Welcome

Managing Through Crisis – Restructuring Program and Financial Plans
Disaster Planning and Recovery

Lauren Frary, M.A., LRC, CSW
Executive Director
The Arc of Somerset County (NJ)
About The Arc of Somerset County

- Incorporated in 1972
- Started with 1 program – pre school
- Initially had 16 children and 4 staff members
The Arc of Somerset County Today

• Today:
  • 35 separate programs throughout the County
  • 1400 children, adolescents and adults served
  • 17 Million annual budget
The Arc of Somerset County

- Full range of programs
  - Early Intervention
  - Day Care
  - Pre School
  - Respite (self hired and Saturday)
  - Parenting & Family Support
  - Residential
  - Employment/day hab/ supported employment
  - Integrated post secondary academic program
  - Camp
  - OT/ PT
WHY?

- Disaster planning, like strategic planning, is an ongoing process.
- As societal challenges change, so should disaster planning.
- Being prepared in advance saves time, resources and potentially lives.
- Provides stakeholders with confidence that your organization is acting in the best interest of those served and the community.
WHO?

- Disaster Planning must involve all the right people
- Internally and externally – you must have “buy in” when the disaster occurs
- Internally – allow all levels of the organization to have input
- Externally – develop relationships with local and state OEM, FEMA police, fire and other responders
HOW?

- Create a routine around disaster planning and test annually
- Financial planning for a disaster should be part of the annual risk management assessment and plan
- Identify all risks and determine the potential financial impact of each
- Consider all funding resources (including fundraising) and the potential impact of loss of funding
- Look at all financial options to determine what funds can be accessed and what expenses can be reduced
Cultivate

- Donor/volunteer and stake holder cultivation should be an ongoing process
- 7 points of contact annually (majority should not be solicitations)
- Create opportunities for acknowledgement of all donors/volunteers
- Determine each donor’s ability/propensity to give
- **Cultivation now will result in a greater return when you ask for support during a disaster**
The Importance of Stewardship

- Stewardship begins with the gift to your organization
- Have a donor acknowledgement/recognition policy
- Acknowledge the donor (regardless of the size of the gift) in a timely and accurate manner
- Ensure follow up to the gift to demonstrate that the donor’s gift is well protected and used efficiently for the organization’s mission
Stewardship

• Always be aware that you hold the public's trust with regard to donor gifts and funding.

• The goal of stewardship is to forge a lasting relationship with the donor – these donors will be more likely to give an additional gift during a disaster if requested.
• Saving is the single most important financial discipline you can master

• Savings often comes in the form of budgeting, getting on a strict saving schedule will ensure you know exactly what you have to work with

• While not everyone can save a significant amount each month, it is important to challenge your budget and stick to a number
Maintain Some Liquidity

- Have a great stock portfolio, but nothing in an actual savings account
- As we saw with the corona virus issue, the stock market plummeted before many had a chance to react
- People with no liquid assets had a terrible choice to make: either live on debt for a few months, or sell off shares at a massive loss
Liquidity

• This could have easily been avoided by setting aside some money in a high-interest savings account.

• Being too aggressive can lead to hefty losses

• Best practice: Three months operating CASH available at any given time
Planning for Risk

• Use a risk assessment tool to prioritize risks and the financial impact

• Make risk assessment/mitigation part of your strategic planning process

• Develop your disaster plan to include those risks

• Develop your response plan
Planning

• Develop your (disaster/recovery) business plan
• Share plans with others/outside experts
• Revisit the plan and have a drill annually
Disaster/Recovery Plan Team

Assemble your Team

• Executive staff
• Key leaders in both operations and programs
• Board members
• Local experts/first responders (FEMA, OEM, Red Cross)
Risk Assessment

Conduct a business impact/risk assessment

- Anticipate the increase in expenses and reduction of revenue that may occur
- Consider relocation of services/administration
- Consider how you will mitigate/transfer potential risks
- Make sure you have updated contact information
Risk Assessment Example

An Example
Pandemic specific Risk Questionnaire
Pandemic Specific Risk Management/ Questionnaire:

- **Legal**
  - Current Coverage sufficient?
  - Business interruption – virus exclusion?
  - Notifying Insurance/Legal counsel when a death occurs?
  - Do contracts/services/vendors need to be cancelled prior to expiration?
  - Are you in compliance with all regulatory agencies?
  - Risk management/Disaster plan updated?

- **Technology**
  - Sufficient technology to support work from home?
  - Technology updated?
  - Protections against network/server failure?
  - Sufficient technology to support activities from home?
  - Sufficient security/firewalls/etc...?
  - Virtual outlets (ZOOM, Works, Teams) secure?

- **Regulatory and Government policy Changes**
  - Regular monitoring of regulatory policy changes?
  - Documented verification of compliance with any changes?
  - Communication of policy changes to relevant employees and Board?

- **Environmental**
  - Reconfigure facilities/vehicles to allow for social distancing?
  - PPE and disinfectant are available throughout the facility?
  - Hand washing stations/hand sanitizer is available throughout the facility?
  - Professional cleaner/disinfecting service available/engaged
  - Work spaces and equipment (computer/phone/activity materials) sanitized regularly?
  - Private screening (temp. taking) area set up?
  - Screening tools kept confidential in compliance with HIPPA?

- **Security**
  - One point of entrance/exit for each facility?
  - Doors locked to control unannounced visitors?
  - Video cameras set up to prevent robbery/vandalism in vacant buildings?

- **Economic/Financial**
  - Pandemic business plan?
  - Analyze loss of revenue and increased expenses?
  - Opportunities for gap funding/grants/fundraising?
  - Reduce/suspend vendor contracts?
• 3 month of operating cash?
  ▪ Line of Credit sufficient?
  ▪ Reserves sufficient?
  ▪ Investments sufficient?
• Daily/ weekly cash flow projection/ analysis?
• Suspension of programs – financial impact?

• Human Resources
  • Sub and temp staffing available?
  • HR polices updated to allow for work from home/ accountability?
  • HR policies to reflect stay at home/ quarantine options?
  • Furlough all non essential employees?
  • Cross train employees to cover other tasks?
  • Understand leave/ disability policies?
  • Consider compensation for remaining employees?
  • Employees trained on all protocols? Training documented?
  • EAP available?
  • Ongoing communication of agency status with all employees?

• Supplies
  • Interruptions to supply chain considered?
  • Alternate suppliers explored?
  • Group purchasing considered?
  • Access local/ county/ State resources (DOH/ OEM/DHS)?

