomb themselves?
- Why did they place the bomb?

Note any identifying characteristics of the caller, including gender, voice characteristics (calm, angry, distorted), accent, speech patterns, and background noises.

Bomb Threat in Person

If a person physically present threatens to blow up the facility, try to remain calm and courteous. Do not panic. If a coworker hears the threat, they should notify the manager who should call 911 if warranted. Try to note exactly what the person says and attempt to learn the same information as in telephone threats.

Note identifying characteristics including:

- Gender, height, and weight
- Accent
- Speech pattern and voice (calm, angry, distorted)
- Clothing description
- Any other helpful information

Remain calm. After the person has left, management should inform customers and staff quietly that a bomb threat has been received and they must evacuate immediately until the building has been checked. Call 911 if not already done.

Bomb Threat Through Mail

- Suspicious packages may include no return address, misspellings in the address, being addressed to a title rather than an individual, poor typing or handwriting, uneven shape, strange odor, excessive tape or string, or rigid or bulky packaging.
- Avoid excessive handling of threatening letters or packages to preserve evidence.
- Report receipt immediately to the manager who will inform the director. If necessary, call 911 and evacuate the building.
- Report receipt of the threatening letter to police for investigation.

Incident Response Team

- Emergency: 911
- Facility manager or supervisor
- Director of the service center
- Director of highway safety

Fire or Explosion Procedures

Fire orders should be displayed prominently, and all employees need to familiarize themselves with evacuation procedures. All employees should evacuate immediately upon hearing fire alarms, assisting customers and others while ensuring cash, inventory, and equipment are not stolen during confusion. Employees must know the locations of all fire alarms and firefighting equipment in their facilities. Designated employees should be identified to escort disabled persons, customers, and visitors out of the building if necessary. No employee should light fires, handle flammable materials carelessly, smoke on facility premises, or use firefighting equipment for any purpose other than firefighting.

Each staff member should receive instruction on handling various types of fire extinguishers and ought to be familiar with the location of the nearest fire alarm. Under no circumstances should firefighting equipment be obstructed or hidden by piling materials in front of it or hanging items on it.

Upon discovering fire:

1. **Evacuate the immediate area, closing doors behind you to contain fire.**
2. **Pull the nearest fire alarm.**
3. **Follow posted escape routes and emergency guidelines.**
4. **If telephone access is available without creating danger, call 911.**

5. **Alert all other employees and customers at the facility.**
6. **Managers should confirm by phone with fire department that alarm was received and emergency services are responding.**
7. **Upon hearing fire evacuation signals, if time permits and when possible, without creating risk, ensure all financial records, money, correspondence, and files are placed in filing cabinets and safes with containers locked before exiting via the nearest exit.**
8. **Do not use elevators during evacuation. Evacuees should be directed to a safe area and first aid or medical assistance arranged for injured persons if necessary.**
9. **Supervisors or designees should account for all staff.**
10. **Wait for emergency personnel outside the building and provide information about any hazardous materials inside and their locations.**
11. **Assist the fire department as requested and follow their instructions. Do not re-enter the building until permission is given.**
12. **Notify the director as soon as possible.**

Incident Response Team

- Emergency: 911
- Facility manager or supervisor
- Director of the service center
- Director of highway safety

Suspicious Package or Object Procedures

Suspicious packages may exhibit warning signs, including:

- No return address
- Misspellings in the address
- Addressed to a title rather than an individual
- Poor typing or handwriting
- Uneven shape
- Strange odor
- Excessive tape or string
- Rigid or bulky packaging

Response Procedures

Do not touch or disturb the package or object. Handle with care and isolate the package to prevent potential activation of explosive or chemical devices.

Report the discovery immediately to your manager who will call 911.

Remain calm. Inform customers quietly that a suspicious package has been received and ask them to please leave the building immediately.

Evacuate the building and wait for directions from police before taking any further action.

Incident Response Team

- Emergency: 911
- Facility manager or supervisor
- Director of the service center

Restraining Order and Trespassing Order Management

When incidents occur affecting staff safety, restraining orders or trespassing orders may be issued. These orders require that affected individuals understand and comply with terms, which often include staying away from protected persons, specific work locations, or departments and not making contact.

Management Procedures

1. Obtain copies of the order and provide them to local law enforcement to ensure the order is in their system for enforcement.
2. Protected staff should carry copies of the order to present to police if violations occur.
3. Document violations with detailed records of every instance including time, place, and specific details of the incident.
4. When witnessing violations, contact law enforcement immediately. Police or sheriff's deputies need to see copies of the order to enforce it effectively.
5. Create safety plans that protect staff and persons protected by the order. Protected persons should remain out of sight of offenders when possible.
6. Staff can contact lawyers or victim services workers for help understanding or modifying orders if circumstances change.
7. Ensure clear communication with all facility staff about the existence and terms of protective orders to ensure coordinated response if the subject appears.

Incident Response Team

- Local law enforcement
- Director of the service center
- Registrar of motor vehicles
- Facility manager or supervisor

Appendix B Service Disruption and Business Continuity Protocols

Power Outage Procedures

If power fails during working hours, immediately usher customers out of the building and lock all doors. Display signs on main doors explaining the closure to inform arriving customers. Contact the electric supplier to determine estimated restoration time. If the manager is not on site, notify them as soon as possible. Notify the director's office so they can inform the deputy minister and minister's office.

Incident Response Team

- Facility manager or supervisor
- Director of the service center
- Deputy minister

Loss of Facility Response

When incidents affect facility operations for 24 hours or longer, the incident response team under direction of the deputy minister determines if and when the team should convene to decide best course of action.

Incident Response Team Responsibilities

- Activate business continuity plan for the department or site as required.
- Provide coordination and management for implementation to ensure delivery of essential government services.
- Decide on extension of business hours if necessary to provide essential services.
- Coordinate with facilities representatives to determine short- and long-term replacement facility options.
- Develop situational reports for distribution to senior management as required.
- Designate personnel to lead on-site activities.

Business Continuity Management Response Team

- Manager of affected the service center location
- Records management coordinator

Required Actions

- Assess the situation and relocate service within existing facilities.
- Ensure those awaiting time-sensitive services can access service within appropriate timeframes.
- Prioritize aspects of service delivery, including timelines for recovery and prioritization of appointments.
- Contact affected customers to inform them of the situation, relocate and reschedule appointments as necessary.
- Select suitable location(s) for priority services from predetermined list.
- Arrange for facilities to be set up appropriately for service delivery.
- Coordinate with IT regarding access to necessary databases and systems.
- Transfer or forward phone numbers to operational locations.
- Monitor the situation and adjust based on priority needs.
- Implement external communication plan as needed.

Short-Term Options

- Use available laptops and portable equipment during emergency.
- Temporary location in affected area estimated to take 2 to 4 weeks to set up.
- Use predetermined processes for obtaining replacement equipment within set timeframes.

Communication Plan

- Issue press release within 24 hours informing the public of alternative service locations.
- Announce a temporary location for the affected facility when established.
- State extended hours if the incident response team decides this is necessary.
- Remind the public of available online services.
- Develop a press release in conjunction with communications officers.

