

# **Ohio Department of Health Laboratory**

## **Safety And Security Manual**

## Contents

Contents .....	2
1. ODH Employee Responsibilities.....	4
2. Employee and Visitor Arrival/Departure.....	6
3. Medical Emergency.....	8
4. Evacuation Procedures .....	9
5. Fire Emergency.....	11
6. Water or Flood Emergency .....	12
7. Tornado Warning .....	13
8. Earthquake Procedures .....	15
9. Power Failure.....	16
10. Elevator Malfunction.....	17
11. Bomb Threat .....	18
BOMB THREAT REPORT .....	19
12. Suspicious Package/Letter.....	22
13. Suspicious Person .....	24
14. Hostage/Weapons Situation or Active Shooter .....	25
15. Workplace Violence .....	26
16. Civil Disturbance .....	27
17. State Vehicle Trouble.....	28
18. Personal and Public Transportation .....	29
19. Hazardous Material Spill .....	30
20. Computer, Internet and Information Security.....	31
21. Cyber-attacks.....	35
22. Essential Employees.....	36
23. Public Safety Emergency Procedures .....	37
24. References.....	38
Appendix A: Important Phone Numbers .....	39
Appendix B: Evacuation Map .....	40
Appendix C: Floor Warden Responsibilities During Emergencies.....	41
Appendix D: Current Floor Wardens and AED Trained Staff .....	42
Appendix E: Intrusion Alarm System (Buildings 4 and 22).....	43
Appendix F: Injury/Illness Reporting and Workers Compensation Procedures for Work-Related Injuries .....	44

Safety/Security Documents: Safety and Security Manual (Version 10)

Date: June 1, 2015

Supersedes: Version 9 (January 2014)

Bureau of Public Health Laboratory, Ohio Department of Health

## 1. ODH Employee Responsibilities

The success of the ODH Laboratory Safety and Security Plan relies upon each employee, regardless of rank or physical location, to respect and become familiar with the safety, security and emergency response procedures of the department. The following responsibilities should be viewed as standard response and awareness guidelines for all ODH Laboratory employees.

- 1.1. Support and be familiar with the department's safety and security procedures.
  - 1.1.1. Each individual requiring regular access to the ODHL facility is issued an identification badge that serves as a picture ID and incorporates a unique employee code that can be read electronically by the proximity card readers.
  - 1.1.2. The ID Badge-Proximity Card is used to deactivate/activate facility intrusion detection systems as needed, provides access to the laboratory building, and provides access to specific areas within the laboratory building.
  - 1.1.3. Agency staff members are required to wear and display agency-issued identification badges at all times while in the ODHL facility. Badges should be worn above the waist on the outermost garment.
  - 1.1.4. Individuals are prohibited from sharing their assigned ID Badge-Proximity Card.
  - 1.1.5. Immediately report lost or stolen identification badges to the Bureau Chief (614-644-4632) or the Laboratory Safety and Security Officer (614-728-0393).
  - 1.1.6. If your ID Badge-Proximity Card is inadvertently left at home, a temporary badge may be issued by the ODHL Safety and Security Office (Building 4, Room 110). This badge will only allow the staff to have general building access only; no access to restricted areas is provided. Staff members are required to return the temporary Proximity Card daily.
  - 1.1.7. When access to the ODHL facility is no longer required, individuals must return the card to their supervisor who will request that campus security office deactivate access to the ODHL facility.
- 1.2. Support and comply with ODH Emergency Response Plan and ODH Laboratory Continuation of Operations Plan (COOP).
- 1.3. Display a building identification badge at all times. Badges should be worn above the waist on the outermost garment.
- 1.4. Immediately report lost or stolen identification badges to the Bureau Chief (614-644-4632) or the Laboratory Safety and Security Officer (614-728-0393).
- 1.5. Treat every alarm as a real event.
- 1.6. Be familiar with any assigned role in the event of an emergency.
- 1.7. Be familiar with after-hours/weekend emergency and security protocols if expected to work outside regular business hours (M-F 8:00am to 5:00pm)
- 1.8. Be familiar with [Appendix A: Important Phone Numbers](#) to reach appropriate safety or security personnel in an emergency.
- 1.9. Participate in safety and security training opportunities (e.g., mock exercises such as fire and tornado drills, etc.).
- 1.10. Be aware of changes around his or her desk and work site such as suspicious persons and packages and take appropriate action.
- 1.11. Be conscious of personal valuables and state-owned property and information, and contain or lock up accordingly.

- 1.12. Be reminded that depending on security risks, packages, handbags, briefcases and other containers may be subject to inspection by the building's security personnel.
- 1.13. Notify his or her supervisor of any gaps in the current safety and security procedures and current disaster recovery plan.
- 1.14. Assist ODH Laboratory Administration by identifying operational changes and facility changes that may alter established emergency procedures to ensure updates are incorporated into the appropriate plans.
- 1.15. Escort visitors to and from his or her office area to the reception area.
- 1.16. Carry a copy of the Ohio Department of Agriculture's Emergency Contact Information Card.

## 2. Employee and Visitor Arrival/Departure

Documentation of all staff and visitors is necessary for security purposes as well as providing a record of all personnel on site during an emergency evacuation. Identification (employee identification badge or visitor identification badge) must be displayed in a visible location at all times while in the buildings.

### 2.1. Employees - Normal business Hours

- 2.1.1. Upon arrival, all staff must register the time on the ODH Bi-Weekly Sign In/Out log.
- 2.1.2. If leaving your immediate work area for an extended time, notify your supervisor or other staff in case of an emergency.
- 2.1.3. Upon departure, register the time on the ODH Bi-Weekly Sign In/Out log.

### 2.2. Employees - After hours/weekends

- 2.2.1. Upon arrival, sign in at the Visitor Register inside the employee entrance of Building 22.
- 2.2.2. All staff must register the time on the ODH Bi-Weekly Sign In/Out log.
- 2.2.3. If leaving your immediate work area for an extended time, notify your supervisor or other staff in case of an emergency.
- 2.2.4. Upon departure, register the time on the ODH Bi-Weekly Sign In/Out log as well as the Visitor Register.
- 2.2.5. Refer to [Appendix E: Intrusion Alarm System](#) if working outside of normal operational hours.

### 2.3. Visitors

- 2.3.1. When possible, give advance notice to the Inventory Control Specialist(s) when visitors are expected. Give visitors internal contact information and be prepared to escort them through the lab upon arrival.
- 2.3.2. All visitors must register at the Building 4 entrance.
  - 2.3.2.1. Sign in at the Visitor Log Book.
  - 2.3.2.2. Obtain a Visitor Identification Badge. The badge contains a time-sensitive seal which becomes invalid after 24 hours.
  - 2.3.2.3. Upon departure, sign out at the Visitor Log Book and destroy the Visitor Identification Badge.
- 2.3.3. All visitors to the laboratory testing areas where confidential information is in use must have a current signed and dated [Ohio Department of Health Visitor Confidentiality and Non-Disclosure Agreement](#) on file with the Laboratory Safety and Security Officer. These forms are available at the laboratory visitor's entrance in Building 4. Documents must be renewed annually.
- 2.3.4. All visitors must be escorted at all times throughout the lab.

### 2.4. Suspicious Person

- 2.4.1. Refer to [Section 13: Suspicious Person](#) if you encounter an unfamiliar person in the lab.

Safety/Security Documents: Safety and Security Manual (Version 10)

Date: June 1, 2015

Supersedes: Version 9 (January 2014)

Bureau of Public Health Laboratory, Ohio Department of Health

2.4.2. Refer to Appendix I of the ODHL Select Agent Program Biosecurity Manual for details on reporting and investigating a security breach.

### 3. Medical Emergency

In the event of a true emergency situation, **call 9-911 immediately**. The Laboratory Administration Office (614-644-2563) has been designated as a “call-back number” for emergency personnel to call for more information if they need it. This phone should be monitored until emergency personnel arrive. Refer to Section 3 of [ODHL Select Agents and Toxins Biosafety Plan: BSL3 Practices](#) for information on emergency evacuation from the BSL3.

