

HANCOCK COUNTY ALCOHOL, DRUG ADDICTION AND
MENTAL HEALTH SERVICES
BOARD SAFETY AND SECURITY ACTION PLAN

The safety and security of employees, visitors, contractors and the general public are of vital importance to the ADAMHS Board.

BOARD EMPLOYEE RESPONSIBILITIES

The success of the Disaster Policy 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 the office. The following responsibilities should be viewed as standard response and awareness guidelines for all employees:

Employees shall:

- Support and be familiar with the office safety and security procedures.
- Be familiar with this list of responsibilities.
- 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.
- Be familiar with the "Important Number to Know" to reach appropriate safety or security personnel in an emergency.
- Be conscious of your personal valuables-contain or lock up accordingly.
- Support and comply with the office's disaster recovery plan.
- Be familiar with your assigned role in the event of an emergency.
- Know your office's designated report-in location (outside of building, but within walking distance - Findlay Fire Station on the corner of McManness and Tiffin Avenue
- Know your office's alternate work location (in the event your building is closed). Report to Hancock County Educational Service Center.
- Notify the Executive Director of any gaps in the current safety and security procedures and current disaster recovery plan.
- Identify operational changes and facility changes that may alter established emergency procedures.

CONCEALED/DANGEROUS WEAPONS

The possession or use of concealed/dangerous weapons is prohibited on ADAMHS Board owned property, in Board vehicles or in any personal vehicle which is used for Board business or is parked on Board owned property. Exception is only given to those employed in the capacity of a law enforcement officer, Bailiff or Judge.

A concealed/dangerous weapon is defined as:

- 1) A loaded or unloaded firearm
- 2) A weapon, device, electronic stun weapon, chemical substance or other material that in the manner it is used, or could ordinarily be used, or is intended to be used, is readily capable of causing serious bodily injury.

MEDICAL EMERGENCY

Reporting a medical emergency:

1. Call 911 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. Inform the Executive Director.

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. Notify the employee's family contact.

FIRE EMERGENCY

Upon discovery of a fire, take the following action:

1. Immediately leave the building and call 911.
2. If possible, close the doors around the fire to contain it.
3. Proceed to the nearest Exit and exit the building according to the evacuation plan.

During evacuation, follow these fire safety procedures:

1. Keep doors closed. Closing doors prevents the spread of fire by minimizing the oxygen flow to the fire. In addition, closed doors limit the spread of smoke.
2. **Do not** attempt to fight the fire.
3. If caught in heavy smoke, take **short** breaths and **crawl** to escape.
4. Exit the building according to the evacuation plan until advised it is safe to return.

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.

FIRE DRILLS

The Safety Officer will conduct full staff fire drills on a yearly basis.

WATER OR FLOOD EMERGENCY

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

1. Contact the Executive Director.
2. Avoid the wet area to prevent injury or accidental electrical shock.

TORNADO WARNING

In the event of a tornado warning issued by the National Weather Service, an announcement will be made advising employees 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.

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.

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

1. Close your door behind you.
2. Move away from the perimeter of the building and exterior to avoid flying glass.
3. Go to the core of the building: file vault.
4. If you are caught in an exterior office, seek protection under a desk.
5. **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.
6. You can be as safe on your own floor as anywhere else, stay in the interior portions of the floor.
7. Remain calm.
8. Once the storm is over, document any visible damage and notify the Executive Director.

EARTHQUAKE PROCEDURES

According to experts, evacuation of the building could, under most circumstances and according to location, 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, telephone communications and utilities could be knocked out.

During an earthquake, take the following action:

1. Take cover under desks and tables.
2. Keep at least 15 feet from windows to avoid flying glass.
3. Stay under cover until you learn that the immediate danger is over.
4. Remain on your floor unless otherwise instructed.

Immediately after an earthquake, take the following action:

1. Extinguish fires, if any. Do not light matches or fire until danger from gas leakage is over.
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.
3. Use telephone for emergency calls only.

POWER FAILURE

Preparing for power failures:

1. Make a list of equipment that must be reset or restarted once power returns. Keep instructions for doing so in the Disaster Policy File Folder.
2. Equipment that operates unattended should be programmed to shut down safely during a power failure and not restart automatically when power returns.
3. Assign an employee to shut off the power to all identified equipment unless there has been an order to evacuate the building. (Finance Director).