Incident Response Team

- Director of the service center
- Deputy minister of transportation
- Director of highway safety
- HR manager
- Communications officer
- Business continuity coordinator
- IT representative

Loss of Information Technology Response

When IT outages affect facilities for 24 hours or longer, the incident response team under direction of the deputy minister determines if and when the team should convene.

Business Continuity Plan

During an IT outage affecting all facilities, facilities should remain open with staff following procedures in the "Interruption of Service" manual. The incident response team meets with directors across government whose services operate through affected facilities within 48 hours to determine extent of service delivery possible without internet access. Within 72 hours, the incident response team informs managers what services to deliver and how to deliver them based on these meetings.

IT representative provides incident response team with updated information on IT infrastructure status so communications can inform the public accurately about when facilities will be fully operational.

Communication Plan

External Communications

- Communications officer works with communications department to develop a press release.
- The press release informs the public that facilities have lost internet connection and that many services are currently unavailable.
- The public is assured that facilities remain open and that they can contact locations to determine which services are available.
- The public is informed that a business continuity plan is in place, and facilities are working with IT and all departments to determine available services and develop a timeline for restoration.
- The public is informed that another press release will be issued in 1 week with more details and estimate for internet resumption

Internal Communications

- Departments with affected services are informed of internet loss.

- Departments are asked to send essential forms to facilities in hard copy.
- Departments are warned of a potential spike in customers contacting them directly for
- services facilities cannot be provided because of internet loss.

Incident Response Team

- Director of the service center
- Deputy minister of transportation
- HR manager
- Communications officer
- Business continuity coordinator
- IT representative
- Director of highway safety

Loss of Staff Response

When staff shortages affect facilities for 24 hours or longer, the incident response team under the direction of the deputy minister determines if and when the team should convene.

Business Continuity Plan

Managers of all facilities keep the incident response team informed of staff shortage numbers. Facilities attempt to maintain as many locations as possible during staff loss events.

Managers contact casual staff as necessary to replace staff who are unavailable. The **first priority** is continuing to staff predetermined essential locations. These locations are maintained by calling casual employees and reallocating employees from smaller facilities. The **second priority** is continuing to operate smaller locations, if possible, even in reduced capacity. If necessary, hours are extended at essential locations to allow customers to access services after regular work hours. The HR manager works with managers, public service commission, and unions if this occurs. In efforts to contain disease spread during staff shortages because of illness, sanitizers are strategically placed throughout facilities.

Recovery Strategy

- Temporarily suspend noncritical functions.
- Consider other departmental staff for temporary assignment.
- Reassign existing staff according to the succession plan.
- Maintain continuation of essential services, including data input and document output functions.

Communication Plan

The communications officer develops press release informing the public which facilities remain open and about new hours of operation during staff loss event.

The public is reminded of alternative service channels, including online services.

The public is informed as soon as other facilities reopen and hours of operation return to normal at all locations.

Incident Response Team

- Director of the service center
- Deputy minister of transportation
- Director of highway safety
- HR manager
- Communications officer
- Business continuity coordinator
- IT representative

Appendix C Specialized Situations

Working Alone and Mobile Operations Safety

Employees sometimes work alone at single-person facilities or during mobile outreach events. The hazard when working alone is the inability to call for help. Therefore, when employees work alone, they should take particular care to avoid risky situations, and practices ought to be implemented that can initiate help when required.

Reasonable Precautions When Working Alone

- Ensure supervisors are aware of the situation and the work being performed or circumstances in which it will be performed.
- Establish regular check-in schedules with supervisors at predetermined times.
- Ensure panic alarm systems function in remote or mobile locations.
- Increase situational awareness and vigilance when working without backup.
- If you fear for your safety, press panic alarm button or call 911 without hesitation.

Documentation

Complete documentation for each employee who works alone with signed copies forwarded to the director's office for record-keeping and safety accountability.

Dealing with Difficult Customers: Detailed Strategies

Dealing with difficult customers at work requires remaining calm and professional, setting clear boundaries, and practicing active listening to understand their perspective. Focus on solutions and shared goals and do not take negative behavior personally. Document problematic behavior for reporting to management and prioritize your well-being through self-care and seeking support from trusted colleagues or mentors.

Maintain Professionalism and Composure

- Stay calm and avoid emotional reactions, which can escalate situations and damage
- your reputation.
- Be polite and respectful, maintaining composure even if the other person does not.

Understand and Empathize

- Practice active listening to fully understand the other person's perspective before responding.
- Seek mutual understanding rather than "winning" arguments.
- Consider their perspective; understanding why someone is difficult makes situations easier to manage.

Set Clear Boundaries

- Establish limits and be assertive about your boundaries while communicating them respectfully.
- Limit interactions when possible, focusing only on work-related tasks.

Focus on Solutions and Positivity

- Shift focus from problems toward finding solutions.
- Focus energy on positive relationships with cooperative colleagues rather than dwelling on difficult individuals.
- Stay positive, which can be powerful even in challenging situations.

Take Action When Necessary

- Document incidents by keeping records of negative behaviors, including time, place, and the details of what was said and done.
- Report serious issues if behavior crosses into harassment or bullying, reporting to managers or supervisors.
- If security or law enforcement personnel are on site, advise them of developing situations.
- Seek support from trusted colleagues, mentors, or professional resources for guidance.

Prioritize Your Well-being

- Do not take it personally; remember that others' behavior is often a reflection of them, not you.
- Practice self-care by taking breaks, listening to calming music, or going for walks to decompress and maintain your mental health.
- Focus on what you can control; you cannot change others, but you can control your own reactions and create positive space for yourself.

When to Escalate

- If verbal de-escalation is unsuccessful and behavior continues or escalates, notify management immediately.
- If customer behavior includes threats, activate appropriate emergency protocols.
- If customer behavior warrants it, management can issue trespassing orders prohibiting return to facilities.

Appendix D Incident Response Team Templates and Communication Plans

Incident Response Team Contact Information Template

Each jurisdiction should customize this template with specific names, phone numbers, and email addresses for their incident response teams. Maintain multiple copies in secure but accessible locations.

Emergency Services

- Emergency: 911
- Local police department (non-emergency): _____
- Local fire department (non-emergency): _____
- Local emergency medical services: _____

Internal Response Team

- Facility manager or supervisor: _____
  - Primary phone: _____
  - Secondary phone: _____
  - Email: _____
- Director of the service center:
  - Primary phone: _____
  - Secondary phone: _____
  - Email: _____
- Deputy minister of transportation: _____
  - Primary phone: _____
  - Secondary phone: _____
  - Email: _____
- Registrar of motor vehicles: _____
  - Primary phone: _____
  - Secondary phone: _____
  - Email: _____
- Director of highway safety: _____
  - Primary phone: _____
  - Secondary phone: _____
  - Email: _____
- HR Manager: _____
  - Primary phone: _____
  - Secondary phone: _____
  - Email: _____
- Communications officer: _____
  - Primary phone: _____
  - Secondary phone: _____
  - Email: _____
- Business continuity coordinator: _____
  - Primary phone: _____
  - Secondary phone: _____
  - Email: _____
- IT representative: _____
  - Primary phone: _____
  - Secondary phone: _____
  - Email: _____

