

Area Safety and Security Action Plan



Agency of Administration
Department of Buildings and General Services
Office of State Security Programs

ASAP

Area-Wide Safety/Security Action Plan

Table of Contents

TITLE

Response to Emergencies Situations/incidents

BIOLOGICAL SPILL RESPONSE

BOMB THREAT

BOMB THREAT CHECKLIST

CHEMICAL BIOLOGICAL RADIOLOGICAL AND/OR NUCLEAR

INCIDENT CBRN

CIVIL DISTURBANCE

EARTHQUAKE EMERGENCY

ELEVATOR MALFUNCTION

EVACUATION PROCEDURES

EVACUATION PROCEDURES – AFTER THE IMPACT

FIRE EMERGENCY

FLOOD OR WATER EMERGENCY

HAZARDOUS MATERIAL SPILL

MAIL HANDLING

MEDICAL EMERGENCY

PANIC ALARMS/BUTTONS

POWER FAILURE

SUSPICIOUS FUMES

SUSPICIOUS PERSON, HOSTILE INTRUDER, HOSTAGE/WEAPONS

SITUATION (RESPONSE TO)

TORNADO EMERGENCY

WEATHER EMERGENCY (DECLARED)

WORKPLACE VIOLENCE

Procedures & Regulations

COMMUNICATION PLAN

COMPUTER, INTERNET & INFORMATION SECURITY

PARKING REGULATIONS IN STATE OWNED PARKING LOTS

STATE EMPLOYEE IDENTIFICATION CARD

TRANSPORTATION, PERSONAL & PUBLIC

VEHICLE TROUBLE

VIDEO-MONITORING EQUIPMENT, USE OF

Responsibilities – Emergency Response Personnel & Employees

EMPLOYEES RESPONSIBILITIES

EMERGENCY BUILDING CONTACT INFORMATION

INCIDENT RESPONSE TEAM (IRT) RESPONSIBILITIES

SAFETY AND SECURITY COORDINATORS RESPONSIBILITIES

SAFETY WARDEN RESPONSIBILITIES

SAFETY WARDEN CHECKLIST

Maps, Floor Plans, Lists, Forms

ACRONYMNS

ASSEMBLY AREA, EMERGENCY

BUILDING FLOOR PLAN

DEFINITIONS

DISASTER EMERGENCY, STATE'S RESPONSE

EMPLOYEE INFORMATION FORM

EXIT INTERVIEW CHECKLIST

NATIONAL INCIDENT COMMAND REFERENCES

THREAT LEVEL – GREEN, BLUE, YELLOW, ORANGE, RED

DEFINITIONS

Safety and Security Coordinator: The Safety and Security Coordinator (SSC) is designated by a Secretary or Commissioner and will represent the Agency or agencies within a geographical area or building. The SSC will have decision making authority, in consultation with management, Secretary and/or Department heads and the Office of State Security Programs, concerning emergency procedures as identified in the ASAP.

Alternate Safety and Security Coordinator: The Alternate Safety and Security Coordinator (ASSC) is designated by a Secretary or Commissioner and will represent the Agency or agencies within a geographical area or building. The ASSC will have decision making authority (in the absence of the SSC), in consultation with management, Secretary and/or Department heads and the Office of State Security Programs, concerning emergency procedures as identified in the ASAP.

Safety Wardens: Safety Wardens are appointed by their Safety and Security Coordinators (SSC) or volunteer. They coordinate, educate and act as a liaison between security and co-workers.

Alternate Safety Warden: Alternate Safety Wardens are appointed by their Safety and Security Coordinators (SSC) or volunteer. They coordinate, educate and act as a liaison between security and co-workers when the Safety Warden is absent or requires additional assistance.

District Facility Manager: District Facility Manager (DFM) provides oversight of Plant Maintenance Supervisors, skilled, semi-skilled and unskilled employees of each state owned building within his/her district. Facilities include buildings, grounds, and related support systems.

Incident Response Team: Members of management and/or staff appointed and trained to respond to all emergency situations within their facility in support of the SSC.

Disaster Recovery Team: Effective disaster recovery requires a team-coordinated approach. Personnel involved in disaster recovery planning and response are: Designated Essential Employees, Senior Teams, Finance, Division Business Offices, program administrators and Safety and Security Coordinators (SSC), information technology personnel, mail and supply personnel, risk management personnel, telecommunications personnel, security personnel, District Facility Managers, Emergency Operations Center's coordinators and other employees as identified.

Safety and Security Workplace Committee: A Safety and Security Workplace Committee is a key element to achieving continuous improvement in a safety and security. The purpose of a safety and security committee is to regularly bring workers and management together in a non-adversarial, cooperative effort to promote safety and security in the workplace. The committee assists the managers and makes recommendations for change regarding safety and security issues. The committee's primary focus is to detect and correct workplace hazards.

- The specific functions of the safety committee are to:
 - Detect hazards;
 - Analyze and solve problems; and
 - Assist in the management of safety and security.

- The specific duties of the safety committee include:
 - Facilitate cooperation between management and employees in initiating, developing, carrying out and monitoring measures designed to ensure the health, safety and welfare of employees;

- Assist in the resolution of safety and security issues at the workplace;
- Assist in the formulation and dissemination (in appropriate languages) of policies, practices and procedures that promote a safe and secure workplace;
- Assist with the development of accident and investigative reporting procedures; and
- Advise the employer on any proposed or actual changes to health and safety policies, practices and procedures at the workplace.
- Committees may also carry out additional duties specific to their own organizations.

**IMPORTANT INFORMATION TO KNOW
EMERGENCY BUILDING CONTACT INFORMATION**

**Osgood Building
Waterbury, Vermont**

*REMEMBER: YOU MUST FIRST DIAL "9" FROM A STATE PHONE TO GET AN OUTSIDE LINE
(example: 9-555-1234)*

BUILDING:

Safety and Security Coordinator (SSC) Office

<i>POC</i>	<i>Position</i>	<i>Office</i>	<i>Office</i>	<i>Cell</i>	<i>Email</i>

BGS:

<i>POC</i>	<i>Position</i>	<i>Office</i>	<i>Office</i>	<i>Cell</i>	<i>Email</i>
Montpelier: 24/7	Security Office	BGS	828-0777		

Department of Human Resources: **828-3491**
Emergency number for Human Resources: **800-644-4402**

EMERGENCY:

Police Department **911**
Fire Department **911**
Vermont State Police **911**
Security Office **828-0777**

AGENCY/DEPARTMENT EMERGENCY INFORMATION LINE:

Emergency Information Line **800-644-4402**

ASSEMBLY AREA: _____

(for temporary building closure: safe distance from your building but within walking distance)

ALTERNATE WORK LOCATION: _____

(In the event your building is closed - report to this location. If a location is not designated, contact your Safety and Security Coordinator (SSC)/supervisor for instructions.)

SAFETY WARDENS FOR YOUR OFFICE

<i>Safety Warden</i>	<i>Rm/Location</i>	<i>Floor</i>	<i>Office telephone</i>	<i>Cell</i>	<i>Email</i>

ASAP ON-LINE:

The ASAP On-Line website is located on the BGS Security Web page

<http://www.bgs.state.vt.us/security/forms/BGS-SEC-Vermont-ASAP-Manual.pdf>

EMPLOYEES RESPONSIBILITIES

The success of the Agency-Wide Safety/Security Action Plan (ASAP) relies upon each and every employee, regardless of rank or physical location, to respect and become familiar with the safety, security and emergency response procedures of their Agency or Department. The following responsibilities should be viewed as standard response and awareness guidelines for all employees at all locations:

Employees at all buildings shall:

- Support and be familiar with the safety and security procedures known as the Agency-wide Safety/Security Action Plan (ASAP).
- Treat every alarm as a real event.
- Participate in safety and security training opportunities (e.g., mock exercises such as fire drills).
- Be aware of changes around your desk and work site such as suspicious persons and packages and take appropriate action.
- Escort visitors to and from your office area to the reception area.
- Display your building identification badge(s) at all times.
- Be reminded that depending on security risks, packages, handbags, briefcases and other containers may be subject to inspection.
- Immediately report lost or stolen identification badges to building security.
- Be familiar with the “Important Numbers to Know” to reach appropriate safety or security personnel in an emergency.
- Be familiar with your assigned role in the event of an emergency.
- Know your office’s designated Assembly Area (outside of building, but within walking distance).
- Know your office’s alternate work location (in the event your building is closed)
- During declared emergencies, call the Emergency Information line for instructions at **800-644-4402**

Biological Spill Response

If there is a biological / blood spill in your facility, utilize the following procedures for proper clean-up.

Immediate Procedures:

- Close doors to the affected area and prevent unauthorized access.
- Contact the SSC.
- Assign a person familiar with incident and facility to assist emergency personnel and to provide them with information.
- Disinfect contaminated areas with 10% bleach solution **only** if you are Bloodborne Pathogen trained and have the proper personal protective equipment.

Biological Spill on Body:

- Remove any contaminated clothing.
- Carefully wash the exposed area with soap and water for 1 minute, taking care not to cause any injury or breakage to the skin.
- For contamination of mucous membranes (eyes, nose and mouth). Flush contaminated area with running water for several minutes.
- Obtain medical assistance.

Minor Cuts and Puncture Wounds (Including Needle Stick Injuries):

- Carefully wash the injury with soap and water for several minutes.
- Obtain medical assistance and recommendations about post-exposure medical treatment for potential bloodborne illness.

Group Discussion:

- Identify any biological spill incidents that have occurred in the past, how were they handled?
- If a spill was to occur, who would you contact for the clean up? If you are performing the cleanup what necessary protective steps would you need to implement to ensure your safety?
- Determine if you or anyone in the group needs Bloodborne Pathogens Training?
- Take time to assess your PPE, determine if you need to order any equipment.

PPE- Ensure that you wear appropriate PPE for spill cleanup.



Bomb Threat

While most threats are false or misleading and designed to disrupt work or school, there is always the potential that the threat is real. This protocol is intended to provide guidance to employees and managers who may be faced with a bomb threat.

Receipt of a Bomb Threat

1. In the event of a written threat, all written materials should be collected and handled as little as possible to preserve any fingerprints that may exist.
2. The person receiving a phone threat should make every effort to gather as much information as possible about the caller and the suspected device.
Located at <http://www.bgs.state.vt.us/security/forms/BGS-SEC-Vermont-ASAP-Manual.pdf>
3. The person receiving the bomb threat should keep the caller on the phone as long as possible.
4. Record every detail, including caller ID information, on what extension the call was received, and the time of the call. Management should be notified immediately in the event of the bomb threat.

After the Threat has been Received

1. The receiver of the call or a co-worker should notify a supervisor, who is then responsible for notifying the Safety and Security Coordinator (SSC) and calling 911.
2. The receiver of the call should immediately bring all information about the bomb threat to the SSC and the responding police department. The SSC should identify him/herself to law enforcement and brief the responding officer on the current status of the incident.

Bomb Threat Management

1. Members of Security and Incident Response Team may be asked to assist the SSC. Additionally, maintenance and custodial staff members will be contacted to assist as needed.
2. The SSC has the authority to decide: to evacuate or not to evacuate, and if so, to re-enter the building. The manager in charge in conjunction with law enforcement officials will assess the bomb threat to make an informed decision about how to proceed.*
3. The decision to search and/or evacuate will be made by the SSC after evaluating these factors:
 - a. Seriousness/Circumstances, credibility of the threat
 - b. Available resources to react/respond to the threat
 - c. Operational impact
 - d. Planned events of the day
 - e. Number of other recent unsubstantiated threats to the area
 - f. Whether suspicious items or packages have been observed for any period of time.
 - g. The location of the threatened building
 - h. The content of the threat itself.
 - i. How detailed in nature was the threat.

* The decision to evacuate a building in response to a bomb threat is separate and distinct from the decision to close a building due to an emergency. The Secretary of Administration, or his/her designee, has the sole discretion to determine whether conditions warrant an emergency closing or reduced workforce for a State building.

Evacuation/Search

1. Without unduly delaying evacuation, employees in the affected building should quickly search their work areas (desk, office space) for anything or anyone that looks unusual or suspicious prior to leaving the building. The employees should not touch or move anything that looks suspicious. The employees will exit the building and report to a pre-determined meeting point and report their findings to a supervisor, who will notify the SSC, and remain at the designated meeting place until released by the SSC or are told to reoccupy the building by the SSC.
2. Incident Response Team (IRT) with the assistance of local public safety representatives will conduct a search of the facility and surrounding area. Search functions will start and end at a designated area to account for all search team members.
3. Do not use radios, cell phones, pagers (if on turn off) or elevators during a search operation.
4. Law enforcement will advise and assist as appropriate. It is imperative that everyone comply with any instructions from the responding law enforcement officer(s) as s/he assesses the potential danger and/or assists with the search.
5. If applicable, law enforcement/security will help secure the entrances to the building, prohibiting entry until authorization has been given by the SSC.

Building Re-entry

1. The building should not be reoccupied by employees or the public until the search team has completed a search of the building and premises and clearance has been given by the SSC.
2. If employees are allowed to reoccupy the building, the employees should again search their work areas before continuing work and immediately report anything new or suspicious.

Safety and Security Coordinator:

Incident Response Team:

Designated Meeting Points:

BOMB THREAT CHECKLIST

CALLERS VOICE:

- | | |
|-----------------------------------|--|
| <input type="checkbox"/> Calm | <input type="checkbox"/> Nasal |
| <input type="checkbox"/> Angry | <input type="checkbox"/> Stutter |
| <input type="checkbox"/> Excited | <input type="checkbox"/> Lisp |
| <input type="checkbox"/> Slow | <input type="checkbox"/> Raspy |
| <input type="checkbox"/> Rapid | <input type="checkbox"/> Deep |
| <input type="checkbox"/> Soft | <input type="checkbox"/> Clearing throat |
| <input type="checkbox"/> Laughter | <input type="checkbox"/> Deep breathing |
| <input type="checkbox"/> Crying | <input type="checkbox"/> Cracking voice |
| <input type="checkbox"/> Normal | <input type="checkbox"/> Disguised |
| <input type="checkbox"/> Distinct | <input type="checkbox"/> Accent |
| <input type="checkbox"/> Slurred | <input type="checkbox"/> Familiar |
| <input type="checkbox"/> Squeaky | <input type="checkbox"/> Whispered |

If voice is familiar, who did it sound like?

BACKGROUND SOUNDS:

- | | |
|------------------------------------|---|
| <input type="checkbox"/> Street | <input type="checkbox"/> Factory machines |
| <input type="checkbox"/> Crockery | <input type="checkbox"/> Animals |
| <input type="checkbox"/> Voices | <input type="checkbox"/> Clear |
| <input type="checkbox"/> PA System | <input type="checkbox"/> Static |
| <input type="checkbox"/> Music | <input type="checkbox"/> Local |
| <input type="checkbox"/> House | <input type="checkbox"/> Long distance |
| <input type="checkbox"/> Motor | <input type="checkbox"/> Booth |
| <input type="checkbox"/> Office | <input type="checkbox"/> Other |

THREAT LANGUAGE:

- | | |
|--|--|
| <input type="checkbox"/> Well Spoken
(Educated) | <input type="checkbox"/> Incoherent
Tape |
| <input type="checkbox"/> Foul | <input type="checkbox"/> Message read by
threat maker |
| <input type="checkbox"/> Irrational | |

Remarks

REPORT CALL IMMEDIATELY TO:

Security: 828-0777

Police 911

**I HAVE A BOMB THREAT
CALLER ON THE PHONE**

**TELL THE SUPERVISOR OR
SAFETY AND SECURITY
COORDINATORS (SSC)**

**NOTIFY POLICE AT
9-911**

**STATE SECURITY AT
802-828-0777**

Chemical, Biological, Radiological and Nuclear

Before an CBRN-based incident occurs, familiarize yourself with this section and refer to the Disaster Recovery plans for additional instructions.