• Public Relations
  • Ongoing communication with all stakeholders (families included)?
  • Stewardship of current donors?
  • Prospecting new supporters?
  • Communication with local legislators regarding impact to agency?
  • Acknowledgement of all donations/ gifts in kind within 48 hours?
  • Update meetings/ communication with Board regularly?
  • Press release publicly thanking donors/ supporters?
  • Ongoing presence on social media?
  • Utilize volunteers for indirect supports?

LF --3/2020
Key Elements: Disaster/Recovery Plan

Develop a Disaster Recovery Plan

- Map out all of the steps to take to continue/reopen
- Assign staff to each task, make sure they have the resources to carry out their part of the plan
- Train each staff assigned to a role on their specific duties
- Follow the guidance of the National/Local Experts
Key Elements: Part 2

Develop a Disaster Recovery Plan

• Consider relocation sites, IT supports, PPE and Cash options

• Make sure all vital documents are backed up to the cloud or kept in a separate secure location

• Prioritize Services that will remain open and those that can be delayed
Key Elements: Part 3

Develop a Communication Plan

• Communicate often and honestly

• Use all methods available including social media to communicate your status

• Keep the public informed, to boost confidence and to access donations
Develop a Communication Plan

• Create a hotline or separate email for specific communications

• Be sure to communicate with Business partners such as Banks, insurance carriers/ brokers, Local OEM/ FEMA/DOH

• Use HR staff to communicate directly with Employees regarding return to work and available resources.
Distribute the Plan

• Make sure all team members have access to the plan both at the office and from home

• Provide a copy to your local OEM/ FEMA/DHS/DOH for comment and awareness
Key Elements: Part 6

Maintain, Test and Revise the Plan

• Review the plan with all stakeholders annually

• Put plan testing/drill on your calendar annually

• Modify or add addendums as needed and as new social/geographic challenges emerge
Disaster Plan

An Example
Disaster Administration Manual
The Arc of Somerset County

Disaster Recovery Administration Manual

2019
Index

Disaster Recovery Summary

Overview 1
Risks and Event Scenarios 1
Plan Activation Summary 2
Responsibility and Delegation of Authority 2
Incident Response Team Roles & Responsibilities 2
Disaster Notification/Communications 4
Building Evacuation 4
Emergency Operations Center 5
Activating the Disaster Recovery Plan 6

Appendix A – Policies & Procedures

Building Emergency Procedures A-1
Business Recovery Locations A-2
Emergency Personnel Policies A-3
Vital Records A-4

Appendix B – Checklists

Administration Coordination Checklist B-1
Finance Coordination Checklist B-2
First Person Onsite Checklist B-3
Functional Area Checklist B-4
Human Resources Coordination Checklist B-5
Incident Commander Checklist B-6
Pre-Evacuation Checklist B-7
Program Coordination Checklist B-8
Public Relations & Communications Coordination Checklist B-9
IT Coordination Checklist B-10

Appendix C – Forms

Communications Information C-1
Personnel & Board Contact Information C-2
Team Contact Information C-3
Team Contact Sheet C-4
Disaster Recovery Administration Manual

Overview
Community organizations have proven themselves to be cornerstones of support to the community, especially in times of need and disaster. When emergencies or disasters strike, The Arc must be well-prepared to quickly and effectively help itself in order to be able to help others to continue their services with as little program disruption as possible.

This plan outlines The Arc's strategy for responding to emergency or disaster, provides information essential to continuity of critical business functions, and identifies the resources needed to:
- ensure safety of individuals served and personnel
- communicate effectively with internal and external stakeholders
- provide timely emergency support
- protect assets and vital records (electronic data and hardcopy)
- maintain continuity of mission-critical services and support operations

Please note that no two emergencies are identical. Therefore, no single plan of action can anticipate and address every possible circumstance. The instructions contained in this plan may not be appropriate in all cases. At no time should you risk your personal safety in complying with any of its provisions.

Risks and Event Scenarios

Disasters are events that exceed the response capabilities of a community and/or the organizations that exist within it. Risks to be considered include those from natural hazards, neighbors, building environment, political or social unrest and risks connected to IT and data security.

The Arc is primarily at risk to disasters caused by:

   Extreme weather events, Flooding, Fire and Train Accidents, Terrorism

These events may impact business operations of the Organization on several Levels:

1. 1-2 Day Business Disruption
   An emergency or disaster that exceeds the capabilities and capacities of a city and/or county government response, but has a short duration such as a service outage, building outage, major fire, or site utility failure. May affect a large number of people for a short amount of time. All operations resume on-site in < 48 hrs.

2. 1 - 2 Week Business Disruption
   A crisis moderate to severe in scope. The Arc may have partial access to facility and/or primary IT systems. Examples include service loss, building access loss or local utility failure. May also include a regional event such as terrorism, contagious diseases or weather related disaster. Some business operations moved off-site. Small-scale work-from home / alternate site and remote access. All operations resume on-site in < 14 days.

3. > 2 Week Business Disruption
   A disaster including a complete loss of a facility and/or primary IT systems. Regional utility failure. All critical business operations moved off-site. Large-scale work-from-home / alternate site and remote access. All operations resume on-site in < 30 days or a new site is required.

During a disaster or emergency, The Arc must maintain "normal" operations required to address time-sensitive, disaster-specific issues. No plan can anticipate or include procedures to address all the human, operational and regulatory issues raised during a disaster or emergency. This plan addresses issues required for continuation of essential business functions, such as needs assessment, communication, volunteer outreach and coordination, and community assistance under rapidly changing circumstances.
Disaster Recovery Administration Manual

Plan Activation Summary
The Arc Executive Director, an appointee, or successor may activate this Plan when it is necessary to manage and coordinate a disaster response. The decision to activate will be made in consultation with members on the Board of Directors.

Responsibility and Delegation of Authority
The individuals included in the Incident Response Team (IRT) List will be responsible for the tasks listed. A checklist for each person is attached to this document in the Appendix.

IMPORTANT: For the FIRST PERSON ON SCENE WHO IS IN CHARGE, no matter what role in disaster; see Check Lists located in the Appendix.

If a designated individual is unavailable, authority will pass to the next individual on the list.

"Unavailable" is defined as:

- The designated person is incapable of carrying out the assigned duties by reason of death, disability, or distance from/response time to the facility.
- The designated person is unable to be contacted within an appropriate time period for the emergency or disaster. In a High Level disaster (see definitions on pages xx), this time period is defined one hour. If the person cannot be contacted within an hour, the second person should be contacted. In a Medium Level crisis, this time period is defined as four hours. In a Low Level emergency, this time period is defined as more than eight hours.
- The designated person has already been assigned to other emergency activities.