Support Services

- Employee assistance program: _____
- Records management coordinator: _____
- Security services: _____
- Facilities management: _____

Communication Plan Template

Incident Type:

Date and Time of Incident:

Immediate Notifications (Within 1 Hour)

- Emergency services (911) if applicable
- Facility manager or supervisor
- Director of the service center
- Other: _____

Secondary Notifications (Within 4 Hours)

- Deputy minister
- Communications officer
- HR manager
- Other: _____

Internal Communications

Staff Notification Method

- In-person briefing
- Email
- Text alert system
- Phone tree
- Other: _____

Key Messages for Staff

- What happened (brief factual summary)
- Current status
- What actions staff should take
- Who to contact with questions
- When next update will be provided

External Communications: Stakeholders to Notify

- Customers with scheduled appointments
- Media (through communications officer only)
- Partner agencies
- Other: _____

Press Release (if applicable)

- Drafted by: _____
- Approved by: _____
- Distributed through: _____
- Timing: _____

Key Messages for Public

- Factual description of the incident (without sensitive details)
- Impact on services
- Alternative service options
- Expected timeline for resolution
- How to get more information

Follow-up Communications: 24-Hour Update

- To whom: _____
- Method: _____
- Key points: _____

Resolution Communication

- To whom: _____
- Method: _____
- Key points: _____

Appendix E Resolution Action Plan and Protocols

Resolution Action Plan: Step-by-Step Guide

This action plan provides step-by-step guidance for resolution phase activities. Not all steps apply to every incident. Mark N/A for steps that do not apply to your specific situation. Customize this plan for your jurisdiction's specific needs and organizational structure.

IMMEDIATE RESPONSE (UPON LAW ENFORCEMENT OR EMERGENCY SERVICES ARRIVAL)

Step 1: Employee Safety Protocol

- All employees immediately raise their hands above their heads with their palms open and visible.
- Employees remain stationary unless directed to move by officers.
- Employees remain silent unless directly addressed by officers.
- Employees follow all law enforcement commands immediately and precisely.
- N/A (explain): _____

Step 2: Scene Command Transfer

- Facility manager identifies law enforcement incident commander.
- Facility manager confirms law enforcement has assumed scene command.
- Facility manager provides facility keys, access codes, and security system Information.
- Facility manager provides facility layout or blueprints if requested.
- N/A (explain): _____

Step 3: Critical Information Delivery (Active Threat Situations)

- Provide number of threats and last known location.
- Provide physical descriptions including clothing and distinguishing features.
- Provide information about weapons observed.
- Provide location of injured persons.
- Provide direction of threat movement.
- N/A (explain): _____

Step 4: Response Team Activation

- Establish response team and list in EAP.
- Establish command post at predetermined location.
- N/A (explain): _____

Step 5: Provide the appointment schedule and visitor log.

- Account for all employees through direct contact or visual confirmation.
- Account for all customers and visitors to the extent possible.
- Report any missing or unaccounted persons to law enforcement immediately.
- N/A (explain): _____

Step 6: Scene Perimeter Establishment

- Respect all perimeters established by law enforcement.
- Ensure all employees remain outside perimeters unless directed by law enforcement.
- Post signage at facility entrances directing arriving customers away.
- Redirect phone calls to inform callers of facility closure.
- N/A (explain): _____

Step 7: Evidence Preservation

- Instruct all employees not to touch, move, or alter anything in scene areas.
- Instruct employees to preserve their own clothing if they had contact with threats or were injured.
- Identify and protect video surveillance systems from accidental deletion or Overwriting.
- Identify and protect access control logs and other electronic records.
- Coordinate with law enforcement regarding security of financial assets within the scene.
- N/A (explain): _____

Step 8: Witness Identification and Separation

- Work with law enforcement to identify all potential witnesses.
- Facilitate law enforcement separation of witnesses.
- Instruct witnesses not to discuss incident with each other.
- Arrange for witness comfort needs (water, restrooms, seating) while maintaining separation.

- Inform witnesses they will be interviewed before release.
- N/A (explain): _____

COORDINATION AND COMMUNICATION (1-4 HOURS)

Step 9: Law Enforcement Liaison Establishment

- Designate primary liaison (typically the director or deputy minister).
- Establish a regular communication schedule with the law enforcement incident commander.
- Provide law enforcement with incident response team contact information.
- Request an estimated timeline for scene release.
- Request information about partial release possibilities.
- N/A (explain): _____

Step 10: Internal Communications

- Brief all incident response team members on current situation.
- Notify all facility employees of the incident and facility status.
- Instruct off-duty employees not to report to work until further notice.
- Provide employees with contact information for support services.
- Establish schedule for regular employee updates.
- N/A (explain): _____

Step 11: External Communications

- Coordinate with the communications officer to prepare an initial public statement.
- Coordinate public statement content with law enforcement to ensure no interference with the investigation.
- Issue a public statement about facility closure and service disruption.
- Update website and phone systems to reflect facility closure.
- Prepare for media inquiries and direct all media to the communications officer.
- N/A (explain): _____

Step 12: Family Notifications

- For employees directly involved or injured, coordinate family notifications with the HR manager.
- Provide families with accurate information about employee status and location.

- Provide families with contact information for support services.
- For serious injuries or fatalities, coordinate notifications with law enforcement.
- N/A (explain): _____

WITNESS INTERVIEWS AND DOCUMENTATION (2–8 HOURS)

Step 13: Support for Employees Providing Witness Statements

- Inform employees of their rights, including the right to legal counsel.
- Make employee assistance program contact information available.
- Allow employees to contact family members to inform them of delays.
- Provide employees with breaks, food, and water during extended interviews.
- N/A (explain): _____

Step 14: Internal Documentation

- Designate staff member responsible for incident documentation.
- Document all communications with law enforcement, including times and content.
- Document all incident response team decisions and actions.
- Photograph or video document scene conditions when law enforcement permits.
- Preserve all electronic logs, surveillance video, and access control records.
- N/A (explain): _____

Step 15: Initial Damage Assessment (When Accessible)

- Assess physical damage to facility, equipment, and inventory.
- Document damage with photographs.
- Assess IT system status and data integrity.
- Estimate lost revenue from facility closure.
- Identify immediate costs incurred (security, emergency response, etc.).
- N/A (explain): _____

INSURANCE AND LEGAL NOTIFICATIONS (2–24 HOURS)

Step 16: Insurance Carrier Notification

- Notify the insurance carrier of the incident as required by policy.

- Provide preliminary information about the incident type and potential damages.
- Request guidance on documentation requirements.
- Coordinate with law enforcement regarding insurance adjuster access to scene.
- N/A (explain): _____

Step 17: Regulatory Reporting (If Applicable)

- Consult with legal counsel to identify mandatory reporting obligations.
- Complete required reports within specified timeframes.
- Document all regulatory notifications made.
- N/A (explain): _____

Step 18: Legal Counsel Consultation

- Brief legal counsel on incident details.
- Obtain guidance on evidence preservation obligations.
- Obtain guidance on employee rights during the investigation.
- Obtain guidance on organizational liability concerns.
- N/A (explain): _____

TRANSITION PLANNING (4-48 HOURS)

Step 19: Facility Re-entry Planning

- Await formal scene release from law enforcement (obtain written confirmation).
- Plan initial re-entry by security or facilities staff only for safety assessment.
- Identify the need for environmental remediation (blood, chemical contamination).
- Arrange for remediation services if needed.
- Plan security enhancements for reopening.
- N/A (explain): _____

Step 20: Operational Recovery Planning

- Determine which services can be restored and the timeline.
- Identify alternative service locations if the facility remains closed.
- Plan for customer communication about service restoration.