What to do if you are exposed to a potential NBC agent:

1. Do not further handle the piece or package suspected of contamination.
2. Notify **Security at 828-0777**.
3. Make sure that damaged or suspicious packages are isolated in place and the immediate area cordoned off.
4. Evacuate the immediate area beyond the perimeter of those exposed.
5. Make a list of all persons who have touched the letter and/or envelope. Include contact information. Provide the list to the SSC.
6. As soon as practical, shower with soap and water.
7. Place all items worn when in contact with the suspected items in plastic bags and keep them wherever you change your clothes and have them available for law enforcement agents.

Evacuation Procedures:

1. Remain calm.
2. Cover your nose and mouth with a cloth, coffee filter, paper towels, etc.
3. Take shallow breaths.
4. Follow the evacuation directions of your Safety Warden and Safety and Security Coordinators (SSC).

Civil Disturbance

A civil disturbance is defined as the presence and result of a riot, a protest, a physical commotion or a need for crowd control.

Upon awareness of a civil disturbance, do the following:

1. Remain calm. Contact *Security and/or your Safety and Security Coordinator*. do not draw any attention to yourself.
2. SSC and/or *Security* will establish contact with the appropriate law enforcement unit(s) and will provide the following information:
 - Type of event:
 - Location:
 - Size of group:
 - Identity of the groups' leader(s) (if possible):
 - Any visible weapons:
 - Types of vehicles and license plate numbers:
3. Leave the immediate area of the disturbance for your own safety.
4. Keep yourself and co-workers away from the situation for their own safety. If you are in your work area and not in the immediate area of the situation remain in your work area unless directed to relocate.
5. Avoid window areas; draw window blinds and keep curtains closed.
6. SSC and/or Security will notify your office when the situation is controlled.

Earthquake Emergency

Although earthquakes are rare in Vermont, Earthquakes strike without warning and the major shock is usually followed by numerous, after shocks, which may last for weeks or months. An earthquake's effect on buildings will vary from building to building. Fire alarm or sprinkler systems may be activated by the shaking. Elevators and stairways will need to be inspected for damage before they can be used.

The major threat of injury during an earthquake is from falling objects and debris, and many injuries are sustained while entering or leaving buildings. Therefore, it is important to remain inside the building and quickly move away from windows, glass and free standing partitions and shelves. Take cover under a sturdy desk or table, in a doorway, or against an inside wall until the shaking stops.

Procedures

Give DROP AND COVER command.

1. After shaking stops, check for injuries, and render first aid if you are able
2. If ordered by SSC, evacuate.
3. DO NOT return to building.
4. DO NOT light any fires.
5. Keep a safe distance from any downed power lines.
6. Stay alert for aftershocks
7. SSC will issue further instructions.

Drop and Cover Procedures

Inside Building

1. Get under desk or table or other sturdy furniture with back to windows.
2. If not near any furniture, sit in a corner or with back against a wall with back to windows.
3. Drop to knees, clasp both hands behind neck, bury face in arms, make body as small as possible, close eyes, and cover ears with forearms.
4. If jackets or other non-breakable objects are handy, hold over head for added protection.
5. Stay away from windows, bookcases, or other heavy objects.
6. Maintain position until shaking stops.

Outside Building

1. Assume DROP AND COVER position in an open space.
2. Maintain position until shaking stops.
3. Move away from buildings, trees, overhead wires, and poles.
4. Do NOT enter building until it is determined to be safe.

If trapped inside after an earthquake:

1. Replace all telephone receivers.
2. Identify working forms of communication – cell phones, office phones, etc.
3. Turn on the radio for information. A radio with back-up battery is suggested in case electric power is disrupted.
4. Evaluate situation and coordinate actions with co-workers and other building tenants.
5. Do not move debris or objects – it may trigger the collapse of a nearby structure.
6. Assess area for gas or liquid leaks or other hazards in your area, if hazards are located provide location, if safe to do so, to co-workers and others in the area.

7. If power outage, do not use candles or lighters until determined safe to do so.
8. Check for fires and extinguish fires if at all possible.
9. Power down computers and lamps. Do not turn on light switches or appliances.
10. Do not flush toilets until authorized by building management.
11. If trapped, listen for emergency evacuation teams -- above you, below you and around you.
12. Remain calm and encourage others to do the same. Help is on the way.

Elevator Malfunction

The following tips are provided in the event you are riding in an elevator that becomes stalled:

1. Please remain calm.
2. **DO NOT** attempt or allow anyone to help you crawl out of a stalled elevator that is between floors (i.e., when the floor of the elevator and the floor of the building are not level with one another). The elevator could start up at any time.
3. Call for assistance by pressing the call/intercom button.
4. Provide as much information as possible concerning the stalled elevator such as:
 - a. Elevator number.
 - b. Nearest floor level if it can be determined.
 - c. Number of people and names of individuals on the elevator.
5. All efforts will be made to release individuals as quick as possible. Recognize that it may take some time for technicians to assess the situation and devise a plan to correct the problem and/or free the persons on the elevator. Elevator technicians may have to enter the elevator shafts to assess the problem.

Fire Emergency

Before a fire occurs, familiarize yourself with this section and refer to the Disaster Recovery plans for additional instructions.

Upon discovery of a fire, take the following action:

1. Pull the fire alarm. See your floor plan.
2. Proceed to the nearest stairwell and exit the building.

During evacuation, follow these fire safety procedures:

1. Use the stairwell exits only.
2. **Do not** use the elevators!
3. Keep doors closed, especially in the stairwells.
4. **Do not** attempt to fight the fire.
5. Stay low – air is cooler and cleaner closer to the floor
6. If caught in heavy smoke, take **short** breaths and **crawl** to escape.
7. Hold a wet cloth over your mouth and nose – use coffee filters, clothing, etc.
8. Test doors by using the back of your hand before opening. **Do Not** open warm doors. Open cool doors slowly; close quickly if you encounter smoke or flames. Use another escape route.
9. Should your clothing catch fire, **Do Not Run**. Stop, drop, cover face with hands and roll until fire is out.
10. Exit the building – do not attempt re-entry until advised it is safe to return.

If trapped inside during a fire emergency:

1. **Do not** break windows.
2. Keep doors closed.
3. Stuff cracks around doors and vents to keep smoke out.
4. Anticipate low or no visibility – do not panic.
5. If caught in heavy smoke, take **short** breaths and **crawl** to escape.
6. Stay low – air is cooler and cleaner closer to the floor.
7. Hold a wet cloth over your mouth and nose – use coffee filters, clothing, etc.
8. Listen for emergency evacuation teams.
9. Remain calm and encourage others to do the same. Help is on the way.
10. Wait at a window and signal for help with a flashlight or by waving a light-colored cloth.

DO NOT PANIC:

Stay calm during a fire emergency. Several fire safety elements exist in most buildings to protect the tenants of the building such as fire alarm/monitoring systems, sprinkler systems, etc.

Flood or Water Emergency

Before a water or flood emergency occurs, familiarize yourself with this section and refer to the Disaster Recovery plans for additional instructions.

When a flood or leak is identified, take the following action:

- Contact your Safety Warden.
- Contact Security at 828-0777
- Avoid the wet area to prevent injury or electrical shock.

Your building management will initiate necessary repairs to restore to normal operations.

Hazardous Material Spill

Before a hazardous material spill occurs in your work area, familiarize yourself with this section. For hazardous spills in the community, please monitor media reports and refer to the Disaster (Business) Recovery Plans for additional instructions.

For identifiable hazardous material spills in your work area:

- Learn the emergency procedures that are posted in a visible location.
- **If procedures are not posted, contact Security or Building maintenance.**

For un-identifiable hazardous material spills in your work area:

- Evacuate immediate area until hazardous material is identified.
- Contact **Security at 828-0777**
- Do not attempt clean up until experts arrive.

Mail Handling

The receipt of mail and packages are common in the normal course of our daily business. Although it is unlikely that employees will receive a piece of mail that contains a biological/chemical agent or bomb, employees should be familiar with the following information and guidelines:

What constitutes a "suspicious" parcel/letter?

The U.S. Postal inspectors identify the following characteristics that may constitute a suspicious letter or parcel that:

- is unexpected or from someone unfamiliar to you
- is addressed to someone no longer with your organization or are otherwise outdated
- has no return address or has an address that can't be verified as legitimate
- has incorrect spelling of addressee's name or title
- shows a city or state in the postmark that is a different location than the return address
- is unprofessionally wrapped with several combinations of tape used to
- secure the package and may be endorsed "Fragile – Handle with Care" or "Rush – Do Not Delay"
- is marked with restrictive endorsements, such as "personal" or "confidential"
- has excessive postage
- is of unusual weight
- feels rigid, or appears uneven or lopsided, have an irregular shape, soft spots or bulges.
- has protruding wires, leaking liquid, powder residue, strange odors or stains.
- Mailed bombs generally do not buzz or tick.
- The contents feel stuck (pressure or resistance) when attempting to remove contents from the envelope or parcel.

What should I do if I've RECEIVED a suspicious parcel/letter in the mail?

1. Remain calm.
2. Gloves should be worn.
3. **Do not** open the parcel/letter. Seal the mail in a plastic bag.
4. Put down the damaged or suspicious package(s), evacuate the room and surrounding area and immediately cordoned off the area.
5. Call the SSC.
6. Ensure that all persons who have touched the mail piece wash their hands with soap and water.

What should I do if I've OPENED a suspicious parcel/letter?

1. As soon as practical, shower with soap and water.
2. Do not further handle the mail piece or package suspected of contamination.
3. Put down the damaged or suspicious package(s), evacuate the room and surrounding area and immediately cordoned off the area.
4. Contact the SSC
5. Evacuate the immediate area beyond the perimeter of those exposed.
6. Make a list of all persons who have touched the letter and/or envelope. Include contact information. Provide the list to the proper officials.
7. Place all items worn when in contact with the suspected mail piece in plastic bags and keep them wherever you change your clothes and have them available for law enforcement agents.

Reporting a suspicious letter or parcel:

1. SSC will contact police and Security at 802-828-0777. Explain that you've received a parcel in the mail that may contain a bomb, biological or chemical substance. Police and/or Security will assume control and will contact the appropriate officials.
2. Notify your SSC who will convey the information to your division's Department Designee.
3. The proper officials will collect the mail, assess the threat situation and coordinate with the FBI, if necessary.
4. If necessary, Security will notify local, county and state health departments and the Vermont Homeland Security Office.

Medical Emergency

Reporting a medical emergency:

1. Notify Building Security/Building Safety and Security Coordinators (SSC) at _____ and provide the following information:
Location of injured or ill person (address, floor number).
 - Any details available about the accident or illness.
 - Name of injured/ill person.
2. If Building Security is unavailable, call 911 and provide the following information:
(Remember: you must first dial "9" from a state phone)
 - Location of injured or ill person (address, floor number).
 - Any details available about the accident or illness.
 - Name of injured/ill person.

Take the following action In the event of a medical emergency:

1. Do not move the injured or ill employee.
2. Try to make the person more comfortable. Cover with coat or blanket.
3. WITHIN 24 HOURS: Contact the Office of State Security Programs at 802-828-0777 to report the incident. For injury or accident, complete and submit an Accident/Illness Report located on the BGS Security Web page <http://www.bgs.state.vt.us/security/index.html>

Panic Alarm/Button Protocol

Name of Office or Department(s):

Number of Panic Buttons:

Wireless:

Hard Wired:

Location of Panic Buttons:

Procedure for using/checking out wireless panic buttons: (list what you want your staff to do)

- Notify supervisor of concern
- Notify clerical staff of your location and that you have a panic button
- Sign the panic button out on the personnel “out” board
- Or whatever criteria you wish to use to ensure that someone is aware of the concern and the usage

If the panic button is pushed.....here is the typical sequence of events:

1. The Central Station (aka monitoring company) calls the State Office Building to ensure that the button hasn't been pressed accidentally.
 - a. If nobody answers the phone (or if the person answers but fails to provide proper identification and password), then notify the local Police Department.
2. The Central Station continues to call everybody on the particular call list to notify them of the event.
3. The Police arrive and handle the situation as necessary.
4. A Supervisor in the building should notify Security at 828-6974 and inform of the incident.
5. A Supervisor in the building completes an incident report form online at www.bgs.state.vt.us/security informing Security of the incident details, etc.

Accidental Panic Button Activation? Call the Central Station and/or local Police Department and notify. (names and numbers here w/ account #)

Should the system be activated during an incident, the alarm system (location here) must be disarmed and then re-armed for future use. To do this, follow these instructions:

(instructions here)

The manager or director in charge of each department located in the building is expected to assume responsibility for decision-making in case of an emergency. In his or her absence, whoever is left in charge will assume the responsibility of the department designee. The safety of all employees and other persons in the building is the highest priority.

Power Failures

In Vermont we experience power outages occasionally. In the event of a power failure, employees are asked to inform their Safety Warden.

When Power Fails

- Shut down equipment which automatically restarts when power is available.
 - Disconnect equipment that runs unattended, and turn off unnecessary lights and equipment.
- This will reduce the risk of power surges and other unforeseen damage or injury that could result when the power comes on unexpectedly.

When the Power Returns

- Reset/restart/check equipment.
- Assess and report any equipment failures to your supervisor.

Emergency Lighting

- Emergency lighting should provide enough light for a safe exit.

Suspicious Fumes

Heating/cooling/ventilation systems are powered by natural gas, propane fuel, fuel oil, wood and electricity. Maintenance personnel perform routine maintenance checks to ensure equipment is operational and working properly. Although infrequent, the malfunctioning of a building's heating, cooling and ventilation systems may occur. Construction projects in or around a building may also result in the creation of unknown and suspicious fumes including sewer gas, equipment exhaust and vehicle exhaust. Although many odors are harmless, be aware that natural gas and other suspicious odors could be combustible and/or toxic. Employees are encouraged to take immediate action and suspicious odors to building maintenance and/or **security**.

If you smell a suspicious odor, take the following action:

1. Inform your supervisor and leave the immediate area.
2. From another location, notify building maintenance and/or security at 828-0777.
3. Do not touch an electrical switch or use your phone.
4. Do not try to locate the source yourself.
5. Do not open windows in an attempt to ventilate.
6. Confirmed natural gas leaks or other dangerous fumes will result in an evacuation. The SSC in consultation with maintenance will make the call to evacuate if deemed appropriate .

Evacuation Procedures:

1. Remain calm.
2. Cover your nose and mouth with a cloth, coffee filter, paper towels, etc.
3. Take shallow breaths.
4. Evacuate the area.
5. If an evacuation is called, follow the directions of your Safety Warden.

Stay a Safe Distance from Building:

Remain a safe distance from the building until the SSC has determined the building is safe to re-enter.