Incident Commander is required to update the Incident Response Team (IRT) list as well as the contact information in the Personnel & Board Contact Information Chart as changes occur.

Incident Response Team Roles & Responsibilities

Board of Directors
- Be available for emergency meetings, conference calls, approvals, etc.

CEO/Executive Director – usually the Incident Commander – IC
- Declare disaster to activate plan and command center.
- Manage the overall response.
- Establish appropriate staffing for the recovery and monitor effectiveness.
- Exercise overall responsibility for coordination between Emergency Operations Center (EOC) and Program Officers in the field.
- Act as The Arc's "public face" to the community.
- Move The Arc toward stated recovery objectives.

Administration
- Ensure that The Arc's offices are returned to normal operations as quickly as possible.
- Continue to provide basic services to individuals with I/DD -- in alternative locations
- Assist in the development of an alternate site as necessary.
- Assist staff with any aspect of travel including transportation and lodging.
- Oversee the investigation of property and equipment damage claims arising out of the event.
- Notify insurers and third party administrators as needed.
- Coordinate paperwork required by insurers to initiate claims process.
Disaster Recovery Administration Manual

IT/Telecom
- Recover computer and telephone technology (hardware and software).

Human Resources
- Is responsible for the "human" aspects of the disaster including post-event counseling and next-of-kin notification; answer questions related to compensation and benefits.
- Provide current roster of personnel.
- Provide emergency contact information for notification of next-of-kin.
- Track, record, and report all on-duty time for personnel working during the event.
- Ensure that personnel time records and other related information are prepared and submitted to payroll.
- Maintain a file of injuries and illnesses that includes results of investigations associated with the event.
- Oversee the investigation of injury claims arising out of the event.
- Attend all Emergency/ Disaster Recovery meetings.
- Update employee HRIS portal with critical information.
- Determine other resources that would support Employees through the disaster/ recovery period.
- Conduct periodic department visits, to assess needs.
- Bring EAP counselors on site as soon as safely possible.
- Distribute resource guide to employees that will information on shelters, food and other necessities.

Finance Management

Maintain appropriate level of funding for all essential business processes.
1. Ensure adequate funds are available to meet operating and recovery needs.
2. Project additional cash needs in relation to expected claims reimbursements.

Ensure easy access to necessary capital.
1. Monitor liquidity of assets based on projected expenses during the recovery.
2. Ensure that electronic accesses (Usernames and Passwords) to bank accounts are safely maintained.
3. Work with the bank relationship manager to utilize the Line of Credit if needed.
4. Work with Finance Committee to determine allocation of resources during recovery.

Continuity of Business Functions.
1. Ensure access to internet, accounting system and finance folder from home or disaster recovery center.
2. Continue to submit Medicaid billing and collect payments while in the process of recovery. Access to internet by programs is also important to be able to process Medicaid billing.
3. Maintain an updated list of active clients and contact information to follow up and collect payment.
4. Maintain an updated list of active vendors with payment schedule and contact information.
5. Coordinate with the vendors the situation and negotiate temporary grace period if needed.
6. Coordinate with the payroll provider where to deliver the payroll checks.
7. Coordinate with the programs where to pick up checks and petty cash.
8. Coordinate with the banks the current situation to help monitor cash movement.
Disaster Recovery Administration Manual

Establish and manage disaster funds and expenses.
1. Obtain an estimate of the total damages and identify available funds and grants that will be used for restoration.
2. Actively participate in the application process for grants (FEMA, SBA and other agencies) as well as in the review of the terms and conditions.
3. Act as a liaison between the Arc and the disaster assistance agencies to coordinate cost recovery process.
4. Keep track of all the expenses, receipts and other back up documents that may be required for reimbursement (grants or insurance) or audit purposes.
5. Prepare analysis reports comparing project costs to aid the executive team in making decisions and in selecting new vendor contracts for the restoration project.
6. Participate in the contract negotiations and review of proposals or quotes.
7. Provide a separate financial report related to the event and restoration to be presented to the board of directors and other stakeholders.
8. Provide information regarding insurance coverage as necessary.

Other responsibilities.
1. Track the total inventory of equipment, supplies and other properties that have been lost, impacted or damaged.
2. Fill out appropriate forms for damage claims and forward them to the insurers within the required time frame.
3. After the event, ensure that insurers and third party administrators or grantors honor contracts and pay claims; update reports on insurance or grant recoveries until claims are closed.

Public Relations / Development
- Is responsible for developing the media messages regarding any event.
- Is responsible for all stakeholder communications including the Board, Arc personnel, donors, grantees suppliers/vendors and the media.
- Serve as the primary media contact.
- Update and maintain Web site.
- Monitor media coverage and provide rumor control.
- Advise existing and new donors about donations.
- Provide customer service to existing, potential, and new donors.
- Use Social media and other resources to set up funding pages and public information
- Liaise with other Arc chapters and appropriate city and county offices.
Disaster Recovery Administration Manual

Disaster Notification/Communications

The Public Relations and Communications Coordinator will notify Arc personnel of plan activation and event status using the following methods:

- Employee/board call/e-mail tree
- Website, Facebook and other social media outlets
- Phone forwarding
- Conference call bridge (866-704-7500, pin-975412#)
- Web site as information center / Therap as secondary communications
- Media contacts
- *See Appendix C-2 and C-3 Personnel

Building Evacuation

Any decision to evacuate the building will be made by The Arc's management or Incident Commander. When the order to evacuate is given, follow the steps outlined in the Building Emergency Procedures Appendix A-1

The Pre Evacuation Checklist includes some guidance if you have notice of evacuation such as a hurricane.

EVACUATION CHECKLIST - GENERAL

1. Remain calm.
2. Immediately proceed to the nearest, safe exit. Assist visitors and colleagues whenever possible without jeopardizing personal safety.
3. Take personal belongings with you. Assume you have no more than one minute to safely collect your belongings.
4. If possible, shut down critical equipment/operations quickly and safely before exiting.
5. Proceed to The Arc's designated assembly area: Main Office – Opposite side of parking lot from building, closest to stores.
6. Once at the assembly area, check in with the Human Resources Coordinator. (See Incident Response Team list)
7. Remain at the designated assembly area until instructions are received.
8. Don't interfere with emergency personnel.

Within agency space, an Emergency kit will be located at Executive Administrative Assistant’s work area. The Executive Administrative Assistant is responsible for keeping this kit current. The kit includes the following materials:

1. Current Board contact list
2. Flashlight and back up batteries
3. First aid kit
4. Map of The Arc office
5. One of the kits should include a battery powered radio with backup batteries.