- Plan for employee return to work, including any modified assignments.
- Establish the date and time for facility reopening.
- N/A (explain): _____

Step 21: Employee Support Services Activation

- Ensure all employees have employee assistance program information.
- Schedule critical incident stress debriefing for all affected employees.
- Identify employees requiring immediate psychological support.
- Arrange for flexible work arrangements for affected employees.
- Plan for ongoing support services during the recovery phase.
- N/A (explain): _____

Step 22: Preliminary Lessons Learned Capture

- Conduct a brief incident response team debrief while events are fresh.
- Document what worked well during the resolution phase.
- Document what could be improved.
- Identify immediate policy or procedure changes needed before reopening.
- Plan for comprehensive lessons learned review during the recovery phase.
- N/A (explain): _____

Step 23: Transition to the Recovery Phase

- Confirm written scene release from law enforcement.
- Conduct facility safety assessment.
- Implement temporary security enhancements.
- Complete environmental remediation if needed.
- Communicate reopening plans to employees.
- Communicate service restoration to customers.
- Officially transition from resolution to recovery operations.
- N/A (explain): _____

Law Enforcement Coordination Checklist

Use this checklist to ensure effective coordination with law enforcement during resolution.

Initial Contact

- ☐ Identify law enforcement incident commander name and contact information.
- ☐ Provide facility manager or director name and contact information.
- ☐ Establish the primary communication method (phone, radio, in-person).
- ☐ Agree on communication frequency and the update schedule.

Information Sharing

- ☐ Provide facility layout or blueprints.
- ☐ Provide employee roster and accountability information.
- ☐ Provide visitor or customer logs if available.
- ☐ Provide video surveillance system access.
- ☐ Provide access control system data.
- ☐ Provide any relevant threat history or previous incident information.

Scene Access

- ☐ Understand scene perimeter boundaries.
- ☐ Identify which areas are secured versus accessible.
- ☐ Obtain permission before entering any secured areas.
- ☐ Coordinate employee access for critical operations (if permitted).
- ☐ Coordinate insurance adjuster access.

Investigation Support

- ☐ Facilitate witness interview space.
- ☐ Provide witness comfort needs (water, restrooms, seating).
- ☐ Provide organizational records as requested.
- ☐ Designate staff to answer investigator questions.

Timeline Coordination

- ☐ Request an estimated timeline for scene release.
- ☐ Understand what factors affect the release timeline.
- ☐ Request notification when partial release is possible.
- ☐ Request notification 24 hours before complete release if possible.

Media Coordination

- ☐ Agree on which information can be publicly released.
- ☐ Agree on which information must remain confidential.
- ☐ Coordinate the timing of public statements.
- ☐ Establish a process for clearing public communications before release.

Scene Release

- ☐ Request written confirmation of scene release.
- ☐ Understand any limitations on released areas.
- ☐ Confirm evidence collection is complete.
- ☐ Understand if investigators may need to return.
- ☐ Obtain contact information for follow-up questions.

Witness Interview Support Protocol

This protocol ensures employees providing witness statements receive appropriate support while maintaining investigation integrity.

BEFORE INTERVIEWS

Employee Notification

- Inform employees they will be interviewed by law enforcement before release.
- Explain this is standard procedure for all witnesses.
- Inform employees that interviews may take several hours.
- Provide realistic timeline estimates.

Rights Notification

- Inform employees of their right to legal counsel.
- Inform employees they can decline to answer questions that might incriminate them.
- Provide employee assistance program contact information.
- Clarify that organizational support is available.

Logistical Support

- Provide access to restrooms.
- Provide water and food if interviews are extended.
- Provide seating in comfortable area.
- Allow employees to contact family members about delayed release.
- Maintain separation between witnesses to preserve statement independence.

DURING INTERVIEWS

Organizational Presence:

- Do not have organizational representatives present during law enforcement interviews unless specifically requested by employee and approved by law enforcement. This preserves statement independence and prevents appearance of organizational influence.
- Employees may consult with legal counsel privately if they choose.

Employee Guidance

- If asked for guidance before interviews, advise employees to:
  - Tell the truth completely and accurately.
  - Say "I don't know" or "I don't remember" rather than guessing.
  - Provide only factual observations, not speculation or opinions.
  - Take time to think before answering if needed.
  - Ask for clarification if questions are unclear.

AFTER INTERVIEWS

Immediate Support

- Check on employee well-being after interview completion.
- Provide employee assistance program information again.
- Arrange transportation if an employee is too distressed to drive.
- Allow employees to go home rather than returning to work if desired.

Follow-Up

- Contact employee within 24 to 48 hours to check on their well-being.
- Remind employees of available support services.
- Inform employees about return-to-work plans and timeline.
- Clarify that employee may be contacted for follow-up interviews.

Documentation

- Document that the employee provided a statement to law enforcement.
- Document support services offered and accepted.
- Do not document content of statements. (This is law enforcement information.)

Evidence Preservation Guidelines

These guidelines help employees understand evidence preservation responsibilities during Resolution.

What Constitutes Evidence

Evidence in workplace incidents may include:

- Physical items (weapons, tools, personal belongings)
- Biological materials (blood, saliva, hair)
- Documents (notes, threats, pseudo-legal materials)
- Electronic data (video surveillance, access logs, computer files, emails)
- Financial materials (cash, transaction records)
- Environmental evidence (fingerprints, footprints, bullet casings)
- Clothing and personal effects of involved individuals

Employee Responsibilities Do

- Leave everything in place exactly as it is.
- Notify law enforcement of evidence you observe.
- Notify law enforcement of time-sensitive or perishable evidence.
- Preserve your own clothing if you had contact with threats or were injured.
- Preserve electronic records by preventing deletion or overwriting.
- Document evidence locations if you can do so without contamination.
- Follow all law enforcement instructions regarding evidence.

Do Not

- Touch, move, or alter any items in incident scenes.
- Clean up blood, materials, or debris.
- Straighten overturned furniture or equipment.
- Collect items for "safekeeping."
- Attempt to preserve evidence yourself.
- Enter secured scene areas for any reason.
- Take photographs of evidence. (Law enforcement will document it.)
- Discuss evidence with other witnesses before interviews.

Special Evidence Categories Video Surveillance

- Immediately secure video systems to prevent deletion or overwriting.
- Provide law enforcement with access to systems and retrieval instructions.
- Preserve all recordings from relevant time periods.
- Maintain chain of custody if video must be copied.

Financial Assets

- Do not remove cash or financial materials from secured scenes.
- Work with law enforcement to develop security plan for materials in scene.
- Document the chain of custody for any financial materials released by law enforcement.
- Photograph financial materials in place if law enforcement permits.