Suspicious Person/ Hostile Intruder –Hostage/Weapons Situation (Response to)

The day-to-day operations of The State require the interaction with internal and external customers. Employees are encouraged to be aware of their work surroundings, co-workers, guests, and unexpected persons in their work areas and to respond appropriately.

If you encounter a suspicious person in your work area, take the following action:

1. If the person appears approachable, ask, “*Can I help you? Are you here to meet with someone?*” If the response seems odd or vague, do not argue or continue the discussion, provide a polite response and move on. Immediately notify **Security at 802-828-0777**
2. If the person appears unapproachable, do not attempt to make contact. Immediately notify **Security at 802-828-0777**
3. If a suspicious person approaches you or a co-worker, be polite and listen to the person’s concerns. A nearby co-worker should immediately contact **Security at 802-828-0777**
4. Provide a description of the suspicious person, making note of the following:
 - Race (Caucasian, Black, Hispanic, Asian, Indian, Middle Eastern)
 - Gender (Male, Female)
 - Hair features (blonde/black -- long/short -- wavy/straight)
 - Facial features (glasses, mustache, beard)
 - Clothing (shirt color, pants color)
 - Location where person was last seen.
5. If safe to do so, observe, at a distance, the movement of the suspicious person. Do not attempt to make further contact. Security will locate the person, determine the person’s purpose in the building, and if appropriate, remove him/her from the building.

Suspicious Activity:

If you witness an activity at your building or in your work area that seems abnormal and not easily explained, share your observation with your supervisor and notify **Security at 802-828-0777**

A Hostile Intruder(s) is:

A hostile intruder is a person (s) who participates in a random or systematic action demonstrating their intent to harm others. The person(s) may use firearms, explosives, knives, etc. to effect mass murder rather than engage in other criminal contact.

Hostile Intruder situations may constitute a life threatening situation. Above all, protect yourself, and remain calm. Other employees may look to you as a role model and leader. In the event that an intruder enters a State building, the following guidelines should be followed, unless doing so would present an unreasonable or elevated risk of harm to yourself or others:

1. If you discover a hostile intruder, you should immediately dial 9- 911 and provide as much information as possible. If possible, also contact Security *at 802-828-0777*
2. You should NOT activate the fire alarms, as doing so is likely to cause people to move from safety.
3. Attempt to move from open areas to a place of cover, concealment and security.
4. If outdoors, you should move inside or take cover, by crouching or lying down behind substantial objects.
5. If inside, move to the closest room, close and lock the door.
6. Turn off lights.
7. Close windows and shades/curtains.
8. Stay away from and out of sight of any doors or windows.
9. Stay calm and quiet.
10. Remain in shelter until contacted by senior staff member(s), or instructed by Security, or law enforcement personnel.

Interaction with Law enforcement:

1. Police entry into the building may or may not be announced.
2. Police will be responding and reacting based on their training and the situation.
3. Follow all police instructions promptly and help any co-workers who need assistance.
4. Information that you provide to law enforcement could be very important to the safety of your co-workers. Expect and cooperate with police interviews.

What if I encounter the Intruder?

1. Remain as calm and quiet as possible.
2. Observe reasonable requests by the intruder but do not volunteer anything.

If you find yourself in a hostage situation:

1. Try to stay calm.
2. Follow instructions of the hostage taker(s).
3. Speak only when spoken to.
4. Don't make suggestions.
5. Try to rest.
6. Be observant.
7. Be prepared to speak on the phone, you may be forced to do so.
8. Don't be argumentative and treat the hostage taker as normal as possible.
9. Be patient.
10. If police assault, drop to the floor and take cover under anything available.

If you attempt to risk an escape, ask yourself:

1. Can I do so quickly, quietly and above all safely?
2. Have I sufficiently studied the hostage taker's pattern of behavior to give me a good chance of escape?
3. Will my absence be noticed?
4. Will my escape endanger the remaining hostages?

A very small percentage of hostages are killed or wounded by the hostage taker.

Tornado Warning

Although Tornadoes are rare in Vermont in the event of a tornado warning issued by the National Weather Service, notification will be made advising building occupants of tornado procedures.

Tornado Watch:

The term “tornado watch” simply means that conditions are right for a tornado to develop. It does not mean that a tornado has been sighted. During a tornado watch, employees will continue to work. Listen for information from building management or building security.

Tornado Warning:

A “tornado warning” indicates that a tornado has been sighted. Employees should be prepared to initiate tornado response plans should action be necessary. If a warning is in effect, the local sirens will sound for three minutes followed by seven minutes of silence. The siren pattern will continue in this manner until the warning has been discontinued. Listen for instructions from either building management or building security.

In the event of a tornado warning, take the following action:

1. Close all drapes to the outside windows and close your door behind you.
2. Follow the directions of your Safety Warden.
3. Move away from the perimeter of the building and exterior.
4. Go to the core of the building: to stairwells, restrooms or interior offices.
5. If you are caught in an exterior office, seek protection under a desk.
6. **Do not** go to the first floor lobby or outside of the building. You are much safer in a steel-framed or reinforced concrete building than you will be on the street or in your automobile.
7. **Do not** get on an elevator. You can be as safe on your own floor as anywhere else, stay in the interior portions of the floor.
8. Remain calm.

If evacuating after the impact of a tornado:

1. Assess emergency evacuation routes – determine if clear, blocked or impassable.
2. If passable, open doors carefully; watch for falling objects.
3. See Procedure 9: Evacuation Procedures - After the Impact.

If trapped inside after a tornado:

1. Replace all telephone receivers.
2. Identify working forms of communication – cell phones, office phones, etc.
3. Evaluate situation and coordinate actions with co-workers and other building tenants.
4. Do not move debris or objects – it may trigger the collapse of a nearby structure.
5. Assess area for gas or liquid leaks or other hazards.
6. If power outage, do not use candles or lighters until determined safe to do so.
7. Check for fires and extinguish fires if at all possible.
8. Clean up or contain spills, excess fluids and materials immediately, if safe to do so.
9. Power down computers and lamps. Do not turn on light switches or appliances.
10. Identify available communication: work phones, cell phones, radios, etc.
11. Do not flush toilets until authorized by building management.
12. If trapped, listen for emergency evacuation teams -- above you, below you and around you. Remain calm and encourage others to do the same. Help is on the way.

Weather Emergency (Declared)

A. Declaring a Weather Emergency

The Secretary of Administration (or designee) has the authority to decide on the appropriate response in an emergency situation including those which are weather related. To reduce driving hazards in severe weather conditions, the Secretary of Administration (with advice from the Agency of Transportation, the Department of Public Safety, and the Department of Human Resources) may decide to delay the opening of some or all State offices or facilities or to curtail operations, for some or all employees, early. This decision will be made by the Secretary of Administration (or designee) only, and is not a decision which Department Heads or Division Directors are authorized to make.

B. Communicating the Weather Related Emergency to Employees

If a delayed opening situation is directed or approved by the Secretary of Administration, Public Safety Headquarters Dispatch will be contacted and will immediately notify local radio and television stations and ask them to broadcast a delayed opening message as early as possible prior to the normal commuting time of State employees. Employees should tune in to their local radio or television stations when the weather is predicted to be adverse. Employees may also call the Toll-free Weather Line: 800-644-4402 or access the Department of Human Resources' Reduced Workforce or Emergency Closing website: <http://www.vermontpersonnel.org/hm/closings.php> for pertinent information.

If the decision is made by the Secretary of Administration during a workday to reduce the workforce or curtail operations early for some or all State employees due to adverse weather, (s)he will notify the Commissioner of Human Resources who will be responsible for notifying agency/department heads as soon as possible. The electronic mail system will be utilized to stay in contact with agencies and departments, the Toll-free Weather Line and Department of Human Resources' website will be updated accordingly.

Workplace Violence

The Agency of Administration is committed to providing all employees with work environments that are safe, secure and free of harassment, threats, intimidation and violence. The State maintains a Workplace Violence Prevention Policy that is posted in the work areas of the department. If you are unable to locate a copy of this policy, please contact The Department of Human Resources.

Upon awareness of violence in the workplace, do the following:

1. If the crisis situation involves an injury:
 - Call **Security at 802-828-0777** who will direct emergency personnel and law enforcement officers to the scene.
 - If Security is unavailable, call 911.
 - Notify a supervisor and/or the SSC.
2. For all other crisis situations:
 - Notify a supervisor and/or SSC.
 - Contact **Security at 802-828-0777**

(The SSC, supervisor or Security shall coordinate with law enforcement, fire, medical and other community resources offering assistance as necessary.)
3. If not directly involved in the incident, secure your office, otherwise seek protection by lying on the floor or barricading yourself in another secured area.
4. Always remain aware of your surroundings and move close to a door if possible.
5. Adhere to the requests of the assailant.
6. Make mental notes regarding the description and mannerisms of the assailant.
7. Remove yourself from the area when security or law enforcement arrives.

Evacuation Procedures

It is the responsibility of each employee to know your office's Safety Warden, as well as each alternate Safety Warden. Every employee also should know the evacuation plan.

Office Safety Warden: _____

Alternate Safety Warden: _____

ASSEMBLY AREA:

(safe distance from your building but within walking distance)

If an evacuation is called, take the following action:

1. Follow the instructions of your office Safety Warden and other security personnel.
2. Your Safety Wardens are those employees who wear **orange** safety vests during evacuations, fire drills and other emergency actions.
3. Assist those co-workers requiring assistance (buddy system).
4. If a co-worker cannot continue evacuation due to illness or incapacitation, assume the buddy role and seek the assistance of a Safety warden.
5. Close the door of your office.
6. Use the stairwells for evacuation.
7. Form a single-file evacuation line and Be alert for fire personnel who use stairways to respond to emergencies.
8. Use the handrails and stay to the right in the stairwells.
9. Report to your office's designated Assembly Area.
10. Call 828-0777 to receive up-to-date status of the situation.

Remember:

- **Do not** use electronic devices (cell phones) inside buildings during bomb threat evacuations.
- **Do not** use the passenger elevators unless instructed to do so.
- **Do not** return to your work area for any reason.
- **Do not** run or panic.
- **Do not** remain near the building after exiting the building. Proceed safely to the predetermined Assembly Area.
- **Do not** return to the building until the SSC gives the "all clear."

Evacuation Assistance List:

Employees with physical or medical limitations will receive special assistance during evacuations.

Employees are encouraged to complete the online form and inform your Safety Warden of your condition.

You will be placed on your area/Safety's Evacuation Assistance List and will receive special evacuation

instructions and assistance. (Blank form found at <http://www.bgs.state.vt.us/security/forms/BGS-SEC->

[Vermont-ASAP-Manual.pdf](http://www.bgs.state.vt.us/security/forms/BGS-SEC-Vermont-ASAP-Manual.pdf))

Evacuation Procedures: After the Impact

This procedure is established to heighten employees' awareness of actions that should be taken and actions to avoid in the event of an impact to their facility due to a natural disaster, fire or explosion. Although the risk of impact is low, employees are advised to be familiar with potential post-impact environments and recommended actions and to identify additional actions that would be advisable in the event of impact at their respective facility.

Inside the building, immediately after an Impact:

1. Anticipate low or no visibility due to fine particles of debris – do not panic.
2. Determine if anyone is hurt. Summon medical teams by calling 911
3. Evaluate situation. Rally and coordinate actions with co-workers & other tenants.
4. Assess emergency evacuation routes – determine if clear, blocked or impassable.
5. Do not move debris or objects – it may trigger the collapse of a nearby structure.
6. Open doors carefully; watch for falling objects.
7. Remain calm and encourage others to do the same.

If evacuating after the impact of an explosion or natural disaster:

1. Follow emergency evacuation procedures.
2. Do not use the elevators.
3. Keep calm and encourage others to do the same.
4. Use great caution when exiting a building.
5. Be aware of broken glass and electrical damage dangers such as sparks or broken or frayed wires when exiting the building.
6. Watch for falling debris; take cover under sturdy furniture; tuck and protect your head with your arms.
7. Upon exiting the building, quickly move away from the building, watch for falling debris.
8. Do not return to the building or attempt to re-enter the building.

If trapped inside after an explosion or natural disaster:

1. Listen for emergency evacuation teams – above you, below you and around you.
2. Anticipate low or no visibility due to fine particles of debris – do not panic.
3. Determine if anyone is hurt. Summon medical teams.
4. Keep calm and encourage others to do the same.
5. Replace all telephone receivers.
6. Identify available communication: work phones, cell phones, radios, etc.
7. Use caution when moving about in a damaged building, be careful of broken glass.
8. Evaluate situation and coordinate actions with co-workers and other building tenants.
9. Do not move debris or objects – it may trigger the collapse of a nearby structure.
10. Open doors carefully; watch for falling objects.
11. Check for fires and extinguish fires if at all possible.
12. Assess area for gas or liquid leaks or other hazards in your area, if hazards are located provide location, if safe to do so, to co-workers and others in the area.
13. Power down computers and lamps.
14. Do not turn on light switches or appliances.
15. If power outage, do not use candles or lighters until determined safe to do so.
16. Do not flush toilets until authorized by building management.
17. Remain calm. Help is on the way.

Communication Plan

The Agency of Administration is the unit of Vermont State government that is responsible for providing the overall administrative guidance and direction to all State agencies. The Agency's role in an emergency/disaster situation is to provide coordination, direction, and support to the responding State agencies, as well as to ensure the continuity of State government. The Secretary of Administration, or his designee, will also serve as the liaison to the Governor's office.

During any emergency, the safety of all State employees is of the utmost importance. We all become one assemblage of employees, devoid of any Agency or Department connection, working together for the safety of all.

Evacuation protocol:

When the alarm sounds to evacuate the buildings;

1. All State employees are to report to their designated locations to check in with their Safety Warden.
2. SSC as well as the highest ranking State Official, on site, will report to the Incident Command Center (CC) located at the XXXXX or the XXXXXX location outside the building (if evacuation is required)

Line of succession:

1. SSC
2. First Alternate SSC
3. Second Alternate SSC
4. Senior (by rank) State Employee

State Officials - If unsure who is on location, go to CC to check in.

3. Safety Wardens and their back up; please refer to the Safety Warden Responsibilities Procedure for instructions.

4. Two Way Radio Communication:

- A. Command Post to Directors Channel 7
- B.
- C.
- D.

The above listed two-way radio channels are for individual Division or Agency/Department use during any emergency. Channel 7 is to be used by both the Command Center and Directors or Agency representatives for all direct two-way communication during any emergency.

Incident Command Center Duties (See Annex J)

SSC

1. Represents the State of Vermont's interest in any decision making process with.
2. Makes the initial call to DHR (828-3491) regarding emergency.
3. Direct communication with Directors and other Agency's Heads.

4. State Employee team leader and spokes person..

Emergency Management Liaison

1. Reports State employees concerns or emergencies to the Command Center leadership.
2. Contacts State Emergency Management Team if necessary.
3. Assists in contacting outside sources as they relate to emergency.
4. Miscellaneous Duties as they arise.

Facilities Liaison

1. Administers head count & reports results to Command Center leadership.
2. Assists in the management of State employees and their well being.
3. Assists in facilitating emergency procedures.
4. Miscellaneous duties as they arise.

Computer, Internet & Information Security

Information security violations can happen anywhere to anyone. It is the responsibility of each employee to protect the information resources we use every day. Proactive daily work habits can help you protect the information resources that State have entrusted to you.