While the power is off:

1. Shut down equipment that automatically restarts when power is available.
2. 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 come on unexpectedly.

When the power returns:

1. Reset/restart/check equipment.
2. Assess and report any equipment failures to the Executive Director.

Emergency lighting:

1. Use flashlight that is located in the workroom.

Data backup:

1. Back up your computer files regularly so as not to lose data when the power goes off suddenly.

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 at your office or on your property.

First: If you receive a bomb threat by phone:

1. Use the Bomb Threat Report (attached on the next page).
2. Remain calm.
3. Keep the caller on the line and attempt to gather additional information.
4. Notify co-worker while caller is on the line. (USE THE SIGN ON THE PAGE AFTER THE BOMB THREAT REPORT)

Second: Report the bomb threat, mail bomb or suspicious device:

1. If possible, use another phone to report the threat; experts can often track the location of threatening call if left untouched.
2. Call 911 and report the threat.
3. You and other co-workers may be requested to assist security with the search, as employees are most familiar with their work surroundings.

If you find a suspicious package or device:

1. Do not touch the suspicious device OR items near the device. Movement may "trigger" a detonation.
2. Evacuate the immediate area to prevent inadvertent exposure to the danger. Vibration from movement near the suspected item may cause an explosion or a timing mechanism may be set to activate the device within minutes of placement.
3. Do not use cellular phones in the immediate area of the device.

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 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):

Caller's Identity	Male	Female	Adult	Juvenile	Age__years
Voice	Loud/Soft	Pleasant Intoxicated	High Pitch Deep Pitch	Raspy Other	
Accent	Local	Not Local	Foreign	Region__ __	
Speech	Fast/Slow	Distinct Distorted	Stutter Slurred	Nasal Lisp	Other_____
Language	Excellent	Good	Fair	Poor	Foul
Manner	Calm/Angry/ Intoxicated	Righteous Deliberate	Coherent Incoherent	Rational Irrational	Emotional Laughing/Other
Background Noise	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 threatening call if left untouched.*
- *Call 911. Explain that you've received a bomb threat, mail bomb or have found a suspicious device at you workplace.*

Telephone Number Receiving Threat: _____ Person Receiving
Call: _____

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

**TELL THE EXECUTIVE
DIRECTOR**

**NOTIFY THE POLICE
BY CALLING 911**

Suspicious Mail Handling

The receipt of mail and packages are common in the normal course of 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. Contact Law Enforcement.
2. Remain calm.
3. **Do not** open the parcel/letter. Seal the mail in a plastic bag.
4. **Do not** further handle the mail piece or package suspected of contamination.
5. Make sure that damaged or suspicious packages are isolated and away from employees.
6. Evacuate the immediate area.
7. 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. Contact Law Enforcement.
2. As soon as practical, shower with soap and water.
3. Do not further handle the mail piece or package suspected of contamination.
4. Make sure that damaged or suspicious packages are isolated.
5. Evacuate the immediate area.

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. Contact Law Enforcement. Explain that you've received a parcel in the mail that may contain a bomb, biological or chemical substance.
2. The proper officials will collect the mail, assess the threat situation and coordinate with the FBI, if necessary.
3. If necessary, Law Enforcement will notify local, county and state health departments and the Ohio Homeland Security Office.

Suspicious Person

The day-to-day operations of the Board 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 Law Enforcement.
2. If the person appears unapproachable, do not attempt to make contact. Immediately notify Law Enforcement.
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 Law Enforcement.
4. Provide a description of the suspicious person, making a note of the following:
 - Race (Caucasian, Black, Hispanic, Asian, Indian, Middle Eastern)
 - Gender (Male, Female)
 - Hair features (blond/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. Law Enforcement will remove suspicious person from the building.

Hostage/Weapons Situation

If you find yourself in a hostage situation:

1. Don't be a hero, 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?

Personal Transportation

Employees are required to travel to accomplish job responsibilities. Whether on your daily commute or on active travel status, please be mindful of the following safety guidelines.

Personal Transportation

- 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.
- When you get into your vehicle, lock your doors.
- Never drive around with your doors unlocked.
- Keep your doors locked and 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 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 law enforcement over the phone or in person.
7. Wait in the vicinity for police assistance to arrive.