**3.1. Be prepared with the following information:**

- 3.1.1. Location of injured or ill person.
- 3.1.2. Any details available about the accident or illness.
- 3.1.3. Name of injured/ill person.

**3.2. Take the following action:**

- 3.2.1. Do not move the injured or ill employee.
- 3.2.2. Try to make the person comfortable. Cover with coat or blanket.
- 3.2.3. A designated person shall go to the building entrance and upon arrival, escort emergency personnel to the scene of the emergency.
- 3.2.4. Remain a minimum of 25 feet away from the scene of the emergency unless directed otherwise by emergency personnel.

**3.3. Notification and Documentation:**

- 3.3.1. Notify appropriate supervisors and the Bureau Chief (614-644-4632).
- 3.3.2. See [Appendix F: Injury/Illness Reporting and Workers Compensation Procedures for Work-Related Injuries](#) for forms and procedures associated with work-related injuries.



## 4. Evacuation Procedures

It is the responsibility of each employee to know the Floor Wardens and alternate Floor Wardens for the areas in which they routinely work ([Appendix D: Current Floor Wardens and AED Trained Staff](#)). It is also the responsibility of each employee to be familiar with the evacuation plan, including evacuation meeting points. Refer to [Appendix B: Evacuation Map](#) for routine evacuation meeting points outside of the buildings. Refer to Section 3 of [ODHL Select Agents and Toxins Biosafety Plan: BSL3 Practices](#) for information on emergency evacuation from the BSL3. Treat all emergency alarms as if they are real.

### 4.1. If an evacuation is called, take the following action:

- 4.1.1. Listen to the PA/alarm system for emergency evacuation type (fire/tornado) and specific instructions.
- 4.1.2. Follow the instructions of the [Floor Wardens](#).
- 4.1.3. Assist those co-workers requiring assistance (buddy system). If a co-worker cannot continue evacuation due to illness or incapacitation, assume the buddy role and seek the assistance of a Floor Warden.
- 4.1.4. Assist any visitors to the appropriate emergency evacuation meeting site.
- 4.1.5. Close the door of your office/lab as you leave.
- 4.1.6. Use the stairwells for evacuation if necessary. Do not use elevators.
  - 4.1.6.1. Prepare to merge with other people evacuating the building.
  - 4.1.6.2. Use the handrails and stay to the right in the stairwells.
  - 4.1.6.3. Be alert for safety personnel who use stairways to respond to emergencies.
- 4.1.7. Report to your designated emergency report-in location.
- 4.1.8. Stay quiet and alert to listen for your name during roll call.
- 4.1.9. Remain at the evacuation site until released by the Bureau Chief, Lab Director or Supervisor.
- 4.1.10. **Do not** leave the emergency evacuation meeting site prior to being given the all clear signal without notifying the floor warden or supervisor.
- 4.1.11. **Do not** use the passenger elevators.
- 4.1.12. **Do not** return to your work area for any reason during an evacuation.
- 4.1.13. **Do not** remain near the building after exiting the building. Proceed safely to the pre-determined emergency report-in location.
- 4.1.14. The Bureau Chief, Assistant Bureau Chief, and Lab Director should move to [Zone A](#) following evacuation for contact and decision-making purposes.

### 4.2. Floor Wardens:

- 4.2.1. Obtain a two-way radio, emergency evacuation kit, available AEDs, Employee Sign-in Book(s) and Visitor logs as applicable and take them to the evacuation meeting sites.
- 4.2.2. Refer to [Appendix C: Floor Warden Responsibilities During Emergencies](#) for more details.
- 4.2.3. If floor wardens are not able to communicate by radio, all floor wardens must meet at the entrance to the lane leading to the Building 22 loading dock to cross-check roll call lists to verify evacuations.

## Evacuation Procedures (cont.)

### 4.3. After-hours/Weekends

- 4.3.1. On-duty supervisor will take after-hours/weekend sign-in book to the evacuation meeting site ([Zone B](#)) to take role and meet with emergency personnel as needed.
- 4.3.2. Remain at the evacuation site until released by the on-duty supervisor.
- 4.3.3. Always report-in to the supervisor before leaving the area.

## 5. Fire Emergency

### 5.1. Upon discovery of a fire, take the following action:

- 5.1.1. Pull the fire alarm and leave the building.
- 5.1.2. **DO NOT** attempt to fight the fire.
- 5.1.3. Call 9-911 from a safe location.
- 5.1.4. If possible:
  - 5.1.4.1. Notify your [Floor Warden](#) and/or Alternate Floor Warden. Floor wardens will immediately begin evacuating the area.
  - 5.1.4.2. Call the Bureau Chief (614-644-4632) or Laboratory Administration Office (614-644-2563). After-hours/weekends, call the BT On-Call Supervisor (614-203-1462).
  - 5.1.4.3. Close the doors around the fire to contain it.

### 5.2. During evacuation, follow these fire safety procedures:

- 5.2.1. Refer to [Section 4: Evacuation Procedures](#) for specific evacuation information.
- 5.2.2. Refer to [Section 3 of ODHL Select Agents and Toxins Biosafety Plan: BSL3 Practices](#) for information on emergency evacuation from the BSL3.
- 5.2.3. Follow the instructions of the floor wardens and evacuate to the designated emergency evacuation meeting site.
- 5.2.4. **Do not** attempt to fight the fire.
- 5.2.5. Use the stairwell exits only. **Do not** use the elevators!
- 5.2.6. Keep doors closed, especially in the stairwells. Closing doors prevents the spread of fire by minimizing the oxygen flow to the fire. In addition, closed doors limit the spread of smoke.
- 5.2.7. Stay low – air is cooler and cleaner closer to the floor.
- 5.2.8. If caught in heavy smoke, take short breaths and crawl to escape.
- 5.2.9. Cover your mouth and nose with layers of fabric that can filter the air but still allow breathing. Examples include two to three layers of cotton such as a t-shirt, handkerchief or towel. Otherwise, several layers of tissue or paper towels may help.
- 5.2.10. Test doors before opening. **Do not** open warm doors. Open cool doors slowly; close quickly if you encounter smoke or flames. Use another escape route.
- 5.2.11. Should your clothing catch fire, **DO NOT run**. Stop, drop, cover face with hands and roll until fire is out.
- 5.2.12. Exit the building – do not attempt re-entry until advised it is safe to return.

### 5.3. If trapped inside during a fire emergency:

- 5.3.1. Keep doors closed; this prevents the spread of fire by minimizing the oxygen flow to the fire.
- 5.3.2. Fill/stuff cracks around doors and vents to keep smoke out.
- 5.3.3. Anticipate low or no visibility – do not panic.
- 5.3.4. If caught in heavy smoke, take short breaths and crawl to escape.
- 5.3.5. Stay low – air is cooler and cleaner closer to the floor.
- 5.3.6. Hold a wet cloth over your mouth and nose – use coffee filters, clothing, etc.
- 5.3.7. Listen for emergency evacuation teams.

- 5.3.8. Remain calm and encourage others to do the same.
- 5.3.9. Wait at a window and signal for help with a flashlight or by waving a light-colored cloth.

## 6. Water or Flood Emergency

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

- 6.1.1. Refer to Section 3 of [ODHL Select Agents and Toxins Biosafety Plan: BSL3 Practices](#) for information on emergency evacuation from the BSL3.
- 6.1.2. Avoid the wet area to prevent injury or accidental shock.
- 6.1.3. If possible, place a “Wet Floor” warning sign to alert others.
- 6.1.4. If during normal lab hours, contact the designated building maintenance liaison or a supervisor in the area.
- 6.1.5. After-hours/Weekends, call the KDR answering service at 1-888-456-3405 and be prepared to provide the following information:
  - 6.1.5.1. Your name
  - 6.1.5.2. Location/Room number of the emergency
  - 6.1.5.3. Telephone number where you can be reached
  - 6.1.5.4. KDR will then contact the appropriate people for response.
- 6.1.6. Contact the [Floor Warden](#) and inform them of the leak.