COMPUTER GUIDELINES:

- Do not share your Outlook account and network passwords except when working with your IT staff or staff of DII.
- Do not use simple, obvious, or predictable passwords. Passwords not to be used include: names of relatives or pets; nicknames; days and months; repetitive characters, etc.
- Be creative when selecting passwords. Choose passwords that are a minimum of eight characters long from a combination of symbols, numbers, uppercase and lowercase letters.
- Do not write down your passwords, or post them on your terminal, or other obvious places. Don't create macros or other shortcuts to record your passwords.
- Change your passwords if you suspect that any of your passwords are known to someone else. Notify your supervisor.
 - For new employees, always change the initial password assigned to you by IT Services as soon as you receive it.
- Change your passwords frequently, at least once every month, or more often if necessary.
- Do not use someone else's Logon ID and password. If you are having problems with your access, contact your IT support staff.
- Do not use your access privileges to enable other individuals to access information that they are not authorized to access, or to submit transactions that they are not authorized to submit.
- When leaving your workstation area, lock your computer (press CTRL + ALT + DELETE) then click on "lock your computer." If your workstation is located near a public area, lock your computer if you are stepping away from your desk, even momentarily.
- At the end of the workday or when finished using your computer, logoff of your computer (press CTRL + ALT + DELETE) then click on "logoff."
- Label all your diskettes and CDs and store those with sensitive information in a secure environment.
- Consider electronic documents and e-mails that are part of official files for record retention before erasing old files and documents.
- All files should be stored on network drives for backup purposes.
- For state employees with Web-based access to the state's computer systems, seek guidance and clearance from the DII before accessing information using wireless, satellite and other evolving technologies.
 - Work with IT Services to arrange for installation of software. Only Organizational IT Specialists are authorized to load software onto an employee's computer.
 - Assistance for the above issue is available through the Organizational IT Service
 - Request System at <http://www.bgs.state.vt.us/infotech/index.html>

INTERNET AND ELECTRONIC INFORMATION GUIDELINES:

- Do not open (i.e., view, detach or launch) suspicious e-mail attachments.
- If you receive a suspicious e-mail attachment, contact your BGS IT Support staff immediately.
- Do not send a copy -- verbally provide your name, the sender's name, date, and name of attachment.

- If you receive an unexpected or suspicious e-mail from someone you know, contact the person who sent you the attachment to verify that they actually sent it and immediately contact Desktop Support.
- Do not configure your e-mail to automatically open attachments. If your e-mail program automatically opens attachments, disengage it or contact your IT Services technician for assistance.
- Ensure confidential or sensitive information on your servers is protected with an effective authentication mechanism, encryption software or firewalls. Ensure your IT Services representative knows the existence and location of confidential and sensitive information.
- Do not use the Internet, electronic mail and online services to transmit or download material that is offensive, obscene, pornographic, threatening or racially or sexually harassing.
- Do not use the Internet, electronic mail and online services to disseminate or print copyrighted materials (including articles and software) in violation of copyright laws.
- Take all reasonable precautions to prevent the inadvertent dissemination of anyone else's information via the Internet, electronic mail or online services.
- Be reminded that access to and use of the Internet, including communication by e-mail, is not confidential. Internet access can and will be monitored. Web browsers leave traceable "footprints" to all sites visited.
- Also, see Cyber-attacks located in this suite of safety and security procedures.

PAPER DOCUMENTS AND FILE GUIDELINES:

- Do not leave sensitive or confidential information lying around. File or dispose of sensitive or confidential information properly and timely.
- Store valuable information in a secure location such as a locked desk, filing cabinet, or office.
- Label your files and diskettes so you can easily identify any information and store in a secure location.

CYBER-ATTACKS

Before a technology-based incident occurs, familiarize yourself with this section and refer to the Disaster Recovery plans for additional instructions.

DII's technological applications operate on a secured technology environment to address and reduce the likelihood of cyber-attacks. Should you receive a suspicious e-mail or become aware of a real or perceived cyber-attack, please do the following:

Reporting a cyber-attack:

1. Do not open or further tamper with the e-mail or your computer.
2. Report the incident to your DII Services technician or DII Services at 828-3544.
3. Report the incident to your IT Specialist.

What is a cyber-attack:

Specific types of potentially damaging "cyber-activities" have different sources and different targets, and carry different levels of risk for enterprises. Examples of a cyber-attack include the following:

- Incidents involving computer "hackers."
- Incidents involving system penetration or tampering.
- Unauthorized access to computing facilities, telecommunication (i.e., telephone, fax, teleconferencing) and networking services (i.e., e-mail) or equipment.
- Use of computing, network and telecommunication facilities for personal profit.
- Destruction or alteration of data, software and equipment.

Hackers: Computer hackers are generally online troublemakers who engage in illegal online activities to further their cause or belief. Targeted systems will likely be compromised and used as staging points for cracking, distributed denials of service or other types of attacks.

Cyber-crime: Cyber-crime is online criminal activity undertaken for financial gain. Cyber-crime activity is expected to rise as criminals attempt to take advantage of perceived uncertainties in financial systems. Fraudulent online solicitations for nonexistent charities also appear following tragedies.

Cyber-terrorism: Cyber-terrorism is a computer-based crime intended to cause loss of life or property in pursuit of political gains. Cyber-terrorist activities will likely target U.S. government facilities as well as infrastructure centers and nongovernmental organizations such as relief agencies. Enterprises, particularly financial institutions, public utilities, telecommunications companies, online trading firms and e-commerce sites, are also likely to be targeted.

Parking Regulations in State owned parking lots

The parking of any vehicle, private or state-owned, in any parking lot shall be within lanes whenever same are established by painted stripes or otherwise and shall conform to any and all other directions posted on the site.

- Parking in all areas shall be in such a manner as to provide ample room for ingress to and egress from the area to all other vehicular traffic.
- Parking at loading docks and platforms shall be restricted to commercial and other service vehicles while in the process of loading or unloading state commodities.
- All persons utilizing state parking lots during times of winter weather shall give due consideration to such hazards as falling ice and snow and slippery ground conditions. Temporary directions, as may be occasioned by snow obstruction, snow removal or other winter conditions, and by maintenance and repair work, shall be complied with.
- Parking in state parking lots shall be limited to state-owned vehicles and to vehicles operated by state employees or by persons actively engaged in state activities. Overnight and weekend parking shall be limited to state-owned vehicles.
- In state-owned parking lots and structures under his jurisdiction, the Commissioner of Buildings and General Services may from time to time designate and assign specific areas to certain buildings, positions, or to certain departments or agencies, as the need may indicate.
- Use of state parking lots shall at all times be entirely at the risk of the owner or operator. The State of Vermont does not at any time or under any condition assume any responsibility for damage to or theft of any privately-owned vehicle in any state parking lot or for personal injury, from any cause whatsoever, to any person or persons utilizing a state parking lot.

Capitol Complex

State employee parking within the Capitol Complex will be controlled through the issuing and use of parking permits and enforcement of parking restrictions. Parking permits will be issued to any state employee who requests a permit.

Vehicles in any lot that are determined to be in violation of the regulations may be subject to towing at the owner's expense.

Vehicles in van pools, or registered car pools, such as Vermont Ride Share, will need to display a BGS-issued parking permit in addition to a registered Ride Share permit.

Park and ride vehicles (individuals not working within the Capital Complex) are encouraged to park in the parking area behind the Department of Labor building at 5 Green Mountain Drive because of the limited parking available in the Capital Complex area. Parking permits are not required to park in this lot.

Parking permits must be displayed and easily viewed on the rear view mirror or dashboard of vehicle.

It is the employee's responsibility to obtain and renew parking permits and to be aware of signage that regulates parking in particular areas. The Department of Buildings and General Services will issue a reminder to update parking permit.

An employee will only be issued one permit (not multiple permits for multiple vehicles). The employee is responsible for ensuring the permit is displayed properly in any vehicle they park in a state-controlled lot. The

employee is also responsible for renewing their permit in December of each year.

Permits are good for the calendar year in which they are issued and all permits expire on December 31 of each year. You may obtain a new permit for the next year starting on December 1 of each year.

Parking permits can be obtained on line at <http://www.bgs.state.vt.us/security/index.html> -- or by contacting the Security Office at 828-0777.

Legislative Session:

Day Use Permits

A day use permit is available at the Security Office, 6 Baldwin Street or the Security Kiosk at 109 Sate Street, for those who have business in the Montpelier Capitol Complex.

Temporary Permits

Temporary permits can be issued for Agency Secretaries, Commissioners and/or State Employees from out of town. Temporary permits are issued for a specific period of time that is less than one year.

Reserved Parking

Some spaces will continue to be reserved at the direction of the Commissioner of Buildings & General Services. Those vehicles must also display a BGS parking permit.

State Vehicles

State vehicles that display a State of Vermont license plate are not required to display a BGS permit.

Overnight Parking

Any vehicle parking overnight for an extended period of time must: (1) park in the DET Signage Signs indicating that parking is by permit only and that violators are subject to towing - will be placed and maintained at the entrance to parking areas in the Capitol Complex.

Please note: With few exceptions - reserved parking spaces and Legislator parking - a BGS permit does not guarantee a parking space within a specific area, but only the right to park in a controlled lot on a space-available basis. Overflow parking is available in the DET parking lot.

VIOLATIONS AND PENALTIES

Any vehicle improperly parked or in any other manner in violation of any part of these rules and regulations may be deemed by the Commissioner of Buildings and General Services or his/her authorized agents to be in violation of these regulations and subject to removal forthwith. The state shall not be responsible for any costs of other expense occasioned by such removal.

DEFINITIONS

- "State Parking Lot" shall mean any paved or unpaved parcel of land, so designated, lot or structure owned or rented by the State of Vermont and under the control and/or jurisdiction of the Commissioner of Buildings and General Services, or that part of a leased building and its adjacent spaces as may be under the control and jurisdiction of the Commissioner of Buildings and General Services by executive or other order of the administration.
- "Operator" shall mean and include every individual who shall operate any vehicle on a state parking lot either as the owner or as the agent, employee, or permittee of the owner or otherwise, and shall include those department heads where so-called "pool cars" are available for use by departmental members.

All vehicles in State parking lots and/or areas are expected to be parked in accordance with State Parking Rules. Vehicles may be towed which are not parked in accordance with those rules. The Office of Security Programs is responsible for ensuring that all vehicles are parked in conformance the state's parking regulations.

For those vehicles which are in violation of the policy, Security shall:

- ▶ Identify the vehicle,
- ▶ Make honest effort to locate the owner, and
- ▶ Request that the vehicle be moved

If the vehicle owner cannot be located or the vehicle is not moved after request

- ▶ Contact the Commissioner's Office for final approval prior to having the vehicle towed.
- ▶ If approved, arrange for the vehicle to be towed at the owner's expense
- ▶ Notify local police that vehicle has been towed, identifying the vehicle, owner's name, and where it has been towed.
- ▶ Maintain a log of illegally parked and/or towed vehicles; incidents of repeated violations will be considered when dealing with subsequent offenses.

In certain situations, the vehicle could be towed without notice to the owner, following approval from the Commissioner's Office. The following parking violations are examples of when this might occur:

Blocking a fire lane
Parked illegally in a handicapped space
Parked in a designated ambulance location.

State Employee Identification Card.

State Identification Cards for Full-time Employees, Part-time employees, members of boards, commissions and contractors shall be worn at all times while inside a state office building.

All State Identification Cards must be obtained through the Department of Buildings and General Services, Division of State Security. (Exception: Department of Public Safety)

Application for State Identification Cards

The Applicant must complete a State Identification Card Request Form. Forms are available on-line at http://www.bgs.state.vt.us/security/forms/badge_access_form.pdf. Once the form has been completed by the applicant email the form to the applicant's Appointing Authority. Once approved and electronically signed by the Appointing Authority the completed form shall be submitted electronically to the Division of State Security by clicking on the "Submit by Email" button at the top of web page (prior to your appointment). Following your submission please contact the Security office at 828-0777 to schedule your appointment.

The Identification Card will:

Include a photograph of the Cardholder, the Cardholder's department or other affiliation with the State, the signature of the Cardholder, and a identification symbol designated by the Commissioner (e.g. V for visitor, C for a 30-day contractor) and may include at the discretion of the Commissioner, the Cardholder's department or other affiliation with the State, a photograph of the Cardholder and the signature of the Cardholder, and on the back of the card employee or other identification number, and the authorizing signature of the Commissioner.

State Identification Cards for volunteers, contractors and visitors shall bear, at a minimum: The signature of the Commissioner and, at the discretion of the Commissioner, the cardholder's name and an identification number.

Access Authorization

The State of Vermont has implemented a card access system allowing access to state facilities. The State Identification Card will serve the dual function of allowing access to designated areas of state facilities through a card reader system.

Access is decided by your Director, Facilitator, or Department Supervisor and authorized by the appointed authority or authorized designee. Additional access can be granted after the card has been issued when your supervisor submits another badge request form requesting the additional access. The cardholder does not have to come get a new picture as the authorizations are added electronically.

The Appointing Authority is Agency Secretary, Department Commissioner, Board Chairperson, Council Chairperson and/or his/her designee. Designee must be appointed in writing and provided to the BGS Office of State Security Programs.

Processing of Photographs and Signatures

The applicant shall make arrangements with the Office of State Security Programs for photographing for the State Identification Card that has been requested and approved by the Commissioner. The applicant may be required to travel to certain sites to be photographed for State Identification Cards.

Delivery and Recordkeeping

Once a State Identification Card has been produced by the Division of State Security, the Card will be delivered to the Applicant. A copy of the processed and signed State Identification Card Request Form remains on file at the Office of State Security Programs and one copy is returned to the Appointing Authority to be filed in applicants personnel file.

Costs

Cost for the initial issuance of a State Identification Card will be waived.

Should a Cardholder lose, or fail to return his or her card in circumstances described below, the replacement or deactivation cost shall be \$10.00 payable by the Cardholder.

Return or Deactivation of Cards

The Commissioner reserves the right to deactivate any or all State Identification Cards at any time in the interest of workplace security or public safety.

Visitors shall return identification cards prior to leaving a state facility.

The Appointing Authority and/or designee shall immediately notify the Division of State Security when one of the following circumstances occurs:

FOR	APPOINTING AUTHORITY AND/OR DESIGNEE
Any Cardholder	Any threatened act or act of violence that reasonably poses an imminent risk to the safety of state employees or the public,
State Employees	Separation of employment
Board/Commissioner Members	Completion, resignation, withdrawal or termination of services,
Contractors	Completion, termination, or expiration of the contract
Volunteers	Completion or termination of volunteer services

Cards shall be immediately returned to the Office of State Security Programs by the Cardholder's department/organization under any of the above circumstances. Cards that do not automatically expire shall be deactivated by the Office of State Security Programs upon any of these circumstances, whether or not a Cardholder returns his or her card.

Visitors must register upon arrival

All visitors who have business in a state office or on a floor must register with the receptionist upon his/her arrival. Visitors will also be required to list the departure time on the sign-out sheet when they have concluded their business with the office. A sign-in sheet should be utilized to solicit the following information: Date, Arrival Time, Departure Time, Visitor's Name, Visitor's Company or State Agency, and Name of Office or Employee to be visited. Offices with more than one entrance point should cordon off or direct visitors to one central location to sign in and receive a visitor badge. Couriers and visitors whose business is to deliver or retrieve packages in the reception area are not required to sign in. Sign-in sheets should be retained for at least 30 days before disposal.