Executive Administrative Assistant. Will take the kits when exiting the building for use in the designated assembly area.
Emergency Operations Center
In the event of a disaster or emergency, the Incident Response Team (IRT) will convene at a physical location known as the Emergency Operations Center (EOC). From this location the IRT will manage the recovery process. The primary EOC may be on-site. The alternate EOC should be located off-site. If neither is available, Incident Response Team members should call in to the conference bridge number shown below.

Primary Location:
3 Jill Court, Building 15, Hillsborough, NJ 08844
908-431-0052

Alternate Location:
Branchburg ATC/OTC
161 Industrial Parkway, Branchburg, NJ 08876
Phone: 732-707-0737 or 9130  Fax: 732-707-1165
Activating the Disaster Recovery Plan

The Incident Commander (IC) sets the plan into motion. Early steps to take are as follows:

1. The Incident Commander should retrieve the Disaster Recovery Plan located in Jill Court. This plan is in printed form in the as well on computer media (CD-ROM). Copies of the plan should be made and handed out at the first meeting of the Recovery Team.

2. The Incident Commander is to appoint the remaining members of the Recovery Management Team. This should be done in consultation with surviving members of the team and with approval of the board. The Incident Commander’s decision about who sits on the Recovery Management Team is final, however.

3. The Incident Commander is to call a meeting of the Recovery Management Team at the Recovery Site or a designated alternate site. The following agenda is suggested for this meeting:
   1. Each member of the team is to review the status of their respective areas of responsibility.
   2. After this review, the Incident Commander makes the final decision about where to do the recovery. If the Jill Court site is to be used, the Incident Commander is to declare emergency use of the facility and notify the site manager immediately. The Incident Commander will also notify DDD, insurance brokers and legal counsel of the temporary closing of the program that is located at the site.
   3. The Incident Commander briefly reviews the Disaster Recovery Plan with the team.
   4. Any adjustments to the Disaster Recovery Plan to accommodate special circumstances are to be discussed and decided upon.
   5. Each member of the team is charged with fulfilling his/her respective role in the recovery and to begin work as scheduled in the Plan.
   6. Each member of the team is to review the makeup of their respective recovery teams. If individuals’ key to one of the recovery teams is unavailable, the Incident Commander is to assist in locating others who have the skills and experience necessary, including locating outside help from other area computer vendors.
   7. The next meeting of the Recovery Management Team is scheduled. It is suggested that the team meet at least once each day for the first week of the recovery process.

4. The Recovery Management Team members are to immediately start the process of contacting the people who will sit on their respective recovery teams and call meetings to set in motion their part of the recovery.

5. The Incident Commander is responsible for immediately clearing the Recovery Site rooms that are to be used by the Recovery Management Team. This includes the immediate relocation of any personnel occupying the room.

6. Mobile communications will be important during the early phases of the recovery process. This need can be satisfied through the use of cellular telephones.
APPENDIX A-1
Building Emergency Procedures

PURPOSE:
PERSON RESPONSIBLE: Primary: Executive Director
Secondary: Associate Executive Director

ACCIDENT/ILLNESS
1. Call 911
2. Do not move the injured/ill person unless it is necessary to avoid further injury
3. Use first aid kits located at Executive Administrative Assistant's desk.
4. Have a designated individual meet the emergency personnel at reception
5. Notify Human Resources
6. Ensure management notifies the employee's emergency contact

All employees should be familiar with the first-aid supply kits located in the break area and on top of the long cabinet across from the Executive Director's Office.

FIRE PROCEDURES
1. Do not panic
2. Call 911
3. Pull fire alarm
4. Take personal belongings with you. Assume you have no more than one minute to safely collect your belongings.
5. If possible, shut down critical equipment/operations quickly and safely before exiting
6. Do not shut off overhead lighting
7. Exit the building using the stairwells. DO NOT USE THE ELEVATORS.
8. Never open a door that may have a fire behind it. Feel the door with the back of your hand. If it is hot, DO NOT OPEN IT.
9. Follow the evacuation route posted in the building
10. Go to the designated meeting place at the back of parking lot, along store wall.
11. Once at the assembly area, check in with the Human Resources Coordinator.
12. Never attempt to fight a fire unless it can easily be put out. Fire extinguishers are located:
   - Conference Room 1
   - Near main office shredder and copier
   - JDCCF – Between Receptionist Desk and Doorway to basement
   - JDCCF – Across from Training Room
   - JDCCF – Between PACT and Main Office pass through, near room 4 Sensory Room
   - JDCCF – Kitchen
   - JDCCF – Hallway near classroom 6
   - Finance – Top of Stairway
   - Finance – Front Office under the second window closest to parking lot
   - Basement

If you hear an alarm, you should immediately assume you are at risk and prepare to leave. Do not, under any circumstances, use the phone system for any reason at this time. You may prevent the system from contacting 911.

If there is smoke, it may be necessary to crawl. There is usually good air and visibility about 18 inches from the floor. Once in the stairwell, keep moving. Stay quiet to hear any instructions from arriving police and fire personnel.
APPENDIX A-1
Building Emergency Procedures

POWER FAILURE
1. Stay where you are and await further instructions
   If instructed to evacuate, use stairwells
Battery-powered emergency lights will automatically come on. Telephones may not operate but FAX lines should operate.

ELEVATOR EMERGENCIES
1. Press emergency button
2. Wait for assistance

SECURITY SYSTEM
Security Cameras are located at various locations at the main office. Fire and emergency doors are equipped with panic bars.

BOMB THREAT
1. Record information concerning the call
2. Keep the caller on the line long enough to obtain as much information as possible
3. Attempt to get the caller to reveal specifics, i.e. location, detonation time, etc.
4. Listen for noises that may provide clues as to the location of the caller, i.e. motors, music, street noises, etc.
5. Listen closely to determine gender, emotional state, accents, speech impediments, etc.
6. Call 911
7. Notify management

SUSPICIOUS MAIL AND PACKAGES
1. Do not open, shake or smell it
2. Handle with care. Do not shake or bump.
3. Contact management to help evaluate the situation and determine next steps
4. If a parcel is open or threat identified, notify management and follow the precautions below.

For a bomb:
1. Evacuate immediately
2. Call 911

For radiological threats:
1. Limit exposure. Don't handle.
2. Evacuate the immediate area
3. Shield yourself from the object
4. Call 911

For biological or chemical threats:
1. Isolate package. Don't handle
2. Call 911
3. Wash hands with soap and warm water

Possible signs of a suspicious package:
- Protruding wires
- Lopsided or uneven
- Rigid or bulky
- Strange odor
- Oily stains or discolorations
- Excessive tape or string
- Wrong title or addressed to title only
- Misspelled words or badly written
APPENDIX A-1

Building Emergency Procedures

No return address
Excessive postage
Possibly mailed from a foreign country

EARTHQUAKE PROCEDURE
1. Evacuate the building using the posted evacuation routes
2. Move away from the building
3. Go to the designated meeting place
4. Once at the assembly area, check in with the Human Resources Coordinate.
5. Be aware of falling debris
6. Do not re-enter the building unless given permission by city officials
7. Remember that being outside does not guarantee your safety. Watch for flying glass, collapsing walls, falling trees, power lines and ground fissures.