## 7. Tornado Warning

In the event of a tornado warning issued by the National Weather Service, an announcement will be made via the building intercom system by the Laboratory Safety Officer or administrative staff. The message will clearly state whether or not the evacuation order is a drill. All occupants of Building 22 and Building 4 are to evacuate to the Building 4 basement. Otherwise, the Building 22 restrooms may be used as an alternate tornado shelter.

### 7.1. 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.

### 7.2. 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. If an evacuation is necessary, an announcement will be made via the building intercom system to take shelter in the Building 4 basement. The Building 22 restrooms have also been designated as alternate tornado shelters.

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

- 7.3.1. Refer to Section 3 of [ODHL Select Agents and Toxins Biosafety Plan: BSL3 Practices](#) for information on emergency evacuation from the BSL3.
- 7.3.2. Follow the directions of your [Floor Warden](#).
- 7.3.3. Move away from the perimeter of the building and exterior.
- 7.3.4. Evacuate to the Building 4 basement. Upon arrival at the basement, gather in your section’s designated area as marked by signage and report to the nearest Floor Warden taking role.
- 7.3.5. Assist any visitors to the appropriate evacuation site.
- 7.3.6. Keep conversation and noise to a minimum so the Floor Wardens can communicate with you and each other.
- 7.3.7. If you are unable to evacuate to the Building 4 basement, the Building 22 restrooms have been designated as alternate tornado shelters. There is a tornado kit located in a cart in the restrooms containing flashlights, glow sticks and a small first aid kit.
- 7.3.8. Floor Wardens may use two-way radios if necessary to communicate any safety concerns to the Laboratory Safety Officer or designee. Otherwise, follow regular evacuation procedures as detailed in [Section 4: Evacuation Procedures](#).
- 7.3.9. **Do not** go 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.

7.3.10. **Do not** get on an elevator. If you cannot navigate the stairs to the Building 4 basement, take shelter in the Building 22 restrooms.

7.3.11. Remain in your designated evacuation area until you are given further instruction by the Floor Wardens, Laboratory Safety Officer, Lab Director or supervisors.

## **Tornado Warning (cont.)**

### **7.4. Floor Wardens**

7.4.1. Obtain available AEDs on the way to the Building 4 basement.

7.4.2. Once in the basement, obtain employee rosters (organized by laboratory sections) from the Tornado Evacuation Kit located on top of a filing cabinet in front of Room 4 and take roll.

7.4.3. After role has been completed, consult with supervisors and determine if anyone is missing.

### **7.5. After-hours/Weekends**

7.5.1. The supervisor on-duty will take the after-hours/weekend sign-in book to the Building 4 basement evacuation site to take role.

## 8. Earthquake Procedures

*Although earthquakes are rare in central Ohio, this area is near the New Madrid Fault Line.*

According to experts, evacuation of the building could, under most circumstances, be an unsafe course of action. Remember that a serious earthquake will be very widely felt, therefore, fire and police department switchboards may be jammed and inoperative, and telephone communications and utilities could be knocked out.

### 8.1. During an earthquake, take the following actions:

- 8.1.1. Refer to Section 3 of ODHL Select Agents and Toxins Biosafety Plan: BSL3 Practices for information on emergency evacuation from the BSL3.
- 8.1.2. Take cover under sturdy furniture, desks and tables.
- 8.1.3. Tuck and protect your head with your arms.
- 8.1.4. Keep at least 15 feet away from windows to avoid flying glass.
- 8.1.5. Stay under cover until you learn that the immediate danger is over.
- 8.1.6. Remain on your floor unless otherwise instructed.

### 8.2. Immediately after an earthquake, take the following action:

- 8.2.1. Do not light matches or toggle power to anything that could generate a spark until given clearance by management or emergency personnel.
- 8.2.2. Administer first aid and assist in rescue operation, as necessary. Carefully move the seriously injured to an emergency treatment center as soon as possible.
- 8.2.3. Use telephone for emergency calls only.

## 9. Power Failure

In the event of a power failure, employees are asked to inform their supervisor or the designated building maintenance liaison of any emergency lighting units that fail to operate when the power goes out or lighting units that fail to provide lighting for at least 15 minutes. Power outages, although inconvenient, provide an opportunity to monitor and test emergency lighting units. Employee assistance will be appreciated by building managers.

### 9.1. Preparing for power failures

- 9.1.1. The laboratory has permanently installed emergency back-up generators.
  - 9.1.1.1. Identify and connect essential equipment to emergency power circuits (red outlets).
  - 9.1.1.2. Be careful not to overload any circuit. Outlets are labeled with their corresponding circuit number.
  - 9.1.1.3. Run equipment through an uninterruptible power supply (UPS) if possible. It may take 20-30 seconds for the emergency power to activate after a power failure.
- 9.1.2. Equipment that operates unattended should be programmed to shut down safely during a power failure and not restart automatically when power returns.
- 9.1.3. Identify hazardous equipment that should be turned off after power fails because it might cause injury when restarted after power returns.
- 9.1.4. Employees need to be aware of the equipment in their respective areas that would need to be shut off.
- 9.1.5. Save any active computer files regularly so as not to lose data when the power goes off suddenly. Make sure files are stored on network drives, which are backed up routinely.

### 9.2. While the power is off

- 9.2.1. Refer to Section 3 of ODHL Select Agents and Toxins Biosafety Plan: BSL3 Practices for information on emergency evacuation from the BSL3.
- 9.2.2. Shut down equipment which automatically restarts when power is available.
- 9.2.3. Check equipment on the emergency power system. In some cases, it may take 20 to 30 seconds for the emergency power to activate after a power failure.
- 9.2.4. Disconnect non-essential 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.

### 9.3. When the power returns

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

### 9.4. Emergency lighting

- 9.4.1. Emergency lighting should provide enough light for a safe exit. Battery-powered lighting will last a couple of hours, but may fail sooner.
- 9.4.2. Monitor level of lighting in hallways and stairwells to ensure you can exit safely.



## 10. Elevator Malfunction

Inform someone working with you that you will be using the elevator and when you expect to be done. This way someone will know to check after a period of time if you have not reported back. This is especially important after-hours and on weekends. Also, carry a cell phone with you on the elevator if possible.

- 10.1. If you are riding in an elevator that becomes stalled:
  - 10.1.1. Press the call/intercom button.
    - 10.1.1.1. This button calls the front desk in the Bromfield Building during normal business hours.
    - 10.1.1.2. KDR answering service (1-888-456-3405) monitors the elevator emergency call buttons after-hours and on weekends. The service will contact ODA Campus Security/Enforcement for follow-up if needed.
  - 10.1.2. Be prepared with as much information as possible concerning the stalled elevator, such as:
    - 10.1.2.1. Elevator location (freight elevator next to loading dock, or passenger elevator off of Building 22 hallway).
    - 10.1.2.2. Nearest floor level if it can be determined.
    - 10.1.2.3. Number of people and names of individuals on the elevator.
- 10.2. If you are able to call an outside number, also call the Laboratory Administration Office (614-644-2563) during normal business hours. After-hours/weekends, call the BT On-Call Supervisor (614-203-1462).
- 10.3. Remain calm. All efforts will be made to release individuals as quickly 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.
- 10.4. **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.

## 11. Bomb Threat

The chances of being the victim of a bomb are extremely remote. Although rare, the chances are considerably greater of receiving a telephoned bomb threat or finding a suspicious and potentially harmful device placed on the premises. In the event of a bomb threat, a building evacuation will be ordered via the building intercom system by the Bureau Chief, Assistant Bureau Chief, Laboratory Safety Officer, or Supervisor.

### 11.1. If you receive a bomb threat by phone:

- 11.1.1. Use the [Bomb Threat Report](#)
- 11.1.2. Remain calm.
- 11.1.3. Keep the caller on the line and attempt to gather additional information.
- 11.1.4. Notify co-workers while caller is on the line using the sign on page 15.