Visitors must wear state credentials or be issued a visitor badge

All visitors, with the exception of state agency employees wearing an agency or state building photo I.D. badge, should be issued a temporary visitor badge after registering. Visitor badges and state I.D. badges

must be visible and worn at all times. State agency employees who display an agency or building photo I.D. badge must sign in with the receptionist but are not required to receive a visitor badge. Visitors will be required to return the temporary visitor badges and list the departure time on the sign-out sheet when they have concluded their business with the office. Peel-n-stick visitor badges should be retrieved and destroyed.

State Offices must display sign re: wearing of Identification badges

A sign should be displayed in a visible location for incoming visitors. The sign should read: “Welcome to XXXX. All visitors must sign-in with the receptionist and receive a visitor badge. All employees must visibly display your I.D. badges at all times.”

Transportation Personal and Public

State employees must engage in a daily commute to our workplaces. Some employees are also required to travel to serve our customers and accomplish job responsibilities. Whether on your daily commute or on active travel status, please be mindful of the following safety guidelines:

Personal Transportation – personal or state-owned vehicle

- Always know where you are, know your surroundings.
- Always be aware of what is going on around you.
- If you are attacked, do something to draw attention to yourself.
- After normal working hours, **Security** may be able to escort you a partial way or to your vehicle.
- When you get into your vehicle, lock your doors; the security officer will not leave you until you drive away safely.
- Never drive around with your doors unlocked and keep windows rolled up.
- If you stop, and someone walks up to your vehicle and it makes you feel uncomfortable draw attention to your vehicle and yourself. Lay on the horn.
- Leave the area and call the police immediately.
- Always remember to get a good description of the suspect and remember where and at what time the incident occurred.

Upon witnessing a attack, carjacking and/or kidnapping:

1. Do not draw attention to yourself.
2. Call 911.
3. Do not attempt to intervene.
4. Get descriptions of the Suspect(s), Victim(s), Weapons(s), Vehicle(s).
5. Remember direction of travel.
6. Give detailed information to security over the phone or in person.
7. Wait in the vicinity for police assistance to arrive.

Public Transportation

- Plan your trip.
- "Call backs" are a good idea. Advise a family member, friend or co-worker of your travel route and time. Call them when you arrive safely.
- Have your exact fare ready before you leave your home, office or a store.
- Use a busy and well-lighted bus stop to get on and off a bus. If you must wait, stay near the attendant's stand or in a well-lighted area.
- Find a seat on the aisle if possible. Sit near the driver or operator, but avoid sitting right next to the door.
- Don't doze off on a bus or become too engrossed in a book.
- Keep your purse, shopping bag, backpack, packages or other belongings in your lap, on your arm, or between your feet. Do not leave them on an empty seat.
- Avoid displaying expensive looking watches, rings, necklaces or other jewelry.
- Be wary of noisy passengers arguing or causing a commotion. This could be staged to distract you while others are trying to steal your valuables.
- Observe the behavior of those around you. If you feel uneasy or threatened, change your seat or alert the driver.
- Minimize the chances of losing your property by avoiding crowded buses.

Vehicle Trouble

In the event of an accident in a state-owned vehicle:

1. Obtain medical assistance for any injured persons.
2. Contact the Vermont State Police at 911. If you are unable to reach the Vermont State Police, contact the local authorities.
3. Complete a police report. In addition, complete:
 - The Automobile Accident or Loss Notice which are located in the vehicle glove box or available online at <http://www.bgs.state.vt.us/fleet/forms.html> and
 - The Department of Motor Vehicle (DMV) Report of Motor Vehicle Crash form which is available on line at <http://www.dmv.state.vt.us/FORMS/ACCIDENTForms.htm>.
4. Obtain information from all involved parties (name, address, vehicle description, insurance, etc.) Do not forget to include the names and addresses of any witnesses.
5. Report the accident to BGS Fleet Management Services (FMS) and Department:

For Motor Pool vehicles and leased vehicles administered by the BGS FMS, call 802-241-4500.

In the event of a breakdown in a state-owned vehicle:

For assistance during the hours of 6:30 a.m. to 5:00 p.m., please contact FMS:

For motor pool vehicles and leased vehicles and administered by the BGS FMS call 802-241-4500.

For vehicles not administered by BGS-FMS, contact the department owning the vehicle, e.g., Fish & Wildlife, etc.

After regular hours, please contact the National Automobile Club's (NAC) Fleet Rescue service at 1-800-894-6060. NAC Fleet Rescue will provide you with towing, jump starts, tire changes, lockouts, fuel and water delivery, and mechanical first aid. This service is not coordinated out of the FMS office, but is part of the Wright Express Fuel Card service. Be prepared to provide the following information to the Wright Express representative:

Vehicle's exact location: street address, cross street/off ramp

License Plate #

Organization's Vehicle ID

Vehicle description: year, make, model, color

State of Vermont's NAC Account #: 8503858-000

Drivers must arrange for their own transportation. If a car is totally disabled, the vehicle will be towed. However, a replacement vehicle is not part of the NAC service.

The employee/driver will need to make separate transportation arrangements. The employee/driver can rent a vehicle through Enterprise, take a taxi home, or (during normal FMS business hours) rent a FMS Motor Pool vehicle if one is available and convenient to the driver's location.

Phone Numbers:

Vermont State Police	911
Fleet Management Services	1-802-241-4500
After hours-----	
NAS Fleet Rescue Service	1-800-894-6060

Use of Video-Monitoring Equipment in, upon or around State Facilities

It is sometimes, necessary, appropriate, and vital to have video-monitoring equipment installed at State Facilities as a means of providing additional security. Video monitoring can be an effective technique when used as part of a total security plan to protect public safety and detect or deter criminal activity.

The Department of Buildings and General Services firmly believes that when used correctly and appropriately, this equipment provides enhanced security for State personnel, those receiving services or conducting business with the State, and the citizens of the State.

The Commissioner of Buildings and General Services shall approve all video monitoring at any State Facility prior to its installation and operation in accordance with the following guidelines:

- Except with specific written permission, only the Department shall own and/or operate video monitoring systems within, upon or around a State Facility. State agencies requesting video monitoring shall work in consultation with the Department of Buildings and General Services on the design, installation and operation planning for all video monitoring. The name, title, and work location of agency personnel necessary to operate the equipment or observe the images shall be submitted to the Commissioner for approval. Each agency shall designate a specific contact person for each surveillance system for the Commissioner's approval. The Commissioner may authorize an agency contact person to grant permission regarding release of stored images as per paragraph 5 of these guidelines. The Department of Corrections and the Department of Public Safety are exempted from the approval requirements of this paragraph but shall comply, to the extent appropriate with respect to legal duties concerning security and public safety, with the guidelines below.
- Each State agency using video-monitoring equipment shall, at minimum, post conspicuous signage at the perimeter of each facility where the monitoring equipment is in use. Signage must be readily observable by the average person, use lettering no smaller than one-half inch in height, clearly identify the agency contact person, and comply with applicable regulatory requirements of Americans with Disabilities Act and Vermont Accessibility laws.
- All reception equipment shall be maintained in a Secure Room that is locked at all times and only authorized personnel shall have access.
- Video monitoring shall generally be limited to common and open spaces trafficked by government employees and those conducting government business. Video monitoring of other areas necessary to ensure State security shall be identified during the design planning stage for approval of the Commissioner. Bathroom interiors shall not be subject to video monitoring.
- Image storage and review: Images taken in, upon or around rest areas and welcome centers may not be stored for more than 168 hours. Images taken in, upon or around all other State Facilities may not be stored for more than 96 hours.
- Stored images are not to be reviewed by, released, reproduced, shown, given or otherwise disclosed to anyone other than authorized agency personnel without the explicit written permission of the Commissioner or an agency contact person authorized to grant such permission by the Commissioner. It is the intent of the State to cooperate with criminal investigations and to honor a valid court order to produce stored images.

AUDITING

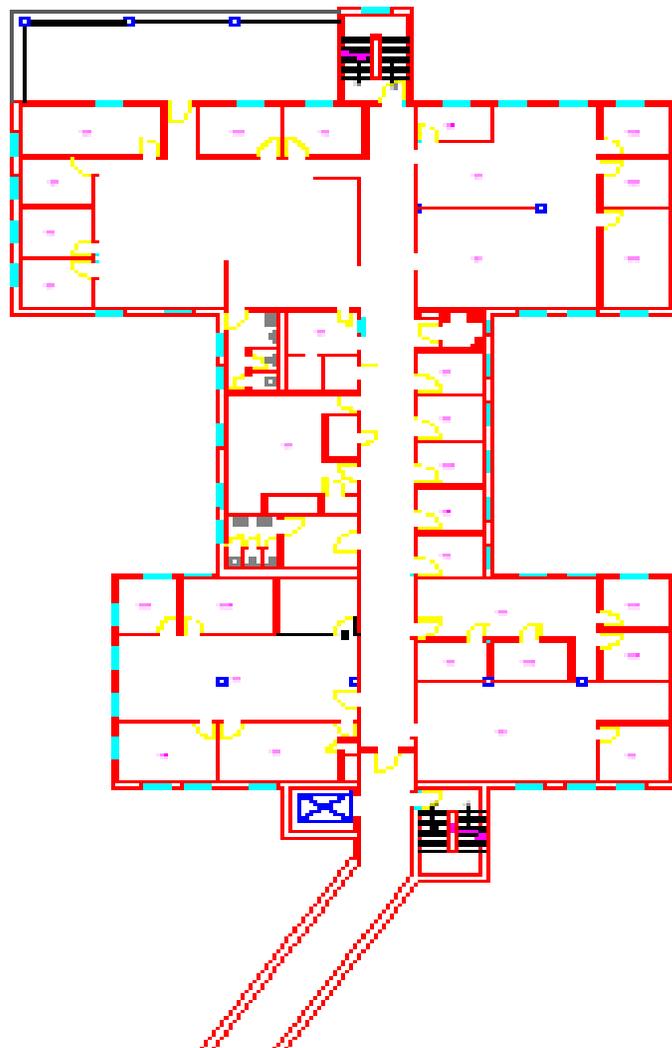
The Department shall maintain a current list of those State Facilities where video-monitoring systems are in use.

State agencies given permission to operate video monitoring equipment, either individually or jointly, shall notify the Commissioner annually, by September 15th of all equipment in use, its location and the contact person for each monitoring system.

EVACUATION FLOOR PLAN

(For Emergency Evacuation and Emergency Equipment)

This floor plan(s) identifies the location of fire escape doors, fire extinguishers and medical equipment. Please be familiar with the location of these items in the event of an emergency.



Osgood 2nd Floor

Familiarize yourself with evacuation plans located on all floors of your building.

Emergency Assembly/Alternate Assembly Locations (For Emergency Evacuation and Emergency Equipment)

This diagram(s) identifies the location of emergency assembly and alternate assembly locations. Please be familiar with the location of these items in the event of an emergency.



Safety and Security Coordinators (SSC) Responsibilities

I. OVERVIEW

The Safety and Security Coordinator (SSC) is appointed by the Secretary or Commissioner and will represent the Agency or agencies within a geographical area or building. The SSC will have decision making authority, in consultation with senior staff members, Secretary and/or Commissioner of Agency or Department and the Office of State Security Programs, concerning emergency procedures as identified in the ASAP.

As Safety and Security Coordinators (SSC) of this department, we are tasked with overseeing our day-to-day business operations while keeping a steady focus on the future needs and expectations of our customers, stakeholders and citizens. We are equally responsible for providing our employees the opportunity to confidently perform their day-to-day responsibilities.

A new charge that each Safety and Security Coordinators (SSC) must undertake and champion is the re-education of employees regarding safety and security in our workplaces. We can no longer afford to take a passive approach to safety, security, or disaster recovery. We must proactively accept responsibility and ensure our employees and services are successfully prepared to respond in the event of an emergency.

II. SAFETY AND SECURITY COORDINATORS (SSC) RESPONSIBILITIES

Safety and Security Coordinators (SSC) are expected to introduce and maintain a heightened level of safety and security awareness in your work Agency(s). The manner in which the responsibilities can best be achieved is left to the discretion of the director of the respective divisions. At all times, Safety and Security Coordinators (SSC) are charged with the following responsibilities:

A. Spring and Fall Reviews of ASAP Plans with Employees

Spring and Fall ASAP Safety and Security Coordinators (SSC) Checklists are attached to these guidelines. These checklists provide directions on the tasks for which Safety and Security Coordinators (SSC) are responsible as well as the topics to be reviewed with their staff. These checklists will be maintained in paper form. Completed checklists should be forwarded to the respective division's department designee.

- During a pre-designated week in March and October, all Safety and Security Coordinators (SSC) will discuss safety and security procedures with their respective employees. This may be a topic of a staff meeting or Safety and Security Coordinators (SSC) may prefer to call a special meeting.
- Engage Safety Wardens in your spring and fall awareness week plan to familiarize employees with the floor plan, designated evacuation route, emergency report-in site, location of fire extinguishers, fire hoses, and location and operation of fire alarm pull stations.
- Assure all employees receive adequate training in safety and security procedures.
- In the spring and fall, ensure that each employee in your office receives or possesses current paper copies of updated safety and security information.
- In the fall, ensure employees are provided a copy of the relevant portion of your office's current Disaster Recovery Plan and are familiar with the plan and their roles in the plan.

- Complete your Spring and Fall Checklist, sign and forward to your respective division's Department Designee.
- See the Spring and Fall Checklist for a complete list of your responsibilities.

B. New Employee ASAP Orientation

Within two weeks of receiving a new employee or an employee who transfers from another division or facility, plan to review the ASAP safety and security procedures, including evacuation paths and introductions to Safety Wardens. Safety Wardens could assist you with this orientation.

C. Employee Emergency Information

Safety and Security Coordinators (SSC) can view the public information portion of the employees' records that they supervise. The private information portion of the employees' records can be viewed by the respective employee and a very limited number of people who would only access the information if the employee is incapacitated or during an emergency. Remind employees that the benefit of entering this information on their personal page is to ensure that the department possesses their basic contact and medical information in the event of an emergency. If an employee requires emergency medical attention, basic medical info can greatly assist the medical professionals in more quickly assessing the employee's possible condition. Likewise, employees' families or friends want to be notified of such medical emergencies. Employees can complete as much or as little of their page as they choose. If employees are concerned about privacy, they can still complete a paper form (found on the ASAP On-line website under ASAP Forms), seal in an envelope that states "Emergency Medical Information for Employee's Name" and place the envelope in an identifiable location in his/her work area. Next, the employee should return to his/her personal ASAP page and enter the identifiable location of the envelope. In the event of an emergency, the sealed envelope can be retrieved and handed to an emergency professional.

Evacuation Assistance

During evacuations, some employees have a more difficult time evacuating the floor due to physical or medical limitations. To ensure that all employees are efficiently and safely evacuated from our buildings during emergencies, employees who may be unable to accomplish the normal evacuation route are encouraged to seek evacuation assistance. To accomplish this, within the employee's emergency information page, employees can specify if they have physical or medical limitations to receive special assistance during evacuations. Encourage your employees to enter their information in this section as appropriate. Employees will be placed on your area/floor's Evacuation Assistance List and will receive special evacuation instructions and assistance. The evacuation assistance information is found in the Private Information portion of the employee's emergency information page and will only be viewable by the Agency of Administration and the Office of State Security Programs Director.