Electronic Data

- Preserve all access control logs, transaction logs, and system logs.
- Do not delete emails, files, or communications related to incident.
- Secure computers and devices to prevent tampering.
- Provide law enforcement with passwords and access credentials if requested.

Employee Clothing and Personal Effects

- If you had contact with threat, were injured, or may have transferred evidence, preserve your clothing.
- Place clothing in clean paper bags (not plastic, which degrades biological evidence).
- Label bags with your name, date, and time.
- Provide to law enforcement or secure until they request it.
- Do not wash clothing or personal items until law enforcement confirms they are not needed.

Evidence Preservation Documentation

Document all evidence preservation activities:

- What evidence was observed and where
- What actions were taken to preserve evidence
- Who handled evidence and when
- What was turned over to law enforcement
- Chain of custody for any materials moved or secured

Scene Release and Facility Re-entry Protocol

This protocol ensures safe and orderly transition from law enforcement control back to organizational operations.

SCENE RELEASE CONFIRMATION

Obtain Written Documentation

- Request written confirmation of scene release from law enforcement incident commander.
- Confirm which areas are released (may be partial release).
- Confirm whether any areas remain secured.
- Understand whether investigators may need to return.
- Obtain contact information for follow-up coordination.

Understand Limitations

- Clarify any restrictions on released areas.
- Understand evidence that may remain in place.
- Confirm whether photographs or documentation are permitted.
- Clarify whether cleaning or restoration can begin.

INITIAL RE-ENTRY

Safety Assessment Team

- Designate the initial re-entry team (security or facilities staff only).

- Equip the team with communication devices.
- Establish the check-in protocol during assessment.
- Do not allow general employee access until safety is confirmed.

Safety Assessment Checklist

- Structural integrity (check for damage to walls, ceilings, floors)
- Environmental hazards (blood, chemical contamination, broken glass)
- Electrical systems (check for damage, ensure safe operation)
- HVAC systems (check for damage, ensure safe operation)
- Plumbing systems (check for damage, leaks)
- Security systems (check functionality, reset alarms)
- Access control systems (check functionality, reprogram if needed)
- Video surveillance systems (check functionality)
- IT systems (check functionality with IT staff before reconnecting)
- Fire suppression systems (check functionality)
- Emergency lighting and exits (check functionality)
- Immediate hazards requiring mitigation before broader access

Assessment Documentation

- Photograph all damage and hazards.
- Document all systems checked and their status.
- Identify immediate needs before reopening.
- Estimate timeline for addressing identified issues.

ENVIRONMENTAL REMEDIATION (IF NEEDED)

Biological Hazards

- Do not attempt to clean blood or biological materials with regular staff.
- Contract certified biohazard remediation company.
- Ensure compliance with Occupational Safety and Health Administration bloodborne pathogen standards.
- Verify remediation completion before employee re-entry.

Chemical or Other Contamination

- Identify the type and extent of contamination.
- Contract appropriate remediation services.
- Ensure proper disposal of contaminated materials.
- Verify remediation completion and safety before employee re-entry.

Security Enhancements Before Reopening Temporary Measures

- Contracted security services if vulnerability was demonstrated
- Modified access control (limiting entry points, visitor escort requirements)
- Enhanced surveillance (additional cameras, monitored systems)
- Law enforcement presence during initial reopening (coordinate with local agency)
- Panic alarm testing and verification
- Staff notification of emergency protocols review

Permanent Enhancement Planning

- Assess security vulnerabilities revealed by incident.
- Develop proposals for permanent security improvements.
- Budget for security enhancements.
- Plan implementation timeline.

Employee Re-Entry Communication Before Re-Entry

- Inform employees of reopening date and time.
- Describe any facility changes or security enhancements.
- Review emergency procedures and any updates.
- Inform employees of available support services.
- Allow employees to ask questions and express concerns.

First Day Back

- Brief staff meeting to address concerns and answer questions.
- Tour the facility to familiarize employees with any changes.
- Review emergency procedures.
- Remind staff of available support services.
- Maintain heightened supervisory presence and availability.

Ongoing Support

- Monitor employee well-being in the days and weeks following return.
- Maintain flexible arrangements for employees struggling with return.
- Continue to provide employee assistance program access.
- Hold regular check-ins to address emerging concerns.

Customer Communication and Service Restoration Public Notification

- Announce reopening date and time through multiple channels.
- Describe any changes to procedures or facilities.
- Provide alternative service locations if full services is not yet restored.
- Provide contact information for questions.

Modified Operations (If Applicable):

- Clearly communicate any limitations on services.
- Provide a timeline for full service restoration.
- Ensure adequate staffing for anticipated customer volume.
- Monitor customer reactions and adjust as needed.

Documentation Templates

Incident Response Team Meeting Notes Template

- **Meeting Date and Time:** _____
- **Meeting Location:** _____
- **Incident:** _____
- **Law Enforcement IC:** _____

Attendees

- Director of the service center: _____
- Deputy minister: _____
- Facility manager: _____
- HR manager: _____

- Communications officer: _____
- Legal counsel: _____
- Other: _____

Current Situation Summary

Law Enforcement Updates

Personnel Status

- Employees accounted for: _____ of _____
- Employees injured: _____
- Employees providing witness statements: _____
- Customers and visitors accounted for: _____ of _____

Facility Status

- Scene secured by law enforcement: Yes / No
- Estimated scene release time: _____
- Partial release possible: Yes / No / Unknown
- Physical damage: None / Minor / Moderate / Severe
- IT systems: Functional / Compromised / Unknown

Decisions Made

1. _____
2. _____
3. _____

Action Items

- **Action:** _____
- **Responsible Person:** _____
- **Deadline:** _____
- **Status:** _____
- **Next Meeting:** _____
- **Meeting Adjourned:** _____

Daily Resolution Phase Update Template

Date: _____

Incident: _____

Report Prepared By:_____

Distribution: Incident Response Team

24-Hour Summary:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Law Enforcement Status

- Scene release status: _____
- Investigation updates: _____
- Estimated timeline for complete release: _____

Personnel

- All employees accounted for: Yes / No
- Witness interviews completed: _____ of _____
- Employees receiving support services: _____
- Employee concerns or needs: _____

Facility

- Accessible areas: _____
- Secured areas: _____
- Damage assessment progress: _____
- Safety concerns: _____

Communications

- Employee updates provided: Yes / No
- Public statements issued: Yes / No
- Media inquiries received: _____
- Stakeholder notifications: _____

Support Services

- EAP contacts made: _____
- Counseling services arranged: Yes / No
- Legal consultations: Yes / No
- Insurance notifications: Yes / No

Operational Planning

- Alternative service arrangements: _____
- Reopening timeline estimate: _____
- Required actions before reopening: _____

Outstanding Issues

1. _____

2. _____

Next 24-Hour Priorities

1. _____

2. _____

Human Resources and Retirement Checklist

Employee Assistance Program Activation

- ☐ Confirm employee assistance program provider details (provider, phone, website, services, session limit).
- ☐ If no employee assistance program: Identify local mental health providers, explore regional agreements, contact state resources, investigate telehealth, partner with community authorities.
- ☐ Communication plan: Email info, post at facility, include in check-ins, send text, verbal announcement, mail info if facility closed.