TORNADO /SEVERE STORM PROCEDURES
1. Exit your exterior office and close the door.
2. If able, open window a small amount.
3. Move away from exterior glass.
4. Move to the lowest floor, interior of the building. Exit stairwells or windowless corridors are safest.
5. Once in a safe area, crouch or kneel down – facing the wall. Lower your head and cover it with clasped hands.
6. Remain in the safe area until the immediate danger has passed. Do not attempt to evacuate the building unless you are instructed to do so.

CHEMICAL HAZARDS
1. Turn off air conditioning systems.
2. Close all windows and doors.
3. Wait for instructions for emergency personnel.

AREA EVACUATION PLAN
1. If an area evacuation plan is activated, do NOT meet at the designated area. Follow the instruction of emergency personnel.
2. Contact with Somerset County OEM will be made for evacuation guidance

ACTIVE SHOOTER PLAN
See appendix for instructions for evacuation and lock down procedures.
Appendix A-2
Business / Service Recovery Locations

PURPOSE:  
PERSON RESPONSIBLE:  Primary: Incident Commander  
          Secondary: Designee

In the event of a disaster, the following business functions may be performed off-site at the locations shown below; or via home office.

<table>
<thead>
<tr>
<th>Department</th>
<th>Function</th>
<th>Performed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>BUSINESS – (Jill Court ATC &amp; Branchburg ATC or Camplain Road)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finance</td>
<td>Payroll, Accounts Payable and Receivable</td>
<td>Finance Staff</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Employee Coordination &amp; Benefits</td>
<td>Human Resources Staff</td>
</tr>
<tr>
<td>IT – Information Technology</td>
<td></td>
<td>Director of IT</td>
</tr>
<tr>
<td>Development</td>
<td>Communications</td>
<td>Director of Development, Assistant Director of Development</td>
</tr>
<tr>
<td>SERVICE – (Phone, Individual Home)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PACT</td>
<td>Family Support</td>
<td>Director of PACT</td>
</tr>
<tr>
<td>Residential</td>
<td>Consumer Program</td>
<td>Director of Residential Services</td>
</tr>
<tr>
<td>Clinical Services</td>
<td>Health &amp; Well Being of Consumers and Staff</td>
<td>Director of Clinical Services</td>
</tr>
<tr>
<td>JDCCF</td>
<td>Provide School* Access</td>
<td>JDCCF Staff, Director of JDCCF</td>
</tr>
</tbody>
</table>

* No location designated at this time
APPENDIX A-3
Emergency Personnel Policies

PURPOSE:
PERSON RESPONSIBLE: Primary: Director of Human Resources
                Secondary: Assistant Director of Human Resources

The board should approve policies for employees which, at a minimum, answer the following questions:

1. May employees work flexible or reduced hours?
   YES-As per Agency Policy, "A flexible schedule may be implemented in certain circumstances when program needs require". The flexible schedule(s) will be determined by the Department Head and approved by the Executive Director.

2. How will employees be classified – essential/non-essential?
   YES-Employees with job titles that directly affect the care of the Consumer will be considered "Essential" and will be directed by their supervisor to the designated work location within the Agency. Employees with job titles that indirectly affect the care of the Consumer will be considered "Non-essential" and will be directed by their Department Head on what action to take.

3. Will The Arc pay employees overtime during response?
   YES-As per Agency Policy, "Overtime will be paid to non-exempt employees for hours worked in excess of their normally scheduled work week in excess of 40 hours".

4. Are employees paid during evacuation/displacement? For how long?
   During Displacement, the Agency will compensate employees based on Agency Policy, Employee FLSA classification and DOL laws;
   Exempt Employees:
   Bad-weather days, and other occasions when work is unavailable to salaried exempt employees who are otherwise available for work will receive their regular weekly pay, provided that they worked some portion of that pay week. If the employee misses an entire week for such displacement/Evacuation, the salary may be reduced by that amount. In that case, the exempt employee will be required to use PTO days to cover evacuation/displacement.
   Non-Exempt Employees:
   Bad-weather days, and other occasions when work is unavailable to a non-salaried, non-exempt employees who are otherwise available for work will received pay for the time actually worked in the designated work location. If there is no designated work location to go to, then the non-exempt employee will be required to use PTO days to cover evacuation/displacement.

5. Should The Arc consider business interruption insurance?
   YES-The Arc currently maintains business interruption insurance.

6. Once The Arc office is reopened, do evacuated employees get charged vacation/personal leave?
   YES-Please see response to question #4.

7. How long do employees have to return to work before termination?
   If an employee cannot return to work due to Evacuation/Displacement on the part of the Agency, they will be considered employed with The Arc until which time they are given clearance to return to work by the Agency.
   If the employee refuses to work due to Evacuation/Displacement on the part of the Agency, Agency Policy states that "3 consecutive days of No-call, No show constitutes voluntary termination".
APPENDIX A-3
Emergency Personnel Policies

8. Eligibility of employees for unemployment insurance?
   YES-If an employee cannot return to work due to Evacuation/Displacement, they will be
   eligible to file for State unemployment compensation immediately.

9. What are the options on coverage for The Arc’s benefit plans? Will The Arc continue to pay for
   evacuated employees who have not returned to work and for how long?
   If an employee cannot return to work due to Evacuation/Displacement on the part of the
   Agency, as per Agency Policy, the Agency will cover the employer portion of the benefit
   premium for a period of 6 weeks. After that time, if the employee has not returned to work,
   the employee benefit will terminate and the employee will be issued COBRA information.

10. Should The Arc consider developing a specialized leave policy for disasters or emergencies
    where the community is effected but not the operation of The Arc?
    Employees will use PTO.

11. What resources should The Arc consider for the support of the employees in an emergency or
    disaster?
    - One call system—will allow Agency to send out emergency bulletins via computer/phone.
    - Local Office of Emergency Management to identify emergency locations to employees in
      their area
    - Notification—A detailed explanation of what The Arc will do in the case of an Emergency.
    - Emergency Phone numbers—Supervisors, employees.
APPENDIX A-4
Vital Records

PURPOSE:
PERSON RESPONSIBLE: Primary: (See each section heading for responsible party)
Secondary: Designee

Vital records are essential for an Arc office or program location to conduct business. They contain
information critical to the continued operation and survival of the organization immediately following a
disaster.