D. Exit Interview Process

- When an employee resigns, transfers, retires or is subject to termination, use the Exit Interview Checklist and follow these steps:
- Recover state assets in possession of said employee such as keys, cell phone, pager, laptop, manuals, etc.
- Recover security access devices such as keys and swipe cards
- Use the Office of State Security Programs to request the deactivation of the employee's security I.D., passwords and accounts. The request system can be accessed at <http://www.bgs.state.vt.us/security/index.html>

- Use the Exit Interview Checklist to conduct the interview, sign checklist and gain employee's signature on checklist. (Note: Checklist is to be signed by Safety and Security Coordinators (SSC) and employee after all state assets/security devices are collected.)
- Submit the completed Exit Interview Checklist to your employee relations officer.

E. Advocate Principles of ASAP and Lead By Example

- Take leadership role in all matters relating to ASAP plans and this list of responsibilities.
- Encourage employee participation in safety and security programs.
- Ensure that new employees and new consultants are introduced to other employees on floor and/or in facility.
- Remind employees to show their identification badges to the guard upon entering the building and to wear their badges above the waist on their outermost garment.
- Remind employees that all packages, handbags, briefcases and other containers may be subject to inspection by the building's guard.
- Remind employees to immediately report lost or stolen identification badges to building security.

F. Coordinate Emergency Response and Evacuations

- Immediately react and respond to all evacuation and emergency announcements.
- Recognize that building security personnel will not have forewarning of an emergency and will not be on your floor to coordinate the evacuation.
- After reaching a point of safety (if entire building is not evacuated) or after reaching your Assembly Area (if entire building is evacuated), engage the assistance of your Safety warden and account for your employees. Instruct your Safety warden to report status of employee count to building security if required to do so. Remain at your designated location until the "all clear" is given by emergency personnel or building security.
- Following the emergency/evacuation event, request from your Safety warden(s) the names of employees who failed to participate or were dilatory in participating and take appropriate action.

G. Support and Foster Role of Safety Wardens

- Assign an office Safety Warden and alternate Safety Warden and support these persons in accomplishing the duties of this role.
- Support and encourage your Safety Warden's leadership role to carry out the safety and security procedures for your office such as ordering evacuation upon notice from Building Management, or Security.
- With the assistance of your Safety Warden, identify emergency response plan (buddy system) for visually, hearing, and physically impaired employees and discuss this plan with your office's employees.
- Support and encourage your Safety Warden's attendance and participation in Safety Warden meetings or training sessions held by the building Safety and Security Coordinators (SSC)/security office.
- Assist Safety Warden in distributing or sharing safety/security information received at these meetings to your employees.
- Acknowledge and reference effort of Safety Warden on annual performance review form.
- Work with and engage your Safety Warden's assistance to heighten safety and security in your office.

H. Update and Share Relevant Safety and Security Information

- Ensure ASAP plans are kept current by notifying your division or office Safety Wardens of changes in points of contact, office changes, etc.

- Maintain Employee Emergency Information forms and ensure office Safety Warden is aware of the location of these forms.
- Ensure that you possess a list of your employees' names and telephone numbers to contact in the event of an emergency.
- Identify and inform employee of emergency report-in site (outside of building, but within walking distance).

I. Maintain and Share Relevant Disaster Recovery Information

- Establish priority list of mission-critical services.
- Establish and maintain a Disaster Recovery Plan for your office/program area - both on-site and off-site.
- Establish or build in redundancy for your critical systems and critical data.
- Identify your essential employees and their assigned roles based on the level of emergency.
- Ensure employees are familiar with their assigned roles in the event of a weather or disaster emergency.
- Identify and inform your employees of your office's alternate work location (in the event your building is closed).
- Identify positions that are likely to be deemed essential for both weather-related emergencies and disaster emergencies and reference this responsibility in position descriptions when possible.

J. Incident Response Team

- Identify members of management and/or staff to support SSC in responding to all emergency situations within their facility in support of the SSC.
- In cooperation with the Office of State Security Programs develop and implement training programs for the IRT.
- Coordinate activities of IRT during recovery operations.

K. Bomb Incident Responsibilities

- Designate a chain of command.
- Establish a command center.
- Decide what primary and alternate communications will be used.
- Establish clearly how and by whom a bomb threat will be evaluated.
- Decide what procedures will be followed when a bomb threat is received or device discovered.
- Determine to what extent the police will assist and at what point the police will respond.
- Provide an evacuation plan with enough flexibility to avoid a suspected danger area.
- Activate ICT to conduct search.
- Designate areas to be searched.
- Establish techniques to be utilized during search.
- Establish a procedure to report and track progress of the search and a method to lead qualified bomb technicians to a suspicious package.
- Have a contingency plan available if a bomb should go off.
- Establish a simple to follow procedure for the person receiving the bomb threat.
- Review your physical security plan in conjunction with the development of your bomb incident plan.

L. Command Center

1. Designate a primary location and an alternate location.
2. Assign personnel and designate decision-making authority.
3. Establish a method for tracking search teams.
4. Maintain a list of likely target areas.

5. Maintain a blueprint of floor diagrams in the center.
6. Establish primary and secondary methods of communication. (Caution-the use of two-way radios during a search can cause premature detonation of an electric blasting cap.)
7. Formulate a plan for establishing a command center, if a threat is received after normal work hours.
8. Maintain a roster of all necessary telephone numbers.

III. RESOURCES AND ASSISTANCE

If you have questions regarding the Agency-wide Safety/Security Action Plan (ASAP), please consult with the Office of State Security Programs at 828-0777.

In the effort of continuous process improvement, you are strongly encouraged to share your ideas to enhance ASAP and/or to facilitate the process developed. Please forward your comments to your Office of State Security Programs

Safety Warden Responsibilities

I. OVERVIEW:

The role of a Safety Warden is an important, vital service to the co-workers whom you assist. The primary function of the Safety Warden is to coordinate, educate and act as a liaison between building security and your many co-workers. You receive training and possess information regarding safety and security procedures that your co-workers do not. Therefore, it is essential that you recognize and respect the importance of this assignment. You are commended for assuming this important role for the State of Vermont

II. OFFICE SAFETY WARDENS

Safety Wardens have either been selected by their Safety and Security Coordinators (SSC) or volunteered for this important role. Each fall, Safety and Security Coordinators (SSC) will review and select Safety Wardens for their office area. Safety and Security Coordinators (SSC) will assess the interest and past participation of the office's current Safety Wardens when making their designations for the coming year.

At all times, Safety Wardens are expected to perform the following duties:

A. Be Prepared and Share Important Information

- Know your building's Safety Warden procedures (i.e., evacuation procedures, location of fire alarms, fire extinguishers, floor exits, final floor checks during evacuations, etc.) and be prepared to act.
- Attend and participate in all meetings or training sessions held by the building Safety and Security Coordinators (SSC)/security office.
- Attend and participate in all meetings or training sessions.
- Educate co-workers regarding the evacuation plan, floor plan, location of extinguishers, fire hoses, and location and operation of the fire alarm pull stations.
- Use office staff meetings or visit co-workers to share safety and security information on a periodic basis.

B. Advocate Principles of ASAP and Lead by Example

- Take a leadership role in all matters relating to the safety and security procedures for your assigned office (such as ordering an evacuation upon notice through an alarm, from Management, and/or Security).
- Advocate the value of your Safety Warden role.
- Partner with your building security personnel.

C. Coordinate Emergency Responses and Evacuations

- During building emergencies (when alarms are sounded), wear your building-appropriate Safety Warden identifiers such as orange vests, arm bands, etc.
- Collect visitor sign-in book and include non-State personnel with your final sweep of your area/floor.
- After reaching a point of safety (if entire building is not evacuated) or after reaching your Assembly Area (if entire building is evacuated), assist Safety and Security Coordinators (SSC) by taking a head count and remain there until the "all clear" is given by emergency personnel or building security.

- Provide to building security and/or emergency personnel, the employee count and other relevant information regarding involvement of smoke, flames, other unusual conditions and persons remaining on the floor.
- Recognize that building security personnel will not have forewarning of an emergency and will not be on your floor to coordinate the evacuation.
- Recognize that you are a main line of defense in the event of an evacuation. Your active role on your floor is essential.

D. Assist Your Safety and Security Coordinators (SSC) and Co-Workers

- Assist your Safety and Security Coordinators (SSC) during Spring and Fall ASAP Awareness Weeks by familiarizing employees with the above procedures.
- Assist your Safety and Security Coordinators (SSC) in advising new employees of above procedures in the first two weeks of employment (new employee orientation).
- Work with Safety and Security Coordinators (SSC) to identify emergency response plans (buddy system) for physically, hearing or visually impaired employees and discuss plan with other Safety Wardens and your co-workers.
- Assist Safety and Security Coordinators (SSC) in identifying a method and location of accounting for all employees in your office in the event of an evacuation.
- Assist your Safety and Security Coordinators (SSC) to ensure that each employee in your office receives handouts of safety and security information.
- Ensure that important security information and phone numbers are posted in a visible area of the office (i.e., Important Information to Know page from the ASAP binder will suffice).

E. Report Your Concerns

- Communicate your concerns and suggestions regarding safety and security to the Office of State Security Programs, your Department Designee, your building Safety captain/coordinator and/or your building security Safety and Security Coordinators (SSC).
- Provide to your Department Designee, post-drill and post-evacuation reports which contain the name(s) of employees who did not participate.
- If you occupy a public floor, log the number of non-participating (non-State employees) visitors; this information should be shared with your respective building security Safety and Security Coordinators (SSC).
- Offer suggestions to improve these guidelines to the Office of State Security Programs.

IV. ROLE OF DIVISION SAFETY WARDEN COORDINATORS AND SAFETY WARDEN CAPTAINS

The Division Safety Warden Coordinators and/or Safety Warden Captains are expected to coordinate the efforts of their divisions and/or other Safety Wardens to provide continuity and a coordinated response. The designation of Safety Warden Coordinator or Floor Warden Captain is left to the discretion of key Safety and Security Coordinators (SSC) on your floor (i.e., Safety and Security Coordinators (SSC) may make the selection or advise Safety Wardens to make the selection among their group of Safety Wardens). At all times, the coordinators and captains are expected to perform the following duties:

- Assist Safety and Security Coordinators (SSC) to ensure that each office has a designated Safety Warden with whom you can communicate security information.
- Coordinate with office administrators/Safety and Security Coordinators (SSC) to conduct annual mock exercises of relevant security and emergency procedures.
- Work with Safety and Security Coordinators (SSC) and other Safety Wardens to identify emergency response plan (buddy system) for physically impaired employees and employees with physical and medical limitations and discuss plan with other Safety Wardens.

- Communicate security information and office information (e.g., security enhancements, concerns, contact information) to your Safety and Security Coordinators (SSC), Department Designee and/or Office of State Security Programs.
- Communicate, as needed, security information to the program Safety and Security Coordinators (SSC) and/or other Safety Wardens and employees.
- Attend and participate in all meetings or training sessions held by the building Safety and Security Coordinators (SSC)/security office.
- Attend and participate in all meetings or training sessions.

Safety Warden Bi-Annual Checklist

The primary function of the Safety Warden is to coordinate, educate and act as a liaison between building security and your many co-workers. During spring and fall ASAP Awareness Weeks, Safety Wardens are expected to perform the following duties:

- ___ 1) Know your building's Safety warden procedures including
 - ___ evacuation procedures ___ location of fire extinguishers
 - ___ location of fire alarms ___ location of floor exits

- ___ 2) Know your role and the role of your floor/work area's fellow Safety Wardens during evacuations.
 - Fellow floor warden: _____ Role: _____
 - Fellow Safety warden: _____ Role: _____
 - Fellow Safety warden: _____ Role: _____
 - Fellow Safety warden: _____ Role: _____

- ___ 3) Possess a current list of your Safety /work area's employees who need evacuation assistance. Partner employees who need evacuation assistance with a "buddy" and ensure both employee and buddy know their intended evacuation path.

- ___ 4) Coordinate with your fellow floor/work area's Safety Wardens to divide duties including but not limited to the following:
 - ___ sweep of your area including offices *ASSIGNED TO:* _____
 - ___ sweep of women's restroom *ASSIGNED TO:* _____
 - ___ sweep of men's restroom *ASSIGNED TO:* _____
 - ___ sweep of each conference room..... *ASSIGNED TO:* _____
 - ___ designate buddy for hearing/
visually impaired employees *ASSIGNED TO:* _____
 - ___ create list of employees who
need evacuation assistance *ASSIGNED TO:* _____
 - ___ retrieve sign-in sheet book..... *ASSIGNED TO:* _____

- ___ 5) Create your evacuation checklist to remind you of tasks to be accomplished during evacuations. Share your checklist with your back-up Safety warden and with your floor/work area's Safety Warden Captain.

- ___ 6) Inform your Safety and Security Coordinators (SSC) if Safety warden designations are needed for other areas of for your floor/work area.

- ___ 7) Advocate Principles of ASAP and lead by example. Advocate the value of your Safety warden role and importance of employee participation in ASAP activities.

- ___ 8) Assist your Safety and Security Coordinators (SSC) in identifying a method and location of accounting for all employees in your office in the event of an evacuation.

- ___ 9) Educate your co-workers regarding the evacuation plan, floor plan, location of extinguishers, fire hoses, and location and operation of the fire alarm pull stations. Use office staff meetings or visit co-workers one-on-one to share safety and security information on a periodic basis.

Name

Date of update

Safety Wardens: Complete this form and retain this and corresponding documents with your Safety warden equipment and/or insert behind the Safety Warden tab in your ASAP Binder

Incident Response Team Responsibilities

1. Bomb Threat Incident

Pre-planning and coordination of ICT are essential in implementing an effective search of building. A central command mechanism is necessary to ensure a thorough and complete response. A building floor plan should be utilized. Wherever possible, the facility should be divided into zones or sections (prior to the actual conduct of the search), and ICT personnel be familiar with the zone or section they will be responsible for the search. Back-ups and supporting volunteers should also be identified for each zone or segment. A building floor plan should be available to those public safety personnel who will be responsible for responding to bomb threats and assist in searches. Not only will these floor plans support identification and assembly of the ICT, but also, as the search is conducted, each area can be "crossed off" the plan as it is searched.

Areas that are accessible to the public require special attention during a search, and may be vitally important if an evacuation is to be conducted. The level of the search should be commiserate with the perceived threat level:

- An occupant search is used when the threat's credibility is low. Occupants search their own areas. The search is completed quickly because occupants know their area and are most likely to notice anything unusual.
- ICT search is used when the threat's credibility is high. The search is very thorough and places the minimum number of personnel at risk. Evacuate the area completely, and ensure that it remains evacuated until the search is complete. Search teams will make a slow, thorough, systematic search of the area.

Search procedures for building:

- The search should begin with the outside and work toward the inside.
- Once inside, the search shall start from the lowest level and work up.
- Two-way radios are to be used for receiving only. Do not transmit. If communications with dispatch is required, use a telephone

During the search procedure the question often arises, "What am I looking for?" The basic rule is: Look for something that does not belong, or is out of the ordinary, or out of place. Conduct the search quickly, yet thoroughly, keeping the search time to a maximum of 15 to 20 minutes. Both the interior and exterior of the building should be searched.