### 11.2. If you find a suspicious package or device:

- 11.2.1. Refer to [Section 12: Suspicious Package/Letter](#) for more details.
- 11.2.2. Do not touch the device OR items near the device. Movement may “trigger” a detonation.
- 11.2.3. Notify your supervisor, Laboratory Safety and Security Officer (614-728-0393) or Bureau Chief (614-644-4632) immediately.
- 11.2.4. Evacuate and cordon off the immediate area to prevent inadvertent exposure to the danger. Vibration from movement near the suspicious item may cause an explosion or a timing mechanism may be set to activate the device.
- 11.2.5. If possible, open windows to minimize the effect of any concussion caused by detonation.
- 11.2.6. Do not use cellular phones or other electronic equipment near the device.
- 11.2.7. Remain quiet and orderly during evacuations; listen for updated instructions.

### 11.3. Report the bomb threat, mail bomb or suspicious device:

- 11.3.1. If possible, use another phone to report the threat; experts can often track the location of a threatening call if the telephone is left unused.
- 11.3.2. Notify your supervisor, or call the Laboratory Administration Office (614-644-2563) or Bureau Chief (614-644-4632). Explain that you've received a bomb threat, mail bomb or have found a suspicious device at your workplace.
- 11.3.3. After-hours/weekends, call the BT On-Call Supervisor (614-203-1462).
- 11.3.4. Contact your [Floor Warden](#).
- 11.3.5. You and other co-workers may be requested to assist building management and the Ohio State Highway Patrol with the search, as employees are most familiar with their work surroundings.

## BOMB THREAT REPORT

Date: \_\_\_\_\_

Time: \_\_\_\_\_ A.M. or P.M.

**Instructions:** Be calm, be courteous, listen and do not interrupt the caller. Notify co-worker by pre-arranged signal while the caller is on the line.

**Exact Words of Person Placing Call:**

\_\_\_\_\_

**Questions to Ask:**

1. What kind of bomb is it? \_\_\_\_\_
2. When is the bomb going to explode? \_\_\_\_\_
3. What does it look like? Please describe it. \_\_\_\_\_
4. Where is it located? Can you give us the office and floor number and building location? \_\_\_\_\_
5. What will cause it to detonate? \_\_\_\_\_
6. Many innocent people may be hurt. Why are you doing this? \_\_\_\_\_
7. What is your name and address? \_\_\_\_\_

**Try to Determine the Following (Circle all appropriate items):**

<i>Caller's identity</i>	Male	Female	Adult	Juvenile	Age __ years
<i>Voice</i>	Loud Soft	Pleasant Intoxicated	High Pitch Deep Pitch	Raspy Other _____	
<i>Accent</i>	Local	Not Local	Foreign	Region _____	
<i>Speech</i>	Fast Slow	Distinct Distorted	Stutter Slurred	Nasal Lisp	Other _____
<i>Language</i>	Excellent	Good	Fair	Poor	Foul
<i>Manner</i>	Calm Angry Intoxicated	Righteous Deliberate	Coherent Incoherent	Rational Irrational	Emotional Laughing Other _____
<i>Background Noise</i>	Office machines Quiet voices	Factory machines Party atmosphere	Trains Street traffic	Animals Music	Airplanes Mixed Other _____

**Additional information:**

\_\_\_\_\_

**Action:**

- *If possible, use another phone to report the threat; experts can often track the location of a threatening call if left untouched.*

- Contact the appropriate personnel (See Monday-Friday/Weekend Info on page 38).  
Explain that you've received a bomb threat in the workplace.

Telephone Number Receiving Threat \_\_\_\_\_

Person Receiving Call: \_\_\_\_\_

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

**NOTIFY THE SUPERVISOR**

**CALL THE  
LAB ADMIN OFFICE**

**614-644-2563**

**or**

**614-644-4632**

## 12. Suspicious Package/Letter

The receipt of mail and packages are common in the normal course of our daily business at ODH. 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.

### 12.1. What constitutes a "suspicious" package/letter?

According to the U.S. Postal Service, a suspicious package is one that:

- 12.1.1. Is unexpected or from someone unfamiliar to you.
- 12.1.2. Is addressed to someone no longer with your organization or is otherwise outdated.
- 12.1.3. Has no return address or has an address that can't be verified as legitimate.
- 12.1.4. Has incorrect spelling of addressee's name or title.
- 12.1.5. Shows a city or state in the postmark that is a different location than the return address.
- 12.1.6. 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".
- 12.1.7. Is marked with restrictive endorsements, such as "personal" or "confidential".
- 12.1.8. Has excessive postage.
- 12.1.9. Is of unusual weight.
- 12.1.10. Feels rigid or appears uneven or lopsided, has an irregular shape, soft spots or bulges.
- 12.1.11. Has protruding wires, leaking liquid, powder residue, strange odors or stains.
- 12.1.12. Has contents that feel stuck (pressure or resistance) when attempting to remove from the envelope or parcel.

### 12.2. If you receive or find a suspicious package or letter:

- 12.2.1. **Do not handle or move** the package/letter. Movement may trigger a detonation.
- 12.2.2. Isolate the package and cordon off and evacuate the immediate area.
- 12.2.3. Do not use cellular phones or walkie-talkies in the immediate area of the package.
- 12.2.4. All persons who have touched the item should wash their hands with soap and water.
- 12.2.5. Notify your supervisor, or call the Laboratory Administration Office (614-644-2563) or Bureau Chief (614-644-4632). Explain that you've identified a suspicious package. They will take further steps to notify the police if necessary.
- 12.2.6. After-hours/weekends, call the BT On-Call Supervisor (614-203-1462).

### 12.3. If you've OPENED a suspicious package/letter:

- 12.3.1. Do not handle the item any further and follow the instructions above.
- 12.3.2. As soon as practical, wash hands with soap and water – shower if possible.
- 12.3.3. Make a list of all persons who have touched the letter and/or envelope. Include contact information. Provide the list to the proper officials.

- 12.3.4. Place all items worn when in contact with the suspected mail piece in plastic bags and have them available for law enforcement agents.

## 13. Suspicious Person

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

### 13.1. If you encounter a suspicious person in your work area:

- 13.1.1. If the person appears approachable, ask *“Can I help you? Are you here to meet with someone? Do you have an ID?”*
  - 13.1.1.1. If the response seems odd or vague, do not argue or continue the discussion. Provide a polite response and move on.
  - 13.1.1.2. Immediately notify a supervisor or the Laboratory Administration Office (614-644-2563) or the Bureau Chief (614-644-4632). On nights/weekends, notify the BT On-Call (614-203-1462).
- 13.1.2. If the person appears unapproachable, do not attempt to make contact.
  - 13.1.2.1. Immediately notify a supervisor or the Laboratory Administration Office or the Bureau Chief. On nights/weekends, notify the BT On-Call.
- 13.1.3. If a suspicious person approaches you or a co-worker, be polite and listen to the person’s concerns.
  - 13.1.3.1. If the person is unpleasant or abusive, do not argue. Provide a polite response and indicate you will locate a supervisor to arrange assistance and move on.
  - 13.1.3.2. Immediately notify a supervisor or the Laboratory Administration Office or the Bureau Chief. On nights/weekends, notify the BT On-Call.
- 13.1.4. It may be necessary to provide a description of the suspicious person. Try to make note of the following:
  - 13.1.4.1. Race
  - 13.1.4.2. Gender
  - 13.1.4.3. Hair features
  - 13.1.4.4. Facial features
  - 13.1.4.5. Clothing
  - 13.1.4.6. Location where the person was last seen
- 13.1.5. If safe to do so, observe, at a distance, the movement of the suspicious person. Do not attempt to make further contact.



## 14. Hostage/Weapons Situation or Active Shooter

### 14.1. If you find yourself in a hostage situation:

- 14.1.1. Don't be a hero and try to stay calm.
- 14.1.2. Follow instructions of the hostage taker(s).
- 14.1.3. Speak only when spoken to.
- 14.1.4. Don't make suggestions.
- 14.1.5. Try to rest and stay calm.
- 14.1.6. Be observant.
- 14.1.7. Be prepared to speak on the phone; you may be forced to do so.
- 14.1.8. Don't be argumentative and treat the hostage taker as normal as possible.
- 14.1.9. Be patient.
- 14.1.10. If police assault, drop to the floor and take cover under anything available.