This information is necessary to recreate the organization’s legal and financial status and to preserve the
rights and obligations of stakeholders, including employees, donors, grantees and others being served.
Records may be required to be in their original form to meet or fulfill evidential requirements.

Here is a suggested list of some of the corporate, financial, and other vital records. These documents
will be obtained via electronic scan and are stored (depending on the document) on the server (with back
up) or in the “cloud”.

Corporate Records: Executive Director
  o Incorporation documents
  o By-laws
  o Tax-exemption documents (e.g. application for tax exemption, IRS Form 1023; IRS
determination letter; and related documents)
  o Board meeting documents including agendas, minutes, and related documents
  o Conflict of Interest and Nondisclosure statements/Code of Ethical Conduct
  o Correspondence with legal counsel and/or accountants not otherwise listed

• Financial documents, including: - Finance
  o Annual information returns going back seven years (e.g. IRS Form 990, 990-EZ, or 1065)
  o Audit and management letters
  o Audit work papers
  o Equipment files and maintenance agreements
  o Treasurer’s annual reports going back three years
  o Bank statements, canceled checks, check registers, investment statements and related
documents going back seven years
  o Line of credit agreement
  o Mortgage and other property information
  o Investment performance reports
  o Investment manager contracts and correspondence

• Donor and Fund Records - Development
  o Fund files including fund agreements and fund statements
  o Gift documentation
  o Grant documentation

• State charitable registration documents - Development/Foundation
• Lease Agreements - Finance
• Deeds, mortgages, notes, security agreements for real estate held for sale - Finance
• Personnel and payroll records including employment applications and employee Handbook – HR
• Insurance forms with policy numbers - Finance
• Signed contracts with vendors - Finance
• Scholarship records (depending on type of organization) - Finance
• Commercial software licenses, including: Information Technology
  o Copies of installation CDs
  o Product keys
  o Serial numbers
  o End User License Agreements
APPENDIX A-4
Vital Records

- National Standards materials, if applicable (This may include many vital records as well as publications and other items The Arc may not consider a vital record.)
APPENDIX B-1
Administration Coordination Checklist

PURPOSE:
PERSON RESPONSIBLE: Primary: Incident Commander
                                Secondary: Designee

Read completely through checklist before taking action

Ensure The Arc’s offices are returned to normal operations as quickly as possible.

1. Assess disaster site immediately.
2. Communicate with landlord (if renting) as soon as possible to determine status and access.
3. Identify key issues affecting facility.
4. Contact vendors for assessment and repairs as necessary.
5. Place and recovery/restoration vendors on notice.
6. Provide oversight and monitoring of response and operation activities.
7. Coordinate and manage restoration vendors to restore site.
8. Contact Health Department for guidance on health risks (i.e. mold, contamination)

Assist in the development of an alternate site as necessary.

1. Order catering and other logistical support for the EOC as necessary.
2. Oversee vendors involved in response and recovery operations.
3. Arrange for delivery of mail, UPS and FedEx to active Arc sites.
4. If a long-term outage is suspected, immediately assess damage to region regarding space issues.
5. Determine space and technology requirements.
6. Search for appropriate leased space as necessary.

Assist staff with any aspect of travel including transportation and lodging.

1. If activated at Hot Site, ensure those working have what they need to conduct business.
2. Review needs for lodging and transportation with team at the EOC.
3. Review needs for lodging and transportation for team if activated as Hot Site.
4. Contact appropriate vendors to arrange for transportation (shuttle, buses, vans, cars, air, train, etc.) lodging, etc.
APPENDIX B-1
Administration Coordination Checklist

PURPOSE:
PERSON RESPONSIBLE:  Primary: Incident Commander
                     Secondary: Designee

Read completely through checklist before taking action

Ensure The Arc’s offices are returned to normal operations as quickly as possible.

1. Assess disaster site immediately.
2. Communicate with landlord (if renting) as soon as possible to determine status and access.
3. Identify key issues affecting facility.
4. Contact vendors for assessment and repairs as necessary.
5. Place and recovery/restoration vendors on notice.
6. Provide oversight and monitoring of response and operation activities.
7. Coordinate and manage restoration vendors to restore site.
8. Contact Health Department for guidance on health risks (i.e. mold, contamination)

Assist in the development of an alternate site as necessary.

1. Order catering and other logistical support for the EOC as necessary.
2. Oversee vendors involved in response and recovery operations.
3. Arrange for delivery of mail, UPS and FedEx to active Arc sites.
4. If a long-term outage is suspected, immediately assess damage to region regarding space
   issues.
5. Determine space and technology requirements.
6. Search for appropriate leased space as necessary.

Assist staff with any aspect of travel including transportation and lodging.

1. If activated at Hot Site, ensure those working have what they need to conduct business.
2. Review needs for lodging and transportation with team at the EOC.
3. Review needs for lodging and transportation for team if activated as Hot Site.
4. Contact appropriate vendors to arrange for transportation (shuttle, buses, vans, cars, air, train,
   etc.) lodging, etc.
APPENDIX B-2
Finance Coordination Checklist

PURPOSE:
PERSON RESPONSIBLE:  Primary: Director of Finance
                        Secondary: Assistant Director of Finance-Operations

Read completely through checklist before taking action

Maintain daily cash funding of all essential business processes.
1. Ensure adequate funds are available to meet operating and recovery needs.
2. Project additional cash needs in relation to expected claims reimbursements.

Prepare and maintain cumulative income and expense report for the event.
1. For community events, coordinate with Incident Commander and communications department to
   construct public reports for use with external constituents and media.
2. For Arc oriented disasters, develop financial reports that are easy to understand for use by staff
   and board members.
3. Prepare and maintain an expense report for the Incident Commander. Report should include
   cumulative analyses and total expenditure for the event.
4. Organize and prepare records for audit.

Ensure easy access to necessary capital.
1. Monitor liquidity of assets based on projected expenses during the recovery.
2. Work with Finance and/or Investment committee to determine allocation of resources during
   recovery.

Coordinate all new vendor contracts.
1. Verify cost data in the pre-established vendor contracts and/or agreements.
2. Prepare and sign contracts as needed. Obtain Incident Commander concurrence as necessary.
3. Ensure that all contracts identify the scope of work and specific site locations.
4. Negotiate rental rates not already established or purchase price with vendors.
5. Finalize all agreements and contracts as required.