What to look for, explosives can be packaged in a variety of containers:

- Most likely it will be camouflaged.
- The container is likely to be a common article such as a shoe or cigar box, a grocery bag, an athletic bag, airline flight bag, suitcase, attache case, etc.
- Look for the unusual or something that appears to be out of place.
- It is important that someone familiar with the area assist in the search in order to note something which is unusual or alien to the surroundings.
- Anything that does not belong, or whose nature and presence cannot be adequately explained is a suspicious object.

Historically, the following areas have been used to conceal explosive or hoax devices in buildings:

<i>Outside Station Areas</i>	<i>Inside Stations</i>
<ul style="list-style-type: none"> ✓ Trash cans Dumpsters Mailboxes Bushes ✓ Street drainage systems Storage areas Parked cars ✓ Shrubbery ✓ Newspaper Stands 	<ul style="list-style-type: none"> ✓ Ceilings with removable panels ✓ Overhead nooks ✓ Areas behind artwork, sculptures and benches ✓ Recently repaired/patched segments of walls, floors, or ceilings ✓ Elevator shafts ✓ Restrooms ✓ Behind access doors ✓ In crawl spaces ✓ Behind electrical fixtures ✓ In storage areas and utility rooms ✓ Trash receptacles ✓ Mail rooms ✓ Fire hose racks

Depending on the nature of the threat, searches may expand to include vehicles in the vicinity of the building.

Locating An Unidentified Suspicious Package

If an unidentified or suspicious object is found, all personnel should be instructed not to move it and to report it to the SSC or Ranking Public Safety Officer (if on scene).

The following information is essential:

- Location of the object
- Reason(s) suspected
- Description of the object
- Any other useful information – how difficult to secure area, evacuate, nearest emergency exits, etc.

Based on this information, decisions will be made regarding the following:

- Removal of persons at risk
- Establishment of perimeter control of the area to ensure that no one approaches or attempts to move the object
- Activities to establish ownership of the object. (In the event that legitimate property has been left behind in error prior to the bomb threat being received.)
- Assignment of someone familiar with the building and the area where the object is located to meet the Explosives Disposal Unit personnel on their arrival (in the event that they have been called)
- Continue implementation of search procedure until all areas have reported to the Command Center, as there may be more than one unidentified object

While ICT with the assistance of public safety personnel are conducting the search, and particularly while they are managing response to a suspicious package, they should keep in mind the following information:

Improvised Explosive Devices (IEDs) and other types of bombs inflict casualties in a variety of ways, including the following:

- Blast over pressure (a crushing action on vital components of the body; eardrums are the most vulnerable).
- Falling structural material.
- Flying debris (especially glass).
- Asphyxiation (lack of oxygen).
- Sudden body translation against rigid barriers or objects (being picked up and thrown by a pressure wave).
- Bomb fragments.
- Burns from incendiary devices or fires resulting from blast damage.
- Inhalation of toxic fumes resulting from fires.

The following are four general rules to follow to avoid injury from an IED:

- Move as far from a suspicious object as possible without being in further danger from other hazards such as traffic or secondary sources of explosion
- Stay out of the object's line-of-sight, thereby reducing the hazard of injury because of direct fragmentation
- Keep away from glass windows or other materials that could become flying debris
- Remain alert for additional or secondary explosive devices in the immediate area, especially if the existence of a bomb-threat evacuation assembly area has been highly publicized

Historically, perpetrators of bombings buildings (in foreign countries such as Israel, France, India, and England) have used two tactics that intensify the magnitude of casualties inflicted by detonation of an explosive device:

- Perpetrators have detonated a small device to bring public safety personnel to the site; a larger, more deadly device has detonated some time after the first device, thereby inflicting a large number of casualties on the first responder community.
- Perpetrators have used a real or simulated device to force the evacuation of a facility only to detonate a much more substantial device in identified bomb-threat evacuation assembly areas.
- These attacks are especially harmful because the evacuation assembly areas often concentrate transit personnel and passengers more densely than would otherwise be the case.

Disaster Emergency

A. Disaster Recovery Team

Effective disaster recovery requires a team-coordinated approach. Personnel involved in disaster recovery planning and response are: Designated Essential Employees, Senior Teams, Finance, Division Business Offices, program administrators and Safety and Security Coordinators (SSC), information technology personnel, mail and supply personnel, risk management personnel, telecommunications personnel, security personnel, Emergency Operations Center's coordinators and other employees as identified.

B. Communication during a Disaster Emergency

In the event of a disaster emergency, the Office of the Governor or Department of Public Safety will communicate with the directors and the emergency contact designee, the Office of Human Resources. Thereafter, the following shall occur:

- Public Safety will issue news releases to all relevant news media
- Employees will monitor their television and radio for instructions
- Employees will refer to their Emergency Information Response Card
- Employees will contact the ASAP Emergency Information line at 802-828-0777
- Check the State's Web site, <http://www.vermont.gov/>, or the BGS website at <http://www.bgs.state.vt.us/>.

C. Crisis Level Designation

The Secretary of Administration will rely upon and follow the Vermont Emergency Management Agency in its designation of a declared disaster emergency. To ensure response to emergency situations in a standardized manner, the following crisis levels are defined to allow Safety and Security Coordinators (SSC) to establish recovery plans based upon the level of emergency. The listed crisis levels for emergencies were defined by the Security Review Team and are offered for consideration. The levels were created to assist Safety and Security Coordinators (SSC) in developing Disaster Recovery plans based on severity of emergency. These defined levels may assist to assess and establish steps for contingency (back-up) plans and to restore critical and non-critical services during minor emergencies. These defined levels will likewise assist customers to more easily understand the recovery steps that will occur during a given event.

These designated crisis levels are similar in level of severity as the crisis action levels designated by the Emergency Management Agency (EMA) known as the Crisis Action System (CAS) which contain four levels titled CAS1, CAS2, CAS3 and CAS4, with CAS4 being the most severe. Although not exact in definition, the elevation of levels are similar in scope and severity to the state business operations.

Crisis level 1: A operating error, equipment failure or loss of data to non-critical service. This emergency does not threaten the delivery of critical services but would create a temporary inconvenience for one or more employees.

Crisis level 2: Customer agency experiences an operating error, equipment failure or loss of data to a critical service. Immediate failure or inability to restore service in short time frame would result in an interruption of service to customers.

Crisis level 3: Customer agency experiences minor or temporary damage to a facility, data, and/or equipment necessary to provide critical services creating a hazardous situation and/or interruption of service to customers. Failure to restore the critical service could impede or disable the state and/or our customer agencies from providing critical services and ultimately jeopardize missions to agency customers and Vermont citizens.

Crisis level 4: Customer agency experiences significant damage to a facility, data and/or equipment necessary to provide critical services. Critical services are rendered inoperable, facility access is not feasible or permissible, and data is lost due to severity of damage or hardship created from emergency.

D. EMA CRISIS ACTION SYSTEM DESIGNATION AND AGENCY OF ADMINISTRATION INVOLVEMENT

Agency of Administration has significant responsibility for the recovery of services on which our state agency customers rely. Agency of Administration also has significant roles at the Vermont Emergency Operations Center and a myriad of responsibilities listed in the state's Emergency Operations Plan (EOP). In addition to staffing for the recovery of critical services, Safety and Security Coordinators (SSC) must also identify the staffing levels needed to accomplish the EOP responsibilities and pre-identify employees to accomplish these responsibilities (for example, emergency procurement and contracting, support, administrative, and logistical services). Agency of Administration also has responsibilities within the Emergency Support Functions (ESFs) and Annexes of the EOP. The Emergency Operations Center has XX ESFs and several support and incident Annexes which are groupings of similar emergency functions which local governments are likely to need from the state. Each ESF or Annex utilizes a team approach and is led by a primary organization that coordinates activities and includes a number of support organizations/agencies that assist in carrying out the special responsibilities. The EOP can be found at: <http://www.dps.state.vt.us/vem/index.html>

The Emergency Operations Center utilizes a graduated emergency response program known as the Crisis Action System (CAS). CAS ensures that the level of state response corresponds to the disaster.

CAS #1: Vermont EMA begins coordinating with other local jurisdictions and/or state organizations to assess an incident. The Assessment Team Leader, ESF#5 personnel, Vermont EMA management and designated representatives will meet. Information is gathered and the event is monitored. Depending on the disaster, CAS#1 is either brought to closure or is elevated to CAS #2.

Agency of Administration Involvement: At CAS#1, depending on the type of disaster, Agency of Administration may be notified by the EMA that an assessment of a known incident is underway. Agency may be called to assist with the assessment.

CAS #2: State liaison personnel are sent to the site of a disaster to assess damage, provide information concerning the on-going situation and/or assess the needs of the political subdivision.

Additional state organizations may be called to the Assessment Room or to the site of the disaster and the local affected jurisdiction may declare an emergency. If state assistance is required, the governor declares a state of emergency and CAS 2 is elevated to CAS 3. If state assistance is not needed, the state will continue to monitor the incident until closure.

Agency of Administration Involvement: At CAS #2, depending on the type of disaster, Agency of Administration will be notified by the EMA that an assessment of a known incident is underway. Agency of Administration may be called to assist with the assessment.

CAS #3: Partial activation of the Vermont EOC with varying levels of 24-hour staffing and partial activation of State Emergency Support Functions (ESFs) occurs as CAS #3. A state emergency may be declared for the affected jurisdiction, and FEMA Region V monitoring of the event may increase to the point that the FEMA Emergency Response Team is sent to Vermont and federal resources are pre-positioned for federal response assistance. State-level damage assessments, needs assessments, and information-gathering operations continue. The Governor may request federal response/recovery assistance during CAS #3. If the incident continues to escalate and/or state resources are inadequate to address response/recovery needs, then the activation will be elevated to CAS #4.

Agency of Administration Involvement: At CAS#3, . Agency of Administration would coordinate and provide the services listed in ESF#7. . Agency of Administration is the “Lead Agency” for Emergency Support Function #7 Resource Support.

CAS #4: Full activation of the Vermont EOC with 24-hour staffing and activation of the majority of state ESFs occur at CAS #4. The governor requests response and recovery assistance from the federal government. The state coordinates with the federal Disaster Field Office (DFO) and State ESF representatives coordinate activities with federal ESF counterparts. The state maintains close coordination with local emergency management agencies.

Agency Involvement: At CAS #4, . Agency of Administration coordinates and provides the services listed in ESF#7 as well as the other responsibilities assigned to Agency of Administration as listed in the Vermont Emergency Operations Plan. Agency would be actively engaged in the 24-hour staffing and other responsibilities relevant to the emergency or disaster due to its role as “Lead Agency” for Emergency Support Function #X (ESF#X), Information and Planning, Standard Operating Procedure.

Standard Operating Procedures within Threat Levels

I. PURPOSE

The U.S. Homeland Security Advisory System (HSAS) uses a color/risk grid to inform the country of the likelihood of terrorist activity. The State of Vermont, Department of Public Safety has established a Threat Level guide to standardize actions within the State of Vermont. The state of Vermont will change threat condition levels automatically when changes are announced by the federal government. Thereafter, the Office of Homeland Security will assess Vermont's threat condition and recommend to the Governor to downgrade or upgrade, as warranted. All state organizations have established Standard Operating Procedures to provide direction and clarification to its Safety and Security Coordinators (SSC) and employees of actions that will occur when a certain threat condition is declared. To establish a basis for action within these threat conditions, The State has established several assumptions (see Section III). This document is intended to serve as a general guide. In the absence of prescribed action, Safety and Security Coordinators (SSC) and employees are expected to take appropriate action, as warranted.

II. THREAT CONDITIONS

Note: Protective measures are progressive. Each increase in the threat condition should include protective measures taken in the preceding threat condition.

A. Green - Low

Threat condition GREEN is declared when there is a low risk of terrorist attacks. The following general precautions within Threat Condition GREEN are to be taken:

1) Employees shall:

- Support and be familiar with the Agency-wide Safety/Security Action Plan (ASAP) including:
 - Be familiar with responsibilities (i.e., employee, Safety warden, Safety and Security Coordinators (SSC))
 - Take appropriate action regarding suspicious people and packages in your work area
 - Always wear ID badges on the outermost garment
 - Treat every alarm as a real event
 - Immediately react and respond to evacuation and emergency announcements
 - Escort visitors (i.e., non-state employees) to and from your office area
 - Ensure visitors comply with facilities' sign in/out processes
 - Be familiar with your assigned role in the event of an emergency
 - Know your office's evacuation report-in location
 - Know your office's alternate work location
 - Notify your superior of any gaps in safety/security procedures
 - Know where a copy of ASAP emergency information is located
 - Participate in departmental review/training during ASAP Awareness Weeks

2) Safety and Security personnel in State owned and managed buildings shall:

- Review security, response and evacuation procedures to ensure action steps are current and effective
- Enforce access control procedures (sign in/out, visitor badges, escorts, etc.) as warranted
- Notify tenants of any modifications to security procedures

- Conduct exercises as required

B. Blue - Guarded

Threat Condition BLUE is declared when there is a general risk of terrorist attacks. The following general precautions will be taken within Threat Condition BLUE:

1) Employees shall:

- Perform actions identified in preceding threat condition

2) Security personnel in State owned and managed buildings shall:

- Perform actions identified in preceding threat condition

C. Yellow - Elevated

Threat Condition YELLOW is declared when there is a significant risk of terrorist attacks. Upon declaration of Threat Condition YELLOW, Employees will take the following action:

1) Directors shall:

Issue internal advisory (News of the Day) to all employees to provide:

- notice of downgrading/upgrading of threat condition
- standard operating procedures within threat condition yellow
- other instructions as appropriate

2) Safety and Security Coordinators (SSC) shall:

- Ensure contact information for essential employee list is current.
- Ensure that staff possess and understand standard operating procedures
- Ensure that staff are aware of and understand other instructions issued by the director

3) Employees shall:

Perform actions identified in preceding threat condition

4) Security personnel in State owned and managed buildings shall:

- Perform actions identified in preceding threat condition
- Elevate protective security measures, as warranted
- Conduct drills as required; conduct evacuation exercises as appropriate

D. Orange - High

Threat Condition ORANGE is declared when there is a high risk of terrorist attacks. Within Threat Condition ORANGE, The State will operate under the assumption that a terrorist incident is probable and action steps will be performed to ensure the department and employees are in a state of readiness. Upon declaration of Threat Condition ORANGE, The State will take the following action:

1) Directors shall:

- Attend briefings of the State of Vermont Office of Homeland Security, and/or the Emergency Operations Center and disseminate relevant information to senior management teams and designated personnel
- Issue internal advisory to Safety and Security Coordinators (SSC), essential employees and Emergency Response Team members to provide:
 - notice of downgrading/upgrading of threat condition
 - instructions within threat condition orange