Critical Incident Stress Debriefing (CISD)

- ☐ Confirm provider and contact.
- ☐ If unavailable: Contact state resources, regional authorities, telehealth options, neighboring jurisdictions, professional associations.
- ☐ Schedule date, time, location, and facilitator.
- ☐ Participant groups: directly involved employees, witness employees, all other facility employees, management and supervisors

Individual Check-In Protocol

- ☐ Supervisors contact each direct report within 48 hours.
- ☐ Document check-in details (employee name, date and time, assessment, concerns, resources, follow-up).

Practical Support

- ☐ Provide paid time off.
- ☐ Arrange transportation if needed.
- ☐ Assist with workers' compensation claims.
- ☐ Connect employees with financial assistance.
- ☐ Provide benefits information.
- ☐ Arrange meal delivery or other assistance.

Short-Term Support (Weeks 1–4)

- ☐ Flexible return-to-work plan: Assess readiness, determine plan (full-time, gradual, modified duties, remote work, continued leave).
- ☐ Workplace modifications: workspace change, schedule adjustment, productivity expectation adjustment, special accommodations
- ☐ Support services: ongoing employee assistance program counseling, peer support groups, on-site counselor availability, regular supervisor check-ins
- ☐ Review schedule: first review and ongoing frequency

Medium-Term Support (Months 1–6)

- ☐ Monitor for warning signs: absences, fatigue, difficulty concentrating, conflicts, substance use, personality changes, and social withdrawal.
- ☐ Intervention protocol: Have private conversation, express concerns, listen, offer resources, document, follow-up, and escalate to HR if needed.

Anniversary Planning

- ☐ Incident anniversary date
- ☐ Form planning committee (HR, communications, facility, employee representative)
- ☐ Plan recognition: acknowledgment, communication, memorial, support resources, flexibility for time off

Long-Term Support (6 Months and Beyond)

- ☐ Maintain employee assistance program access indefinitely.
- ☐ Continue peer support groups.
- ☐ Keep flexibility policies.
- ☐ Annual review of support needs.
- ☐ Provide resources for delayed trauma responses.
- ☐ Extended care for affected employees: mental health treatment, medical leave, workers' comp, trauma programs, Americans with Disabilities Act accommodations.

Return-to-Work Assessment and Planning

- ☐ Pre-return assessment: physical readiness, psychological readiness, logistical considerations, support network
- ☐ Select return option: full return, gradual return, modified duties, remote work, extended leave
- ☐ First day back protocol: Prepare workspace, brief team, welcome employee, and review security and support resources.
- ☐ Ongoing monitoring and check-ins: week 1, daily; weeks 2 to 4, every other day; months 2 to 3, weekly; months, 4 to 6, biweekly; 6+ months, monthly

Adjustment Protocol

- ☐ If the return-to-work plan isn't working, assess issues, employee input, and triggers.
- ☐ Adjustment options: Modify schedule, change duties, change workspace, increase support services, and return to leave temporarily.

Retirement Support

- ☐ Supervisors provide supportive remarks to the employee.
- ☐ Provide employee assistance program activation if needed.
- ☐ Confirm HR provider and contact.
- ☐ Create an exit plan with the employee.

Appendix F Lessons Learned Tools and Templates

Post-Incident Lessons Learned Checklist

HSEEP-Aligned After-Action Review Guide

Adapt this checklist to your jurisdiction's needs and requirements.

STEP 1: INCIDENT OVERVIEW

Basic Information

- Date:
- Time:
- Location:
- Type of incident:
- Duration:
- Recovery period:

Impact

- Areas affected:
- Employees affected:
- Customers affected:
- Service disruption:
- Agencies involved:

STEP 2: PEOPLE-FOCUSED ANALYSIS

Leadership and Decision Making

- Roles and responsibilities were clear.
- Leadership had sufficient situational awareness.
- Decisions were made at appropriate levels.
- Leadership was visible and accessible.

Staff Response and Behavior

- Staff recognized incident early and responded appropriately.
- Employees were confident using procedures.
- Employees felt empowered to act.
- Stress, fear, and fatigue minimally affected performance.

Communication

- Internal communications were clear, timely, and consistent.
- Staff knew how to report and escalate.
- Public communication was effective.
- Coordination was successful.

Training and Culture

- Employees were adequately trained.
- Employees recalled and used training.
- Culture encouraged reporting and transparency.
- Post-incident support was provided.

Key People Strengths

1._____

2. _____

Key People Gaps

1._____

2. _____

STEP 3: RESOURCES AND TOOLS ANALYSIS

Environmental Design (CPTED)

- Lighting, visibility, and sightlines supported response.
- Building layout helped response.

- Spaces were clearly defined and controlled.
- There were no significant environmental vulnerabilities.

Access Control and Physical Security

- Access control measures functioned as designed.
- Entrances, barriers, and controlled points were effective.
- There were no vulnerabilities in public access areas.
- Physical security features performed as intended.

Technology and Equipment

- Alarms, cameras, and communication tools performed reliably.
- Staff knew how to use the available tools.
- Backups or redundancies were available.
- No technology failures hindered response.

Staffing and Operational Resources

- Staffing levels were sufficient.
- External partners engaged quickly and effectively.
- Supplies and protective equipment were available.

Emergency Plans and Procedures

- Plans were accessible, current, and usable.
- Plans addressed this incident type.
- Procedures were clear and practical under stress.

Key Resource Strengths

1._____

2. _____

Key Resource Gaps

1._____

2. _____

STEP 4: IMPROVEMENT ACTIONS

Issue: _____

Corrective Action:_____

Owner: _____

Resources: _____

Target Date: _____

Priority:_____

Priority Levels

- **High:** Severe vulnerability; implement immediately.
- **Medium**: Moderate vulnerability; implement within 6 months.
- **Low:** Minor vulnerability; implement within 12 months.

STEP 5: VALIDATION AND INTEGRATION

Testing Plan

- Tabletop exercise (date: _____)
- Functional drill (date: _____)
- Full-scale exercise (date: _____)

Plan Updates

- Emergency plans update:
- Facility standards update:
- Training programs update:

Verification

- Progress review frequency:
  ☐ Monthly ☐ Quarterly ☐ Annually
- Overall improvement plan owner:

Knowledge Sharing

- Share across locations or departments:
  ☐ Yes ☐ No
- Share with peer jurisdictions: ☐ Yes ☐ No
- Share with AAMVA: ☐ Yes ☐ No

After-Action Report Template

EXECUTIVE SUMMARY

Incident Overview: [2- to 3-paragraph summary]

Key Findings: [3–5 most important lessons]

Priority Recommendations: [top 3–5 recommendations]

SECTION 1: INCIDENT DESCRIPTION

- Date/time/location: _____
- Incident type: _____
- Duration: _____

Narrative: [chronological description of what occurred]

Timeline:_____

Time: _____

Event: _____

Decision Maker: _____

Agencies Involved: _____

Immediate Outcomes: _____

- Injuries: _____
- Facility damage: _____
- Service disruption: _____
- Financial impact: _____