### 14.2. If you attempt to risk an escape, ask yourself:

- 14.2.1. Can I do so quickly, quietly and safely?
- 14.2.2. Have I sufficiently studied the hostage-taker's pattern of behavior to give me a good chance of escape?
- 14.2.3. Will my absence be noticed?
- 14.2.4. Will my escape endanger the remaining hostages?

### 14.3. Active shooter situation

14.3.1. An active shooter is an individual actively engaged in killing or attempting to kill people in a confined and populated area, typically through the use of firearms. The U.S. Department of Homeland Security has outlined the following information regarding what to look for and how to respond to an active shooter situation.

#### 14.3.1.1. Characteristics of an active shooter situation:

- 14.3.1.1.1. Victims are selected at random.
- 14.3.1.1.2. The event is unpredictable and evolves quickly.
- 14.3.1.1.3. Law enforcement is usually required to end an active shooter situation.

#### 14.3.1.2. Coping with an active shooter situation:

- 14.3.1.2.1. Be aware of your environment and any possible dangers.
- 14.3.1.2.2. Take note of the two nearest exits in any facility you visit.
- 14.3.1.2.3. If you are in an office, stay there and secure the door.
- 14.3.1.2.4. Attempt to take the active shooter down as a last resort.

#### 14.3.1.3. How to respond when an active shooter is in your vicinity:

- 14.3.1.3.1. Evacuate
  - 14.3.1.3.1.1. Have an escape route and plan in mind.
  - 14.3.1.3.1.2. Leave your belongings behind.
  - 14.3.1.3.1.3. Keep your hands visible.

## 15. Workplace Violence

ODH is committed to providing its employees with a work environment that is safe, secure and free of harassment, threats, intimidation and violence. Refer to [ODH Directive 22: Workplace Violence](#) for more details, or contact the Office of Human Resources (614-466-2434).

### 15.1. Upon awareness of violence in the workplace, do the following:

15.1.1. If the crisis situation involves an injury:

15.1.1.1. Call 9-911

15.1.1.2. Notify a supervisor.

15.1.1.3. Call the Laboratory Administration Office (614-644-2563) or the Bureau Chief (614-644-4632). On nights/weekends, notify the BT On-Call (614-203-1462).

15.1.1.4. Notify Human Resources.

15.1.2. For all other crisis situations:

15.1.2.1. Notify a supervisor.

15.1.2.2. Call the Laboratory Administration Office or the Bureau Chief. On nights/weekends, notify the BT On-Call.

15.1.2.3. Notify Human Resources.

### 15.2. After the appropriate persons have been notified:

15.2.1. Personnel appointed by the Director shall coordinate with law enforcement, fire, medical and other community resources offering assistance as necessary.

15.2.2. If not directly involved in the incident, move to a secure area.

15.2.3. Always remain aware of your surroundings and move close to a door if possible.

15.2.4. Adhere to the requests of the assailant.

15.2.5. Make mental notes regarding the description and mannerisms of the assailant.

15.2.6. Remove yourself from the area when security or law enforcement arrives.

## 16. 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.

### 16.1. Upon awareness of a civil disturbance, do the following:

- 16.1.1. Remain calm. Do not draw any attention to yourself.
- 16.1.2. Campus and building management will establish contact with the appropriate law enforcement unit(s). Be prepared to provide the following information:
  - 16.1.2.1. Type of event
  - 16.1.2.2. Location
  - 16.1.2.3. Size of group
  - 16.1.2.4. Identity of the groups' leader(s) (if possible)
  - 16.1.2.5. Any visible weapons
  - 16.1.2.6. Types of vehicles and license plate numbers
- 16.1.3. Leave the immediate area of the disturbance for your own safety.
- 16.1.4. Keep yourself and co-workers away from the situation for their own safety. Remain in your work area unless directed to relocate.
- 16.1.5. Avoid window areas; draw window blinds and keep curtains closed.
- 16.1.6. Building management will notify you when the situation is controlled.

## 17. State Vehicle Trouble

Refer to [ODH Directive 36A: Leased Vehicle Policy](#) for more details.

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

- 17.1.1. Obtain medical assistance for any injured persons.
- 17.1.2. Contact the State Highway Patrol at 1-877-7-PATROL (1-877-772-8765). If you are unable to reach the State Highway Patrol, contact the local authorities.
- 17.1.3. Complete a police report. In addition, complete the State Employees Accident Report and the B.M.V. Report, which are located in the glove box.
- 17.1.4. Obtain information from all involved parties (name, address, vehicle description, insurance, etc.) Do not forget to include the names and addresses of any witnesses.
- 17.1.5. Contact ODH Operations Management (Robert Ginn, 614-752-9314) to report the incident.

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

- 17.2.1. For assistance during the hours of 7:00 a.m. to 4:30 p.m., please contact ODH Operations Management (Robert Ginn, 614-752-9314) as soon as possible.
- 17.2.2. After regular hours, please contact the State Highway Patrol (740-587-0786) if you need immediate assistance.

## **18. Personal and Public Transportation**

All ODH employees must engage in a daily commute to their workplaces. Some employees also are 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:

### **18.1. Individual Transportation – personal or state-owned vehicle**

- 18.1.1. Always know where you are – know your surroundings.
- 18.1.2. Always be aware of what is going on around you.
- 18.1.3. If you are attacked, do something to draw attention to yourself.
- 18.1.4. When you get into your vehicle, lock your doors.
- 18.1.5. Keep your doors locked and windows rolled up.
- 18.1.6. 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 and then leave the area and call the police immediately.
- 18.1.7. Always remember to get a good description of the suspect and remember where and at what time the incident occurred.

### **18.2. Upon witnessing a carjacking and/or kidnapping:**

- 18.2.1. Do not draw attention to yourself.
- 18.2.2. Call 911.
- 18.2.3. Do not attempt to intervene.
- 18.2.4. Get descriptions of the suspect(s), victim(s), weapons(s), and/or vehicle(s).
- 18.2.5. Remember direction of travel.
- 18.2.6. Give detailed information to security over the phone or in person.
- 18.2.7. Wait in the vicinity for police assistance to arrive.

### **18.3. Public/Mass Transportation**

- 18.3.1. Plan your trip.
- 18.3.2. Have your exact fare ready before you leave. This way you won't have to fumble for your money at the fare box or display extra cash.
- 18.3.3. 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.
- 18.3.4. Find a seat on the aisle if possible. This allows you to observe everything around you and to avoid getting "boxed in" against the window.
- 18.3.5. Sit near the driver or operator, but avoid sitting right next to the door. Thieves may try to snatch jewelry or personal belongings from people near the door and then exit quickly.
- 18.3.6. Don't doze off on a bus or become too engrossed in a book. It can make you an easy target.
- 18.3.7. Keep your belongings in your lap, on your arm, or between your feet. Do not leave them on an empty seat.
- 18.3.8. Avoid displaying expensive-looking watches, rings, necklaces or other jewelry.
- 18.3.9. 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.

- 18.3.10. Observe the behavior of those around you. If you feel uneasy or threatened, change your seat or alert the driver.
- 18.3.11. Minimize the chances of losing your property by avoiding crowded buses.

## 19. Hazardous Material Spill

To be prepared in the event of a hazardous material spill in your work area, refer to the Material Safety Data Sheet (MSDS) or GHS Safety Data Sheet (SDS) to become familiar with any potential hazards associated with materials you will be working with **BEFORE** working with them. Refer to the Laboratory Chemical Hygiene Plan and the ODHL Select Agents and Toxins Biosafety Plan for further details.

### 19.1. For identifiable hazardous material spills in your work area:

- 19.1.1. Be familiar with the location and use of appropriate spill kits.
- 19.1.2. Contact lab staff trained in hazardous material operations (HAZWOPER) if the spill involves mercury, radiological materials, or any large volume (greater than one gallon or greater than one pound) chemical spill.
- 19.1.3. Notify a member of the HAZWOPER team once any spill kit has been used so materials can be replaced.