- additional instructions from Governor, Agency of Administration, and/or Dept. of Public Safety
 - Issue internal advisory (News of the Day) to all employees to provide:
 - notice of downgrading/upgrading of threat condition
 - standard operating procedures within threat condition orange
 - other instructions as appropriate
 - Consult with State of Vermont Office of Homeland Security and senior personnel to assess and institute additional action, as warranted
- 2). Safety and Security Coordinators (SSC) shall:
- Secure essential employee staffing level on first day of each new pay period
 - ascertain essential employee availability for two-week period
 - assign alternate personnel as needed to ensure essential coverage of critical services and fulfillment of obligation to State's Emergency Response Teams
 - inform director if essential employee staff level is deficient
 - Ensure customer contact list is current - maintain off-site copy
 - Review Contingency Plan: Identify steps that enable your office to maintain operations
 - consider modifications to shifts, employee assignments, employee availability, alternate work location, required supplies, IT requirements, etc.
 - notify employees of relevant steps
 - Disaster Recovery Plan: Review and assess disaster recovery plans
 - Review disaster recovery plan; ensure actions/information are current
 - Remind employees of assignments within plan
 - Notify employees of any modifications to plan
 - Ensure integrity of your critical operations and information
 - Verify backup information/off-site copies are current (establish schedule)
 - Verify off-site copies of critical information/documents
 - Verify location and access to stored back-up data
 - Notify off-site location of elevated threat condition - verify access to this location
 - Review respective responsibilities within the Terrorist Incident Annex
- 3)Employees shall:
- Perform actions defined in previous threat conditions
 - Heighten awareness and report suspicious persons/packages/vehicles to building security
 - Place increased emphasis to ensure that all visitors (non-state employees) display security badges and are escorted at all times
 - Report to building security, any unlocked rooms and storage areas not in regular use
- 4)Security personnel in State owned and managed buildings shall:
- Perform actions defined in previous threat conditions
 - Implement and conduct infrastructure security plans for threat condition orange
(*restricted information: maintained under separate cover*)
 - Restrict public access to critical infrastructure facilities
 - Notify tenants of security level modifications and impact
 - list date/time changes are effective
 - list modifications
 - provide instructions as appropriate
- 5)IT personnel shall:
- Perform actions defined in previous threat conditions
 - Implement critical infrastructure security measures for threat condition orange

(restricted information: maintained under separate cover)

- Test redundant systems and access to off-site data storage
- Review networking capabilities and/or establish alternative connection paths
- Report any data concerns/deficiencies to respective Safety and Security Coordinators (SSC)
- Collect/maintain offsite, appropriate network and contact information
- Report suspicious activity to appropriate officials

E. Red - Severe

Threat Condition RED is declared when a terrorism incident has occurred. Upon declaration of Threat Condition RED, The State will take the following action:

1) Directors shall:

- Issue internal advisory to place on alert status, all essential employees and Emergency Response Team members
- Issue internal advisory to Safety and Security Coordinators (SSC), essential employees and Emergency Response Team members to provide:
 - notice of upgrading to threat condition red
 - reminder that public facilities may be closed to non-state personnel with minimal notice
 - overview of standard operating procedures and added instructions within threat condition red
 - additional instructions from Governor, Secretary of Administration and/or Dept. of Public Safety
- Issue internal advisory (News of the Day) to employees to provide:
 - notice of upgrade to threat condition red
 - overview of standard operating procedures within threat condition red
 - other instructions as appropriate
- Respond to activation of Emergency Operations Center and Terrorist Incident Annex
- Provide briefings and attend briefings of the State of Vermont Office of Homeland Security, the State Security Review Committee, and/or the Emergency Operations Center and disseminate relevant information to/from senior management teams and designated personnel
- Consult with Governor's Office, State of Vermont Office of Homeland Security and senior personnel to assess and institute additional action, as warranted:
 - levels of access/levels of service including but not limited to:
 - mail processing and scanning
 - lockdown of facilities
 - relocation issues
 - personnel issues - department level, statewide level
 - IT services
- communication to employees, customers, vendors re: modified service levels

2) Safety and Security Coordinators (SSC) shall:

- Perform actions defined in previous threat conditions
- Respond to activation of Emergency Operations Center and Terrorist Incident Annex
- Evaluate staffing levels/service levels based on situation, threat of further attacks, etc.
- Assess impact of restrictions/limitations imposed at Threat Condition Red
- Notify and instruct employees, customers, vendors of restrictions/limitations
- Be prepared for closure/evacuation of building

- Be prepared to relocate operation to alternate location

3) Employees shall:

- Perform actions defined in previous threat conditions
- Await instructions from Directors and/or Safety and Security Coordinators (SSC)

4) Security personnel in State Owned and Managed Buildings shall:

- Perform actions defined in previous threat conditions
- Close buildings to all visitors and state employees who do not possess building ID/credentials
- Conduct security procedures as defined for threat condition red
(restricted information: maintained under separate cover)
- Notify tenants of security level modifications and impact
 - list date/time changes are effective
 - provide instructions as appropriate

5) IT personnel shall:

- Perform actions defined in previous threat conditions
- Implement critical infrastructure security measures for threat condition red
(restricted information: maintained under separate cover)

III. ASSUMPTIONS

To establish a basis for action within threat condition levels orange and red, The State have identified several triggering events. Within the framework of this document, the following assumptions have been applied.

- 1) Activation of Threat Condition RED represents that:
 - a terrorist act has occurred in the state of Vermont.
 - a terrorist act has occurred in a neighboring state or to a target outside the state, indicating a clear and present danger exists in the state of Vermont.
 - a major act of terrorism has occurred outside the state of Vermont and may/may not have the potential to affect or involve the state.
- 2) Activation of Threat Condition ORANGE represents that a credible threat of a terrorist act has been received and tangible (physical) targets and/or demographic targets have been identified as potential subjects of the terrorist act and these subjects exist or reside in the State of Vermont.

IV. EVALUATION AND MAINTENANCE

The actions within the threat condition levels will be reviewed on an annual basis and revisions will be announced and distributed as warranted.

Reference:

State of Vermont Emergency Operations Plan (EOP)

National Incident Command

Incident Commander/Unified Command

The

Incident Commander (IC) or the **Unified Command (UC)**

is responsible for all aspects of the response, including developing incident objectives and managing all incident operations.

The IC is faced with many responsibilities when he/she arrives on scene. Unless specifically assigned to another member of the Command or General Staffs, these responsibilities remain with the IC. Some of the more complex responsibilities include:

- Establish immediate priorities especially the safety of responders, other emergency workers, bystanders, and people involved in the incident.
- Stabilize the incident by ensuring life safety and managing resources efficiently and cost effectively.
- Determine incident objectives and strategy to achieve the objectives.
- Establish and monitor incident organization.
- Approve the implementation of the written or oral Incident Action Plan.
- Ensure adequate health and safety measures are in place.

Command Staff

The Command Staff is responsible for public affairs, health and safety, and liaison activities within the incident command structure. The IC/UC remains responsible for these activities or may assign individuals to carry out these responsibilities and report directly to the IC/UC.

- The **Information Officer's** role is to develop and release information about the incident to the news media, incident personnel, and other appropriate agencies and organizations.
- The **Liaison Officer's** role is to serve as the point of contact for assisting and coordinating activities between the IC/UC and various agencies and groups. This may include Congressional personnel, local government officials, and criminal investigating organizations and investigators arriving on the scene.
- The **Safety Officer's** role is to develop and recommend measures to the IC/UC for assuring personnel health and safety and to assess and/or anticipate hazardous and unsafe situations. The Safety Officer also develops the Site Safety Plan, reviews the Incident Action Plan for safety implications, and provides timely, complete, specific, and accurate assessment of hazards and required controls

General Staff

The **General Staff** includes Operations, Planning, Logistics, and Finance/Administrative responsibilities. These responsibilities remain with the IC until they are assigned to another individual. When the Operations, Planning, Logistics or Finance/Administrative responsibilities are established as separate functions under the IC, they are managed by a section chief and can be supported by other functional units.

- The **Operations** Staff is responsible for all operations directly applicable to the primary mission of the response.
- The **Planning** Staff is responsible for collecting, evaluating, and disseminating the tactical information related to the incident, and for preparing and documenting Incident Action Plans (IAP's).
- The **Logistics** Staff is responsible for providing facilities, services, and materials for the incident response.
- The **Finance and Administrative** Staff is responsible for all financial, administrative, and cost analysis aspects of the incident.

The following is a list of Command Staff and General Staff responsibilities that either the IC or UC of any response should perform or assign to appropriate members of the Command or General Staffs:

- Provide response direction;
- Coordinate effective communication;
- Coordinate resources;
- Establish incident priorities;
- Develop mutually agreed-upon incident objectives and approve response strategies;
- Assign objectives to the response structure;
- Review and approve IAP's;
- Ensure integration of response organizations into the ICS/UC;
- Establish protocols;
- Ensure worker and public health and safety; and
- Inform the media.

The modular organization of the ICS allows responders to scale their efforts and apply the parts of the ICS structure that best meet the demands of the incident. In other words, there are no hard and fast rules for when or how to expand the ICS organization. Many incidents will never require the activation of Planning, Logistics, or Finance/Administration Sections, while others will require some or all of them to be established. A major advantage of the ICS organization is the ability to fill only those parts of the organization that are required. For some incidents, and in some applications, only a few of the organization's functional elements may be required. However, if there is a need to expand the organization, additional positions exist within the ICS framework to meet virtually any need.

The **General Staff** includes Operations, Planning, Logistics, and Finance/Administrative responsibilities. These responsibilities remain with the IC until they are assigned to another individual. When the Operations, Planning, Logistics or Finance/Administrative responsibilities are established as separate functions under the IC, they are managed by a section chief and can be supported by other functional units.

- The **Operations** Staff is responsible for all operations directly applicable to the primary mission of the response.
- The **Planning** Staff is responsible for collecting, evaluating, and disseminating the tactical information related to the incident, and for preparing and documenting Incident Action Plans (IAP's).
- The **Logistics** Staff is responsible for providing facilities, services, and materials for the incident response.
- The **Finance and Administrative** Staff is responsible for all financial, administrative, and cost analysis aspects of the incident.

The following is a list of Command Staff and General Staff responsibilities that either the IC or UC of any response should perform or assign to appropriate members of the Command or General Staffs:

- Provide response direction;
- Coordinate effective communication;
- Coordinate resources;
- Establish incident priorities;
- Develop mutually agreed-upon incident objectives and approve response strategies;
- Assign objectives to the response structure;
- Review and approve IAP's;
- Ensure integration of response organizations into the ICS/UC;
- Establish protocols;
- Ensure worker and public health and safety; and
- Inform the media.

The modular organization of the ICS allows responders to scale their efforts and apply the parts of the ICS structure that best meet the demands of the incident. In other words, there are no hard and fast rules for when or how to expand the ICS organization. Many incidents will never require the activation of Planning, Logistics, or Finance/Administration Sections, while others will require some or all of them to be established. A major advantage of the ICS organization is the ability to fill only those parts of the organization that are required. For some incidents, and in some applications, only a few of the organization's functional elements may be required. However, if there is a need to expand the organization, additional positions exist within the ICS framework to meet virtually any need.

For example, in responses involving responders from a single jurisdiction, the ICS establishes an organization for comprehensive response management. However, when an incident involves more than one agency or jurisdiction, responders can expand the ICS framework to address a multi-jurisdictional incident.

The roles of the ICS participants will also vary depending on the incident and may even vary during the same incident. Staffing considerations are based on the needs of the incident. The number of personnel and the organization structure are dependent on the size and complexity of the incident. There is no absolute standard to follow. However, large-scale incidents will usually require that each component, or section, is set up separately with different staff members managing each section. A basic operating guideline is that the Incident Commander is responsible for all activities until command authority is transferred to another person.

Another key aspect of an ICS that warrants mention is the development of an IAP. A planning cycle is typically established by the Incident Commander and Planning Section Chief, and an IAP is then developed by the Planning Section for the next operational period (usually 12- or 24-hours in length) and submitted to the Incident Commander for approval. Creation of a planning cycle and development of an IAP for a particular operational period help focus available resources on the highest priorities/incident objectives. The planning cycle, if properly practiced, brings together everyone's input and identifies critical shortfalls that need to be addressed to carry out the Incident Commander's objectives for that period.

This document is to be used as a reference in determining incident response. The following link will also assist in providing more detailed information and forms to use.

<http://www.osha.gov/SLTC/etools/ics/org.html>

EMPLOYEE EMERGENCY INFORMATION

Employees are provided this form for completion. Submission of this form is not mandatory although it is encouraged so that basic contact and medical information is available in the event of an emergency.

Name: _____ Today's Date: _____

Home address: _____ Home Phone No: _____

MEDICAL INFORMATION:

Healthcare Insurance Carrier: _____

Doctor's Name: _____ Phone No: _____

Specialist's Name: _____ Phone No: _____

Preferred Hospital: _____

Known allergies to medications: _____

Other information that a medical professional should know: _____

EMERGENCY CONTACT INFORMATION:

Person(s) to contact in the event of an emergency:

Name: _____ Home Phone No: _____

Relationship: _____ Cellular: _____

Employer: _____ Work Phone No: _____

Pager: _____

Name: _____ Home Phone No: _____

Relationship: _____ Cellular: _____

Employer: _____ Work Phone No: _____

Pager: _____

Please submit this form to your Safety and Security Coordinators (SSC)/supervisor

NOTE: If you are concerned about privacy, submit this form to your supervisor in a sealed envelope. Place your name on the envelope and note "TO BE OPENED IN THE EVENT OF A MEDICAL EMERGENCY ONLY."

EXIT INTERVIEW CHECKLIST

Supervisors must complete this form for employees who are separating employment from or transferring to another division. Upon completion and upon signature of both supervisor and employee, submit this form to your division's employee relations officer. An employee's final paycheck will be contingent upon submission of the Exit Interview Checklist.

Date: _____

Supervisor's name: _____

Employee's name: _____

Division: _____

Office: _____

Separation date: _____

Employee is (check one):

- Transferring to another office in the same division
- Transferring to another division
- Transferring to another state agency, board or commission
- Leaving state government

Has the employee returned: Yes No N/A

Building I.D. badge _____

Security/access badges _____

Keys _____

Pager _____

Cell Phone _____

Blackberry _____

Flash Drive _____

Laptop computer _____

Secure ID token _____

ASAP Binder _____

Other _____

Is this employee: Yes No

A Safety Warden _____

An Essential Employee – Weather _____

An Essential Employee – Disaster _____

Visually, hearing, or physically impaired _____

Have the following officials been contacted (attach copy of e-mails to this form):

IT Services administrator/LAN to terminate accounts and access privileges

Telephone Coordinator to make necessary changes in phone service, voicemail, etc.

Your Division Safety and Security Coordinators (SSC) to ensure all equipment is returned.

Building Security of this employee's departure (if visually, hearing, or physically impaired)?

_____ If the employee is transferring to another agency or leaving state government, did you, as supervisor, ensure this employee has a scheduled exit interview appointment to meet with the division's employee relations officer and/or the Department of Human Resources? Important benefit information and separation documentation are reviewed with the employee at this meeting.

MEETING DATE/TIME: _____

Supervisor signature date Employee signature date

ACRONYMNS

ASAP	Area Safety and Security Program
ASSC	Alternate Safety and Security Coordinator
BGS	Buildings and General Services
CAS	Crisis Action System
CBRN	Chemical, Biological, Radiological, Nuclear
CC	Command Center
DFM	District Facility Manager
DHR	Department of Human Resources
DII	Department of Information and Innovation
DMV	Department of Motor Vehicles
EMA	Emergency Management Agency
EOC	Emergency Operation Center
EOP	Emergency Operations Plan
ESF	Emergency Support Functions
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FMS	Fleet management Services
HSAS	US Homeland Security Advisory System
IAP	Incident Action Plan
IC	Incident Commander
IED	Improvised Explosive Device
IRT	Incident Response Team
IT	Information Technology
NAC	National Automobile Club
SSC	Safety and Security Coordinator
UC	Unified Command