Coordinate with Incident Commander on all expenses exceeding pre-established limits.
1. Establish and maintain documentation of all purchasing activities.
2. Keep the Incident Commander informed of all significant issues involving the finance function.

Establish and manage disaster funds and general ledger accounts.
1. Establish and maintain all necessary documentation for recovery process.
2. Track costs for use of equipment owned and leased.
3. Process and track emergency grants.

Notify insurers and third party administrators as needed.
1. Prepare required documentation (insurance carriers and government agencies) as necessary to
   recover all allowable disaster response and recovery costs.
2. Provide information regarding insurance coverage as necessary.

Oversee the investigation of injuries and property and equipment damage claims arising out of
the event.
1. Track the total inventory of equipment, supplies and other items that have been lost, impacted or
   damaged.
2. Maintain a chronological log of property damage reported during the event.
3. Coordinate the investigation of all damage claims as soon as possible.
APPENDIX B-2
Finance Coordination Checklist

Coordinate paperwork required by insurers to initiate claims process.
   1. Coordinate the preparation of appropriate forms for damage claims and forward them to the insurers within the required time frame.

Collect and maintain documentation on all disaster information for reimbursement from private insurance carriers, FEMA, SBA, and other agencies.

Coordinate all fiscal recovery with disaster assistance agencies.
   1. Act as the liaison between the Arc and the disaster assistance agencies to coordinate the cost recovery process.

After the Event
Ensure that insurers and third party administrators honor contracts and pay claims; update reports on insurance recoveries until claims are closed.
APPENDIX B-3
First Person On Site Checklist

PURPOSE:
PERSON RESPONSIBLE: Primary
Secondary:

NOTE: This checklist is to be used by the first person that assumes initial control of the situation. That person is called the Incident Commander (IC) until the designated IC per the IRT arrives and is up to speed.

Immediate Response
Go to scene if appropriate and safe to do so.

Initial Assessment
Assess facts as known.
- Continuing danger? Take action to protect anyone in danger. Assess situation and initiate further evacuation if necessary.
- Emergency Response Services (Police, Fire, Medical, Hazardous Materials, ATF, FBI, County Office of Emergency Management)
- Has 9-1-1 been called?

Communication
Assess what has been done and what hasn’t. Determine where help is needed.
- Who needs to be notified?
- Has Senior Management been notified? Other key personnel? Division of Developmental Disabilities.
- Have key business unit managers been notified? Have they activated their department phone trees?
- Do I need assistance with communication? If so, who do I need help from and what do I need them to do?
  - Develop messages and updates
  - Deliver/coordinate delivery
  - Deal with the press
- Will the Emergency Hotline be activated for this incident? Has it been done? Who is handling the recording and updates?
- Has the Board been notified? If so, who has done the notification? Who will provide the updates?
- Parent Reach notification system

Building and Systems Assessment
Conduct the initial damage assessment – (Facilities and Building Management).
- What is the status of utilities (water, electricity, gas)?
- What is the status of the phone system?
- What is the status of the IT system?
- Is the building habitable now? Short-term outage? Longer-term outage?
- Do key vendors need to be contacted immediately (general contractor, other vendors)?
- Does the damage require a restoration vendor (water, fire, or smoke damage)?

Security / Facility Control
- Does the incident area need to be secured?
- Does the Arc need to hire its own security?
  - If so, how many security staff do we need? Where?
  - If so, what entrances and exits need to be secured?
APPENDIX B-3
First Person On Site Checklist

☐ Who can be put in place until additional security arrives?
☐ Can staff enter the area to begin clean-up or are authorities still in control of the area?

Escalation

☐ How could this situation escalate in severity?
☐ What preparation is needed in case it does escalate? Are any controls needed?
☐ Does the Arc need any assistance from the Board, the City or other nonprofits? If so, who does it need help from and what help is needed?

Employee Concerns

☐ Do families of victims need to be notified? Who will do the notification? When and how will it be done?
☐ Is there a need for professional crisis intervention, group debriefings, etc?
  ☐ If so, notify Employee Assistance Program (EAP) Provider.
  (Princeton Health Care - 1-800-527-0035)
☐ Do Arc personnel need any other support? Do their families?
☐ What are the main concerns of staff and employees? How are rumors being addressed and managed?
☐ Is the Emergency Hotline number updated at least every four hours?
APPENDIX B-4
Functional Area Checklist

PURPOSE:
PERSON RESPONSIBLE: Primary: Assistant Director of Finance – Operations
Secondary: Director of Finance

Administration — In Executive Administrative Assistant’s workspace, an emergency office supply box will be maintained. The box includes the following:

1. Stationery and envelopes – One box of each
2. Three reams of paper
3. Twenty file folders and five file pockets
4. Three boxes of pens and pencils
5. Two staplers with staples
6. One roll of first class stamps
7. One box of paperclips – both sizes
8. Sticky notes
9. Specialized stationery – acknowledgement, grant letters, etc.

Executive Administrative Assistant will take the office supply box with them when exiting the building and will receive instructions from the Incident Commander at the designated assembly area.

Finance — The following items should be readied during an evacuation, as time permits, by the finance staff: Unprocessed gifts and checks

1. A box of check stock-Operating Account, HUD 1, HUD 2, ACHO, Foundation
2. A box of deposit slips and stamp
3. Insurance documentation
4. Last month’s bank statements
5. Foundation Investment account information
6. Policy and procedure manual

Information Technology — See Appendix for details, also see IT disaster recovery plan
APPENDIX B-5
Human Resources Coordination Checklist

PURPOSE:
PERSON RESPONSIBLE:  Primary: Director of Human Resources
                      Secondary: Assistant Director of Human Resources

Read completely through checklist before taking action

Account for personnel at the assembly area in the event of an evacuation and account for personnel after an after-hours disaster.

Be responsible for the “human” aspects of the disaster including post-event counseling, next of kin notification; answer questions related to compensation, benefits and travel policy.
   1. Determine what “human” issues need attention.
   2. Determine whether the psychological needs of affected staff are being addressed.
   3. Recommend other activities that may be needed (memorial services, etc.) to the Incident Commander.
   4. Assist in creating updates to the Emergency Hotline.
   5. Partner with communications in creating employee communications.
   6. Determine what psychological support is necessary.
   7. Coordinate Critical Incident Stress Debriefing (CISD) sessions as needed.
   8. Provide immediate assessments before employees leave the location if needed.
   9. Offer support to employees and significant others.
  10. Keep the Incident Commander informed of significant issues affecting human resources and payroll.

Provide current roster of personnel and emergency contact information for next of kin notification.
   1. Ascertain what the immediate and on-going plans are to communicate with Arc personnel and their families.
   2. Provide emergency contact notification information to managers of affected employees.