### 19.2. Current HAZWOPER trained staff:

- 19.2.1. Steve York (614-728-0393)
- 19.2.2. Ray Scharf (614-644-4678)
- 19.2.3. Katherine Grandfield (614-728-0391)
- 19.2.4. Denise Reed (614-728-0398)

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

- 19.3.1. Evacuate the immediate area until hazardous material is identified.
- 19.3.2. Immediately notify a supervisor, the Laboratory Administration Office (614-644-2563) or the Bureau Chief (614-644-4632). On nights/weekends, notify the BT On-Call (614-203-1462).
- 19.3.3. Do not attempt clean up until experts arrive.

## 20. Computer, Internet and Information Security

Information security violations can happen anywhere to anyone. It is the responsibility of each ODH employee to protect the information technology (IT) resources we use every day. Proactive daily work habits can help you protect the IT resources that DAS has entrusted to you.

Note that all visitors to the laboratory testing areas where confidential information is in use must have a current signed and dated [Ohio Department of Health Visitor Confidentiality and Non-Disclosure Agreement](#) on file with the Laboratory Safety and Security Officer. These forms are available at the laboratory visitor's entrance (Stackhouse Laboratory entrance) in Building 4.

The following statements are just guidelines. Refer to [ODH Directive 7C: Use and Security of Agency IT Resources](#), [ODH Directive 26B: Management and Security of ODH Authorized Equipment](#), [ODH Directive 23A: Information Technology and Sensitive Equipment Management](#) and [OMIS Letter 6A: Unauthorized Personal Information Disclosure and Notification](#) for more details.

### 20.1. Computer guidelines:

- 20.1.1. Do not share your computer, network and/or application (Outlook, OAKS, etc.) passwords except when working with the ODH Helpdesk or Office of Management Information Systems (OMIS) Administrator.
- 20.1.2. Do not use simple, obvious, or predictable passwords. For example, do not use the names of relatives or pets; nicknames; days and months; repetitive characters, etc.
- 20.1.3. Be creative when selecting passwords. Strong passwords use a minimum of eight characters and include a combination of symbols, numbers, upper and lowercase letters.
- 20.1.4. 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.
- 20.1.5. Do not use the "save password" option when using web-based applications.
- 20.1.6. Change your passwords if you suspect that any of your passwords are known to someone else. Notify your supervisor.
- 20.1.7. For new employees, always change the initial password assigned to you by the OMIS Administrator as soon as you receive it.
- 20.1.8. Change your passwords in accordance with the schedules established for the computers, networks and applications that you use.
- 20.1.9. Do not use someone else's Login ID and password. If you are having problems with your access, contact the ODH Helpdesk via phone (614-752-5190) or email ([helpstar@odh.ohio.gov](mailto:helpstar@odh.ohio.gov)).
- 20.1.10. Do not use your access privileges to enable others to access information that they are not authorized to access or to submit transactions that they are not authorized to submit.
- 20.1.11. 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

Safety/Security Documents: Safety and Security Manual (Version 10)

Date: June 1, 2015

Supersedes: Version 9 (January 2014)

Bureau of Public Health Laboratory, Ohio Department of Health

momentarily. Your computer will automatically lock after 15 minutes of inactivity.  
Remember – Lock it when you leave it!



## **Computer, Internet and Information Security (cont.)**

- 20.1.12. At the end of your workday, shut down your computer. This shut down heightens security, reduces energy usage and enables OMIS to deploy updates to your computer.
  - 20.1.13. Secure all portable devices (i.e., CDs, disks, flash drives, etc.) and store those containing sensitive information in a safe environment. Consult with your supervisor before removing a portable device from your work location.
  - 20.1.14. Consider electronic documents and e-mails that are part of official files for record retention before deleting old files and documents. Consult with your supervisor for guidance.
  - 20.1.15. All files should be stored on network drives for backup purposes. Personal files should not be stored on network drives.
  - 20.1.16. For ODH employees with web-based access to the state's computer systems, seek guidance from the ODH Helpdesk or the OMIS Administrator before accessing information using wireless, satellite and other evolving technologies.
  - 20.1.17. Do not install software without prior clearance from OMIS.
- 20.2. Internet, e-mail and other IT resources guidelines:**
- 20.2.1. Do not open (i.e., view, detach or launch) suspicious e-mail attachments.
  - 20.2.2. If you receive a suspicious e-mail attachment, contact the ODH Helpdesk via phone (614-752-5190) or email ([helpstar@odh.ohio.gov](mailto:helpstar@odh.ohio.gov)) immediately. Do not send a copy – verbally provide your name, the sender's name, date, and name of attachment.
  - 20.2.3. 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 the ODH Helpdesk.
  - 20.2.4. Do not configure your e-mail to automatically open attachments. If your e-mail program automatically opens attachments, disengage it or contact the ODH Helpdesk for assistance.
  - 20.2.5. Ensure confidential or sensitive information on ODH systems is protected with an effective authentication mechanism, encryption software or firewalls. Ensure the OMIS administrator knows the existence and location of confidential and sensitive information.
  - 20.2.6. Any personal use of IT resources that disrupts or interferes with government business, incurs an undue cost to the state, could potentially embarrass or harm the state, or has the appearance of impropriety is strictly prohibited. Personal use that is strictly prohibited includes, but is not limited to: violations of law, illegal copying, operating a business, accessing personal services, accessing sexually explicit material, harassment, gambling or wagering, mass e-mailing, and solicitation.
  - 20.2.7. Take all reasonable precautions to prevent the inadvertent dissemination of anyone else's information via the Internet, electronic mail or online services.

## Computer, Internet and Information Security (cont.)

20.2.8. State employees have no reasonable expectation of privacy in conjunction with their use of state-provided IT resources. Contents of state computers may be subject to review, investigation and public disclosure. Access and use of the Internet, including communication by e-mail and instant messaging and the content thereof, are not confidential, except in certain limited cases recognized by state or federal law. Web browsers leave traceable "footprints" to all sites visited. The state reserves the right to view any files and electronic communications on state computers, monitor and log all electronic activities, and report findings to appropriate supervisors and authorities.

### 20.3. Paper documents and file guidelines:

- 20.3.1. Do not leave sensitive or confidential information lying around. File or dispose of sensitive or confidential information properly and timely.
- 20.3.2. Per HIPPA guidelines, all patient information is considered confidential. Make sure that these materials are not left in places where unauthorized access may occur. Also, make sure that no patient information is thrown in the trash. It must be shredded prior to disposal.
- 20.3.3. Faxed information must contain a [cover sheet](#) with the information confidentiality clause.
- 20.3.4. Store valuable information in a secure location such as a locked desk, cabinet, or office.
- 20.3.5. Label your paper files for identification and store sensitive files in a secure location. If portable devices (disks, CDs, etc.) are included as part of a sensitive file, be sure to encrypt or password protect these portable devices. Personally owned flash (USB) drives are not permitted to be used with ODH computers or laptops. If flash drives are necessary in order to do your job, only a state-owned fully FIPS 140-2 compliant flash drive is permitted to be used. For questions regarding flash drive usage, please consult contact the ODH Helpdesk.

## 21. Cyber-attacks

ODH'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:

### 21.1. Reporting a cyber-attack:

- 21.1.1. Do not open or further tamper with the e-mail or your computer.
- 21.1.2. Immediately report the incident to ODH Helpdesk via phone (614-752-5190) or email ([helpstar@odh.ohio.gov](mailto:helpstar@odh.ohio.gov)).
- 21.1.3. Report the incident to your supervisor.

### 21.2. What is a cyber-attack:

- 21.2.1. 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:
  - 21.2.1.1. Incidents involving computer "hackers."
  - 21.2.1.2. Incidents involving system penetration or tampering.
  - 21.2.1.3. Unauthorized access to computing facilities, telecommunication (i.e., telephone, fax, teleconferencing) and networking services (i.e., e-mail) or equipment.
  - 21.2.1.4. Use of computing, network and telecommunication facilities for personal profit.
  - 21.2.1.5. Destruction or alteration of data, software and equipment.

21.3. **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.

21.4. **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.

21.5. **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, also are likely to be targeted.

## **22. Essential Employees**

### **22.1. Definition**

22.1.1. An essential employee is defined as an employee whose presence at the work location or alternate work location is critical to maintaining business operations during a weather and/or disaster emergency. Essential employees normally consist of a skeletal crew of employees necessary to maintain essential office functions such as security, health and safety, and mission-critical services.