SECTION 2: ANALYSIS

What Worked Well

- People and performance: _____
- Resources and tools: _____
- External coordination: _____

Gaps and Challenges

- People and performance: _____
- Resources and tools: _____
- External coordination: _____

SECTION 3: RECOMMENDATIONS

CATEGORY	RECOMMENDATION	OWNER	RESOURCES	TARGET DATE	PRIORITY
Training					
Procedures					
Facilities					
Technology					
Staffing					
Communication					

SECTION 4: IMPLEMENTATION

- Overall improvement plan owner: _____
- Review frequency: _____
- Validation plan: _____
- Follow-up review dates: _____

Budget Justification Template

Improvement Request:_____ **Submitted by:** _____ **Estimated Cost:** _____

1. **Incident Background** [Describe the incident that revealed this gap.]
2. **Gap or Vulnerability** [Describe the specific gap and how it affected the response.]
3. **Proposed Improvement** [Describe what you're proposing and how it addresses the gap.]
4. **Risk Reduction Benefit** [Explain what risks this improvement reduces or eliminates.]
5. **Cost–Benefit Analysis**

   Costs

   - Initial investment: _____
   - Implementation: _____
   - Training: _____
   - Ongoing maintenance: _____

   Benefits

   - Risk reduction value: _____
   - Incident cost avoidance: _____
   - Employee safety improvement: _____
   - Operational efficiency gains: _____

6. **Alternatives Considered** [Why this proposal is preferred over alternatives]
7. **Implementation Timeline** Target completion:
8. **Consequences of Not Funding** [What risks remain if not implemented]

Lessons Learned Sharing Template for AAMVA

Jurisdiction: _____ **Incident Date:** _____

Contact: _____

1. Incident Overview

- Type: _____
- General location: [state or region] _____
- Facility type: _____
- Time of day: _____

2. Context [relevant context without compromising security]

3. What Happened [general description for learning purposes]

4. Response Actions [what worked well]

5. Challenges Encountered [difficulties without assigning individual blame]

6. Key Lessons Learned

- For MVA administrators: _____
- For frontline staff: _____
- For security planning: _____
- For facility design: _____

7. Improvements Implemented [what you're doing differently]

8. Recommendations for Peers [what other jurisdictions should consider]

9. Resources That Would Have Helped [what would have been valuable]

Note: These tools support systematic lessons learned processes that translate experience into enhanced preparedness. Customize for your jurisdiction's needs. Use these tools. Share your experiences. Learn from others. Together, we build a culture of safety and continuous improvement.

Appendix G Glossary

active threat — An immediate and ongoing situation in which an individual or individuals are actively engaged in causing or attempting to cause death or serious physical harm to others within a facility or its vicinity. An active threat is distinguished from a general security disturbance by its immediacy and lethality. Response protocols differ significantly from those used in disturbance or de-escalation situations. See also Run, Hide, Fight.

after-action review (AAR) — A structured evaluation conducted following any drill or real-world incident. The AAR identifies what worked; what did not; and where procedures, training, or facilities need improvement. It should involve both internal staff and, when possible, outside observers to prevent organizational bias. Findings should be documented and used to update the Emergency Action Plan and related training materials.

bystander effect — A psychological phenomenon in which individuals fail to act during an emergency because they assume someone else has already taken action. Emergency Action Plans must explicitly counter this tendency by authorizing and expecting all employees who witness life-threatening events to immediately call 911 and alert others, regardless of whether they believe someone else may have already done so.

CISA (Cybersecurity and Infrastructure Security Agency) — An agency of the U.S. Department of Homeland Security responsible for protecting the nation's critical infrastructure from physical and cyber threats. CISA provides resources, training, assessments, and guidance to help public and private sector organizations strengthen their security posture. For MVA facilities, CISA is a primary federal resource for active threat preparedness, facility security assessments, and employee safety training, including the Run, Hide, Fight framework. CISA resources are available at no cost to government agencies at cisa.gov.

closing sweep — A daily end-of-business protocol in which designated staff inspect the entire facility, including restrooms, storage areas, and less-trafficked spaces, to confirm that no unauthorized individuals remain in the building before it is secured for the night. The closing sweep is a foundational access control measure and should be documented and assigned to specific roles in the Emergency Action Plan.

code words or plain language protocols — Pre-established verbal signals, alarm tones, or code phrases used over public address systems or intercoms to communicate specific emergency actions such as evacuation, lockdown, or shelter in place without creating panic or confusion among the public. All staff should be trained in their agency's code word and plain language system and practice it during drills.

containment	Both a phase of the Security Management System lifecycle and a category of action taken to limit the scope and impact of an incident after it has been identified. As a lifecycle phase, containment follows Identification and precedes resolution. As an action, containment may include verbal de-escalation, physical separation of parties, activation of emergency protocols, or other measures designed to stop a situation from expanding. The appropriate containment strategy depends on the nature and severity of the threat.
CPTED (Crime Prevention Through Environmental Design)	A security philosophy that uses the physical layout and design of the built environment to deter criminal behavior and enhance safety. CPTED strategies include natural surveillance (clear sightlines), territorial reinforcement (clearly defined public versus employee zones), access control through design, and environmental maintenance. MVA facilities are encouraged to use a formal CPTED assessment as part of their facility security planning.
culture of safety	An organizational mindset in which security is understood as a core component of customer service and employee well-being, not an obstacle to operations. Building a culture of safety requires visible leadership commitment, consistent training, accessible reporting pathways, and agency-wide participation in security practices. It reflects the understanding that every employee has a role in maintaining a safe environment.
de-escalation	A set of verbal and behavioral techniques used to reduce the intensity of a conflict or potentially threatening situation before it reaches a point requiring physical intervention or emergency response. De-escalation should always be the first response when circumstances permit. Staff should be trained to recognize when de-escalation is no longer appropriate, including when a customer is impaired, when the situation is deteriorating despite de-escalation attempts, or when a threat appears imminent, and to transition swiftly to emergency protocols.
duty of care	The legal and ethical obligation of an employer to take reasonable steps to protect employees, customers, and others from foreseeable harm within the workplace. In the context of MVA facility security, duty of care informs decisions about training, physical security investment, incident response protocols, and threat assessment practices. Agencies that fail to act on known or reasonably foreseeable risks may be found to have breached this obligation.
Emergency Action Plan (EAP)	A written, agency-specific document that outlines the procedures employees should follow in response to emergencies, including fire, medical events, active threats, natural disasters, and other critical incidents. The EAP identifies evacuation routes, shelter and rally point locations, designated personnel responsibilities, communication protocols, and coordination procedures with local emergency responders. The EAP should be reviewed at least annually, communicated to all staff, and incorporated into agency training and drills. Note: Do not confuse with Employee Assistance Program, which is spelled out in full throughout this document to avoid confusion.

employee assistance program — A confidential, employer-sponsored resource that provides employees with access to professional support services, including mental health counseling, crisis intervention, financial guidance, and referral services. In the context of the Security Management System, the employee assistance program plays a critical role in the recovery phase following a critical incident, supporting staff who may be experiencing trauma, stress, or other psychological impacts. Agencies should ensure employees are aware of this resource before an incident occurs, not only after. Note: This term shares the abbreviation EAP with Emergency Action Plan. Throughout this document, EAP refers exclusively to the Emergency Action Plan.