Computer, Internet and Information

Information security violations can happen anywhere to anyone. It is the responsibility of each employee to protect the information resources used everyday. Proactive daily work habits can help you protect the information resources that the Board has entrusted to you.

COMPUTER GUIDELINES:

- Do not share network passwords.
- 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 4-6 characters long from a combination of both numbers and 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.
- 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 need more access than you presently have or if you are having problems with your access, get assistance.
- 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.
- If your workstation is located near a public area, logoff or enable a screen-saver with password capabilities if you are stepping away from your desk, even momentarily.
- Logoff at the end of the workday or when finished using your terminal or workstation.
- Label all your diskettes 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 regularly and frequently.
- Ensure you have a legal license for any computer software program before you install it. Software piracy is a serious violation that may result in punishment by both the Board and the software vendor.

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, immediately contact the Executive Director.
- 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.
- Do not configure your e-mail to automatically open attachments.
- Ensure confidential or sensitive information on your servers is protected with an effective authentication mechanism, encryption software or firewalls.
- 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.
- Do not use the Internet, electronic mail and online services to provide access to confidential information.
- Do not use the Internet, electronic mail or online service account or signature line other than your own.
- 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.

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

The Board'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:

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.
- Uses of computing, network and telecommunication facilities for personal profit.
- Destruction or alteration of data, software and equipment.

Reporting a cyber-attack:

1. Do not open or further tamper with the e-mail or your computer.
2. Report the incident to the Executive Director.

Hactivism: Hactivist (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.

SAFETY INSPECTION CHECK LIST

The Safety Officer will ensure that the Safety Inspection Check List is completed on a monthly basis.

IMPORTANT INFORMATION TO KNOW

EMERGENCY:

Police Department 419-424-7150
Sheriff's Office 419-422-2424
State Highway Patrol 419-423-1414
Fire Department 419-422-4242

CENTURY HEALTH:

**2515 North Main Street
Findlay, OH 45840**

General Office 419-425-5050
After Hours 1-888-936-7116
Executive Director, Corey Walker 419-399-9750 (home)
9864 Rd. 95 419-399-7059 (cell)
Pandora, OH 45879
Clinical Director, Tina Pine 419-436-0144 (home)
480 Angela Dr 419-937-7260 (cell)
Fostoria, OH 44830

FAMILY RESOURCE CENTERS:

1941 Carlin Street
Findlay, Oh 45840
419-422-8616
Findlay Site Director, Tonnie Guagenti 419-722-9281 (cell)
109 N. Main 419-995-2390 (pager)
Buckland, OH 45819 419-657-2224 (home)
Clinical Director, Cara Reynolds 419-382-8464 (home)
1019 Radcliffe Dr. 419-722-0023 (cell)
Toledo, OH 43609 419-412-1408 (pager)

Family Resource Centers

799 South Main Street
Lima, Oh 45804
1-800-472-5279
Interim Director, Tonnie Guagenti

FOCUS ON FRIENDS:

519 Trenton Avenue
Findlay Ohio 45840
419-423-5071

IMPORTANT INFORMATION TO KNOW

Ohio Department of Mental Health

614-466-2596 www.mh.state.oh.us

30 E. Broad Street

Columbus Oh 43215

Tina O'Grady, All Hazards Coordinator Phone 614-466-6152

Email: O'GradyT@mh.state.oh.us

Joseph Hill, Risk Administration, Manager Phone 614-644-6996

Ohio Department of Alcohol and Drug Addiction Services

614-466-3445 www.odadas.state.oh.us

2 Nationwide Plaza 12th Floor

280 N. High Street

Columbus, Oh 43215

L&M SUPPORTIVE HOUSING:

11012 Newland Rd.

Lakeview, Oh 43331

937-842-5887 (home/office)

Director, Lisa Markel, 419-230-1788 (cell)

AMERICAN RED CROSS:

419-422-9322

LOCAL EMERGENCY AGENCY:

419-424-7092

24 HOUR CRISIS HOTLINE:

1-888-936-7116

EMERGENCY REPORT-IN LOCATION:

Report to the Findlay Fire Station on the corner of McManness and Tiffin Avenue

ALTERNATIVE WORK LOCATION:

Hancock County Educational Service Center

7746 CR 140

Findlay, Oh 45840

419-422-7524