### **22.2. Designation and Notification of Essential Employees**

22.2.1. Essential employees are designated by an employee's Division Chief or ODH Director. Employees are notified by letter of this designation and their job responsibilities in the event of an emergency. It is possible that an essential employee may be temporarily reassigned to assist with the recovery and restoration of a business service outside of his/her normal job duties.

### **22.3. Annual review and designation of Essential Employees**

22.3.1. Each year, by September 1, ODH managers will reevaluate the level of employees required to recover and restore the critical service and designate these employees as essential for weather emergencies and/or disaster emergencies.

22.3.2. By October 1, ODH managers will compile the list of essential employees. The list of essential employees is posted and forwarded to the Director of Public Safety and the labor unions, as appropriate per labor agreements.

### **22.4. Notification of Essential Employee Designation**

22.4.1. Employees who are designated as essential employees are advised of the designation by letter. Essential employees are also advised that they should expect to work during weather emergencies or disaster emergencies unless otherwise advised. However, essential employees are not guaranteed work. Essential employees must keep this letter to facilitate their travel to and from work on state roadways and highways during a declared weather emergency or disaster emergency.

### **22.5. Guidelines for employees**

22.5.1. For guidelines regarding employee responsibilities during a weather emergency, please contact Human Resources (614-466-2434). Note that any employee who is on scheduled leave during a declared weather emergency or disaster emergency shall be charged leave for the days previously requested regardless of the declared emergency.

## 23. Public Safety Emergency Procedures

ODH follows [DAS Directive HR-D-11: Public Safety Emergency Procedures](#), which establishes uniform procedures for all state agencies implementing public safety emergency procedures (including weather emergencies) for bargaining unit and exempt employees.

### 23.1. Essential vs. non-essential employees

- 23.1.1. Refer to [Section 22: Essential Employees](#) for detailed information.
- 23.1.2. In the event that the state declares a weather-related public safety emergency affecting work hours and operations for the State of Ohio, ODH employees who have been designated in writing as "essential" in a public safety emergency should report to work regardless of the severe weather, unless otherwise directed not to report.
- 23.1.3. All "non-essential" employees should tune in to local media for the latest information about any changes to building access and/or work hours.
- 23.1.4. Under most winter weather conditions, employees are expected to report to work as usual, while exercising extra caution and allowing for greater driving time to account for typical traffic hazards and delays.
- 23.1.5. Employees should also follow work unit procedures and/or contact their immediate supervisor as soon as possible if for any reason they are unable to report for work or if they are unable to report on time.
- 23.1.6. If you have any questions, please contact Human Resources (614-466-2434).

### 23.2. OPHCS Alert System

- 23.2.1. ODH also uses the Ohio Public Health Communications System (OPHCS) to communicate with employees. Any statewide or agency-specific closures will be communicated through OPHCS.
- 23.2.2. As an OPHCS user, you are required to login and validate your profile at least every 60 days so you can be reached when you are not at work.
- 23.2.3. Refer to the [OPHCS Pocket Guide](#) to assist in using the OPHCS system. The OPHCS Pocket Guide has been designed as an easy reference tool for accessing the website, updating your profile and confirming alerts.
- 23.2.4. For emergency notifications, please be sure to set your high alert profile with either your home phone or cell phone number, not your work number. Personal phone numbers are confidential and will not be shared.

## 24. References

- 24.1. Ohio Department of Administrative Services Agency-wide Safety/Security Action Plan (May 2010 Revision). Retrieved June 2013, from <http://das.ohio.gov/ASAP/SafetyandSecurityProcedures.aspx>.
- 24.2. Ohio Department of Health. *ODHnet*. Policies, Procedures and Forms. Retrieved June 2013 from [http://odhnet1/ppf/ppf\\_index.aspx](http://odhnet1/ppf/ppf_index.aspx).
- 24.3. Ohio Department of Health. *ODHnet*. Workers' Compensation. Retrieved June 2013 from [http://odhnet1/en/employee\\_services/human\\_resources/benefits/WorkersComp.aspx](http://odhnet1/en/employee_services/human_resources/benefits/WorkersComp.aspx).
- 24.4. Ohio Department of Health. Ohio Public Health Communication System (OPHCS). Retrieved June 2013 from <https://ophcs.odh.ohio.gov/Documents/New%20OPHCS%20Pocket%20Guide.pdf>.
- 24.5. Ohio Department of Health Laboratory. Laboratory Chemical Hygiene Plan. Version 1.
- 24.6. Ohio Department of Health Laboratory. ODHL Select Agent Program BioSecurity Manual. Updated 6-26-2012.
- 24.7. Ohio Department of Health Laboratory. ODHL Select Agents and Toxins Biosafety Plan. Updated 6-12-2012.

## Appendix A: Important Phone Numbers

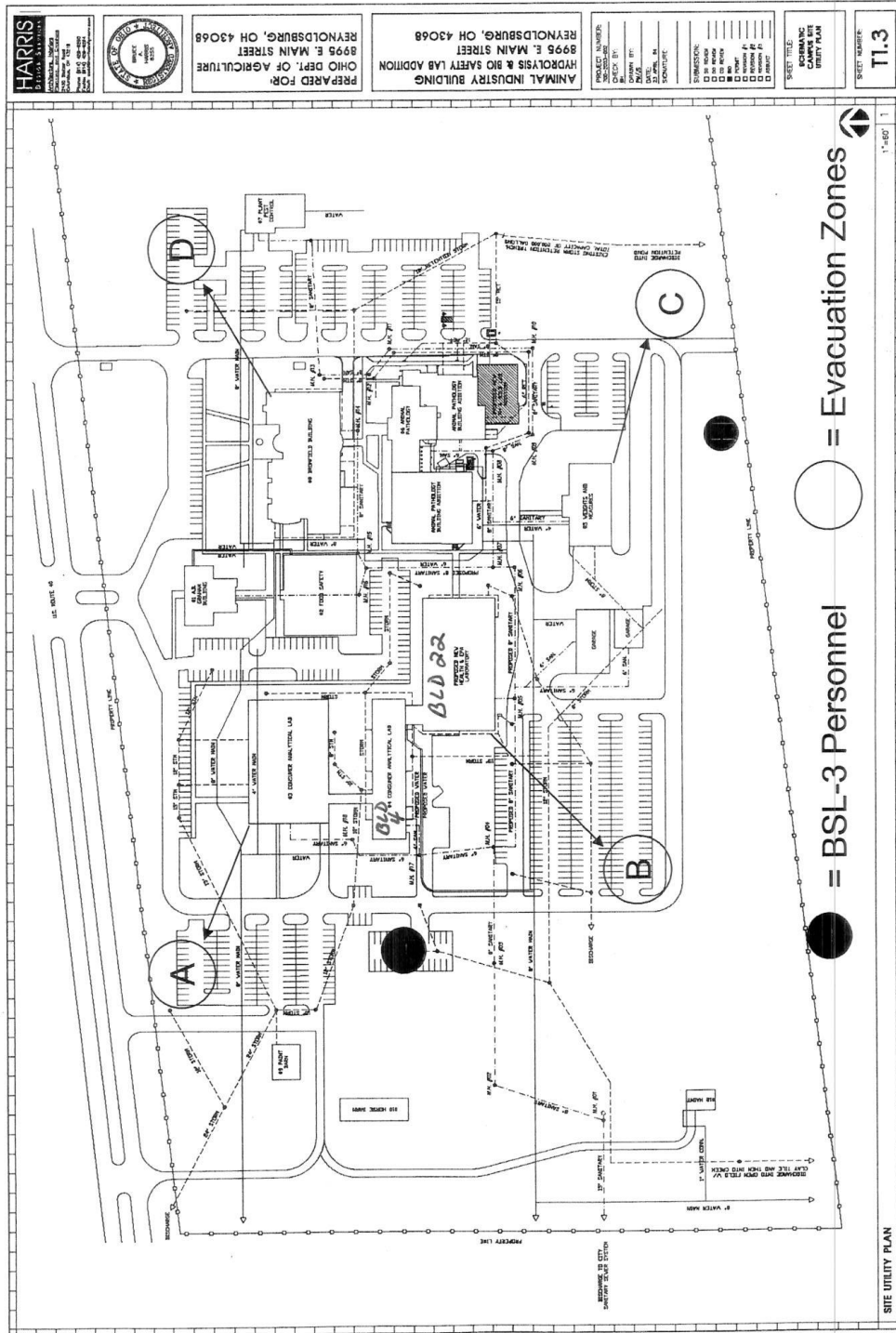
### External:

Fire/Police/Ambulance	9-911
Police (non-emergency)	
Licking County Sheriff's Office	740-670-5555
Ohio State Highway Patrol	740-927-0065
Truro Township Fire Department (non-emergency)	614-864-2445
Hospital (Mt. Carmel East)	
Non-emergency	614-234-6000
Emergency Room	614-234-6010
Department of Health	
Main Office	614-466-3543
Human Resources	614-466-2434
24/7 Public Health Response	614-722-7221
ODA Facilities Maintenance (Jeff Sholl)	614-374-7250
ODA Enforcement (Gary Hill)	614-728-6240

### Internal:

Laboratory Administration	
Rosemarie Gearhart (Bureau Chief)	614-644-4632
Dr. Tammy Bannerman (Lab Director)	614-644-4596
Supervisors	
Dr. Rosemary Hage (Newborn Screening)	614-644-4605
Brian Harrison (Biowatch)	614-728-0527
Larry King (Gen Micro)	614-752-9064
Sharon Linard (Follow-up and Data Entry)	614-644-4659
Kevin Sohner (Special Micro)	614-644-4668
Steve York (Quality Assurance and Safety)	614-728-0393
After Hours/Weekend Emergencies	
BT On-call	614-203-1462
KDR Answering Service	1-888-456-3405
ODA Facilities Maintenance (Jeff Sholl)	614-374-7250
ODA Campus Security (Gary Hill)	614-736-1326

# Appendix B: Evacuation Map





## Appendix C: Floor Warden Responsibilities During Emergencies

1. Ensure all personnel in your area are evacuating in an orderly and timely fashion. Provide assistance to disabled or injured persons as well as any visitors.
2. Ensure personnel do not use elevators during the evacuation.
3. Check restrooms, conference rooms and other remote areas for those who may not have heard the alarm.
4. Ensure employees close doors when exiting their areas.
5. Obtain AEDs, trauma bags, employee rosters and visitor log books as you proceed to the evacuation area.
6. Guide personnel to the designated [evacuation zone](#).
7. Once evacuated, coordinate with other floor wardens to complete roll call and verify all personnel are accounted for. Report any missing persons to the Laboratory Safety Officer or designee.
8. Maintain order at the evacuation areas until given further instructions by the Lab Director, Bureau Chief, Laboratory Safety Officer or designee.
9. After an evacuation:
  - a. Exchange the used Emergency Evacuation Rosters with a new copy from the Laboratory Safety Officer's office.
  - b. Report any issues or difficulties that arose to the Laboratory Safety Officer for resolution.
10. In the event of a [medical emergency](#), the first floor warden to respond is in charge of the situation.
  - a. Instruct someone to dial 9-911 and monitor the call-back phone until emergency personnel arrive.
  - b. If certified, administer first aid and/or CPR as needed. Otherwise contact someone [certified in First Aid and CPR](#).
11. Additional duties:
  - a. Periodically inspect their areas and report any hazardous conditions such as malfunctioning lights, obstructed hallways and aisles, and blocked fire alarms or extinguishers.
  - b. Ensure that employees in your area are familiar with evacuation procedures and locations of fire alarms.

## Appendix D: Current Floor Wardens and AED Trained Staff

Building 22 – First Floor		
NE Quad	Rick Bokanyi	Primary
	Eric Brandt	Alternate
Room 144	Jason Bean	Alternate
SE Quad	Donna Lee	Primary
	Rosemary Hage	Alternate
SW Quad	Rashmi Gaur	Primary
	Brian Harrison	Alternate
	Chelsea Dennis	Alternate
	Brent Lee	Alternate
	Amer Jameel	Alternate
	Shelley Pigg	Alternate
NW Quad	Jared Ford	Primary
	Melinda Dunn	Alternate
BSL3 & TB Areas	Eric St. Germain	Primary
		Alternate
Building 4	Dennis Cheyfitz	Primary
	Ray Scharf	Alternate
	Steve York	Alternate
Current As of 4/3/2013		

### CPR and AED Trained Personnel as of 04/3/2013:

Steve York	Melinda Dunn
Ray Scharf	Sharon Linard
Karen Cottrell	Beth Kolp
Dennis Cheyfitz	Rebekah Carman
Brian Harrison	Rosemary Hage
Denise Reed	

## Appendix E: Intrusion Alarm System (Buildings 4 and 22)

1. ODH Buildings 4 and 22 are equipped with an after-hours intrusion alarm system (burglar alarm) to detect break-in or entry by unauthorized individuals. This system automatically activates from 11:59 PM to 05:30 AM every day, 365 days a year. It is monitored by Simplex.

**NOTE: ODH staff must be accompanied by a Supervisor who will disable the system when entering Buildings 4 or 22 during these hours.**

2. Building access ID cards must be programmed by ODA to have arming and disarming authorization to operate the system.
3. The intrusion alarm siren is mounted on the south wall of building 22 near the emergency generator fuel tank privacy wall. It can be heard from outside areas of both buildings.
4. Note: the proximity card readers for the intrusion system are different from the square readers used for routine building access. Intrusion alarm card readers are thin, vertically mounted on the wall, and surrounded by red tape.
  - a. Swipe building access ID card near reader to deactivate/activate the alarm.
  - b. Do not swipe any ID card not issued by ODA (ODH-issued ID card, etc...) to prevent possible read errors and denial of arming/disarming access.
  - c. Avoid all dual access card swipes. If more than one access card is swiped, the system may not read the correct access card ID number and arming/disarming will be denied. This is an operator error, not a system error.
5. Arming/disarming locations in the buildings.
  - a. Building 22, south entrance door - located on east wall of vestibule.
  - b. Building 22, north entrance door - located on west wall of vestibule.
  - c. Building 22, west loading dock entrance door, next to north door (not BSL3 entrance door).
  - d. Building 4, east entrance door, north wall of vestibule.
6. Arming/disarming privileges:
  - a. ODH – all supervisors only.
  - b. EPA – all staff assigned to the laboratory.
7. Note the locations of the intrusion detectors in your work areas and do not place any items (boxes, lab coats, etc.) in the line-of-sight between detectors. These can cause false alarms when the system is activated.

## **Appendix F: Injury/Illness Reporting and Workers Compensation Procedures for Work-Related Injuries**

### **Employee Responsibilities:**

1. Notify your supervisor or human resources (HR) immediately.
  - a. Notification can include:
    - i. Completion and filing of an Employee Accident Report (Form [ADM 4303 Injury/Illness Report](#) (Rev. 8/2012)).
    - ii. Email notification with follow-up Employee Accident Report.
    - iii. Phone call with follow-up Employee Accident Report
  - b. After initial notification, continue communication with HR regarding any paperwork supplied by your treating physician or absence relating to your Workers' Compensation claim.
2. Seek treatment from a CareWorks network provider or BWC certified provider.
  - a. Mount Carmel East is designated as the provider for the ODH Lab, but you may receive treatment at any BWC certified provider.
  - b. Refer to a list and map of [BWC certified providers](#) in the Columbus area.
3. Show the BWC CareWorks I.D. Card (BWC Policy # 10003114-0) to each medical provider that treats your work related injury. Cards are available in the Quality Assurance Supervisor's office (Building 4, Room 110).

### **Supervisor Responsibilities:**

1. Notify HR immediately via completion and filing of a [Supervisor Accident Report \(HEA0332\)](#) or email/phone notification with follow-up Supervisor Accident Report completion.

### **Witness Responsibilities:**

1. Complete and file the [WC Witness Statement](#) with HR immediately.

Refer to [OHR Letter 12: Workers' Compensation Process](#) for more details.