hardening — Physical and procedural modifications made to a facility to reduce its vulnerability to unauthorized entry, violence, or other security threats. Hardening measures may include installing security cameras, reinforcing entry points, adding barriers or access control systems, improving lighting, and establishing clear sight lines. Hardening is a core component of the preparation phase of the Security Management System lifecycle and is most effective when informed by a formal facility security assessment.

incident commander — The law enforcement or emergency management official who assumes authority over an active incident scene upon arrival of first responders. When an incident commander is onsite, agency staff defer to their direction and do not take independent action related to the threat. The role of MVA management shifts at this point to supporting responders with information, facilitating access, and managing unaffected staff and operations.

lockdown — A protective protocol activated when a threat is present inside or immediately adjacent to a facility, making evacuation unsafe. During a lockdown, all exterior and interior doors are secured, lights may be turned off, and staff and customers shelter in place until law enforcement clears the building. Lockdown is the most restrictive of the three primary protective protocols. Distinct from lockout (external threat, doors secured, business may continue inside) and shelter in place (environmental hazard, staff move to interior safe areas). See also lockout, shelter in place.

lockout — A security protocol activated when a threat exists in the surrounding area but has not entered the facility, and full evacuation or lockdown is not yet warranted. During a lockout, exterior doors are secured, and business may continue inside the building while law enforcement addresses the external situation. Distinct from lockdown (threat inside the facility) and shelter in place (environmental or atmospheric hazard). Agencies should establish clear criteria for activating a lockout and ensure all staff understand the distinction. See also lockout, shelter in place.

NIMS (National Incident Management System) A standardized framework developed by the Federal Emergency Management Agency that establishes a common language, organizational structure, and set of protocols for emergency response across agencies and jurisdictions. Aligning MVA security protocols with NIMS facilitates seamless coordination with law enforcement, fire services, and emergency medical responders during a crisis.

operational disruption Any event that interrupts or significantly impairs normal agency operations, including but not limited to system outages, facility damage, civil unrest in the surrounding area, environmental hazards, or staffing emergencies. Operational disruptions are distinct from active threats in that they do not necessarily involve direct violence or imminent physical danger. However, they require a planned response, clear communication protocols, and defined decision authority.

public-view monitor A video display screen positioned so that members of the public can see themselves being recorded by security cameras. Public-view monitors serve as a proven behavioral deterrent by increasing self-awareness and reducing the likelihood of aggressive or disruptive conduct. They are a low-cost, CPTED-aligned hardening measure appropriate for most MVA customer service environments.

radius of concern A predefined geographic and situational boundary around an MVA facility that determines when an external incident triggers a protective response such as a lockout. Decision thresholds, including the type of incident, its proximity to the facility, and relevant contextual factors, should be established in consultation with local law enforcement and documented in the Emergency Action Plan. Defining the radius of concern in advance removes hesitation during a crisis and ensures consistent application across shifts and leadership changes.

rally point A designated location at a safe distance from a facility where staff and customers congregate and are accounted for following an evacuation. Agencies should designate both a primary and a secondary rally point. The secondary location serves as an alternate gathering site if the primary becomes unsafe because of hazmat conditions, wind direction, proximity to an active threat, or other evolving circumstances. Rally points should be documented in the Emergency Action Plan and practiced during drills.

Run, Hide, Fight A survival response model recommended by the U.S. Department of Homeland Security for responding to active threat situations. Run instructs individuals to evacuate immediately if a safe path exists, leaving belongings behind. Hide directs individuals to barricade and shelter in a secure location when evacuation is not possible.

Fight authorizes individuals to use any available means to survive only as an absolute last resort when no other options remain. Training on this model should be scenario-based and regularly practiced. See also active threat.

secure help room	A designated room within the employee-only area of a facility where staff can retreat if a threat breaches the service counter or public area. The room should feature a reinforced door with a deadbolt, a hardline telephone, a copy of the Emergency Action Plan, a first aid kit, and emergency contact information. Placement should allow quick, unobtrusive access from customer service stations without requiring staff to pass through public areas.
Security Management System (SeMS)	A cyclical, programmatic approach to physical security that integrates safety into the daily operations and culture of an agency. SeMS replaces reactive, checklist-based security with a proactive system of ongoing planning, risk assessment, training, and continuous improvement. The six-phase incident response lifecycle—preparation, identification, containment, resolution, recovery, and lessons learned—is the operational framework of the SeMS.
shelter in place	A protective protocol used primarily in response to environmental or atmospheric hazards such as tornadoes, severe weather, or hazardous material incidents in the surrounding area. During shelter in place, staff and customers are directed to designated interior safe rooms or hardened spaces away from windows and exterior walls. Distinct from lockdown (internal security threat requiring barricading) and lockout (external security threat with doors secured but operations continuing). See also lockdown, lockout.
tailgating	The practice, whether intentional or inadvertent, of an unauthorized individual gaining access to a secured area by following closely behind an authorized person as they enter. Also referred to as piggybacking. Tailgating is one of the most common ways physical access controls are bypassed and does not require technical skill or forced entry. Staff should be trained to avoid holding secured doors open as a courtesy and to politely challenge or report individuals who do not badge in independently.
Threat Assessment Team (TAT)	A multidisciplinary group of trained staff responsible for receiving reports of concerning behavior, evaluating the nature and level of risk, and coordinating an appropriate organizational response. TAT members typically represent management, human resources, legal, and agency security or law enforcement partners. The TAT operates with a proactive orientation, identifying warning signs early and intervening before situations escalate, and is responsible for balancing privacy obligations with the agency's duty to protect the safety of staff and the public.

Appendix H Employee Safety and Security Working Group Roster

CHAIR

Jeannelle Yitagesu
Director
South Dakota Department of Public Safety

MEMBERS

Michelle Poirier
Deputy Registrar
Prince Edward Island Transportation and Infrastructure

Jennie Hoggatt
Field Operations Director
Texas Department of Public Safety

Tina Braddy
Regional Manager, Bureau of Field Services
Wisconsin Division of Motor Vehicles

Benjamin "Mitch" Mitchell
Director, Driver Control Section
Colorado Division of Motor Vehicles

Crandall Heard
General Counsel
Georgia Division of Driver Services

Matthew Kestian
General Counsel
Indiana Bureau of Motor Vehicles

Robert Keener
Special Operations Bureau Commander
Kansas Highway Patrol

Even Sether
Captain, Criminal Investigations Division
Oregon State Police

C. Dylan Huff
DMV Investigator
South Carolina Department of Motor Vehicles

James Dilisio
Assistant Registrar of Service Center Operations
Massachusetts Registry of Motor Vehicles

AAMVA STAFF

Darcy Doty
Project Manager
Vice President, Motor Vehicle Administration Operations & Customer Experience

Paul Steier
Vice President, Law Enforcement Programs and Services

OUR VISION

Safe drivers
Safe vehicles
Secure identities
Saving lives!

American Association of Motor Vehicle Administrators
4401 Wilson Blvd, Suite 700
Arlington, Virginia 22203
703.522.4200 | **aamva.org**