Track, record and report all on-duty time for personnel who are working during the event.
   1. Establish and maintain documentation of all payroll activities.
   2. Ensure records are accurate and complete. All EOC staff must be keeping time sheets (exempt or not) as their time may be reimbursable by insurance.
   3. Provide instructions to all employees to ensure time sheets and travel expense claims are completed properly.

Ensure that time records, travel expense claims, and other related information are prepared and submitted to payroll.
   Assess payroll cycle and implications of the date of incident.

Maintain a file of injuries and illnesses associated with the event that includes results of investigations.
   1. Notify state OSHA of any fatalities or serious injuries on the job.
   2. Maintain a chronological log of injuries and illnesses reported during the event.
   3. Coordinate the investigation of all injury claims as soon as possible.
   4. Coordinate the preparation of appropriate forms for all verifiable injury and damage claims, and forward them to insurers within reasonable time frames.
   5. Answer insurance coverage questions as needed.
APPENDIX B-5
Human Resources Coordination Checklist

Notify insurers and third party administrators as needed.
1. Place service providers on alert.

After the Event
Refer or make available counseling services for employees and their families.
Provide necessary recovery time (time-off) for staff assisting with recovery efforts.
APPENDIX B-6
Incident Commander (IC) Checklist

PURPOSE:
PERSON RESPONSIBLE: Primary: Associate Executive Director
Secondary: Executive Director

Read completely through checklist before taking action

Declare disaster to activate plan and Hot Site.
1. Respond immediately and review situation.
2. Review the appropriate level of activation based on the situation as known. Determine the probable length of business interruption.
3. Determine the Level of business impact, (i.e., High, Medium or Low Level)
4. Obtain the most current briefing from whatever sources are available.
5. Activate plan at the appropriate level.
6. Activate the computer “Hot Site” if necessary.

Manage the overall emergency response.
1. Ensure that the Emergency Operations Center (EOC) is properly set up and is ready for operations.
2. Hold action plan meeting within the first hour of activating:
   o Determine the initial objectives (to focus the EOC and the recovery effort).
   o Define the operational period (how long till the next briefing and review of the objectives).
   o Review staff levels to resolve any major shortfalls.
   o Establish strategic objectives.
   o Estimate duration of the incident.
3. Determine priorities for response, allocation of resources, and procurement.
4. Review the potential of this event to become a sustained operation (extending over 24+ hours)? If so, ramp up logistical support immediately; ensure sufficient staffing for the next 36+ hours (spread staff out).
5. Brief Board on status.
6. Ensure that activity logs are being kept that include who, what, where, when, and how (including costs) for all actions taken and/or requested.

Establish appropriate staffing for the recovery and monitor effectiveness.
1. Mobilize appropriate personnel for the initial activation.
2. Assign all the recovery checklists to any affected department leadership.
   o First Person On-Site Who Is In Charge Checklist
   o Incident Commander (IC) Checklist
   o Finance Checklist
   o Administration Checklist
   o IT and Telecommunications Checklist
   o Human Resources Checklist
   o Public Relations & Communications Checklist
   o Program Checklist
3. Pace yourself and monitor stress levels in the EOC and the team members. Exercise overall responsibility for coordination between Emergency Operations Center (EOC) and program managers in the field.

Act as The Arc “public face” to the community.
1. Review all external communications for accuracy.
APPENDIX B-7
Pre-Evacuation Checklist

PURPOSE:
PERSON RESPONSIBLE: Primary: Incident Commander and Designees
Secondary: Designee

This checklist covers some basic planning information to consider before any evacuation as well as information if an evacuation is imminent.

Basic Planning Information
1. Make a video or take photographs of the building and its contents annually and store offsite.
2. Provide instructions for shutting off water and gas lines coming into Arc offices. Assign an employee to take care of this procedure in the case of a known evacuation.

48 hours until evacuation
1. Go shopping – One gallon of water per day and food for all essential employees and volunteers for at least three days.
2. Go shopping – Other response supplies identified
3. Remind board, employees and volunteers of communication plan, check-in times/locations and method of communication
4. Have employees and board members complete evacuation contact information if different than normal contact information
5. Remind employees of disaster plan
6. Communicate with vendors, donors, grantees, etc. concerning information in plan
7. Gather vital records according to plan
8. Begin working on IT recovery portion of the plan
9. Start Incident Commander checklist

24 hours until evacuation
1. Gather evacuation boxes – see IT section of plan as well as Evacuation Checklist by functional area
2. Record new voicemail message, as stated in Telecommunications Instructions.
3. If appropriate, raise electronics off the floor and away from windows
4. File all papers and lock cabinets
5. Withdrow petty cash
6. Pack up equipment to be evacuated
7. Lock all windows, close every interior door, post contact information in waterproof cover conspicuously (in case emergency crews need to contact you) and lock office as normal

2 hours until evacuation
1. Gather evacuation boxes – see IT section of plan as well as Evacuation Checklist by functional area
2. Record new voicemail message, as stated in Telecommunications Instructions.
3. If appropriate, raise electronics off the floor and away from windows
4. File all papers and lock cabinets
5. Lock all windows, close every interior door, post contact information in waterproof cover conspicuously (in case emergency crews need to contact you) and lock office as normal.
APPENDIX B-8
Program Coordination Checklist

PURPOSE:
PERSON RESPONSIBLE:  Primary: Incident Commander
                      Secondary: Designee

Read completely through checklist before taking action

Supervise The Arc community response.
1. Begin second-tier assessments of community needs. Work with identified nonprofits (intermediaries) to determine support levels.
2. Detail staff to key community outposts to monitor and assess ongoing needs. Feed that information to Development and Public Affairs.

Review community communications.
1. Work with Development and Communications to inform donors and community about areas of critical needs based on key grantees' reports.

Approve grants and loans to nonprofits in the affected areas.
1. Check on Department staff. Work with CEO/Executive Director and key grantees on specific needs, and consult with program officers.
2. Have Finance and Grants Management begin working on moving grants to key grantees.
4. Work with Finance and Grants Management to process grant payments to intermediaries.

Liaison with other Arcs and appropriate city and county offices.
1. Contact Program Departments to ascertain status and needs after disaster. Report back to Executive Director and appropriate relief agencies if individuals have special needs.
2. Feed information on needs to Development and Public Affairs obtained from nonprofits.
3. Collaborate with other area funders and/or recovery agencies (e.g., Red Cross, United Way, Salvation Army, NGO's, other Arcs, City Offices of Emergency Services, etc.)
APPENDIX B-9
Public Relations & Communications Coordination Checklist

PURPOSE:
PERSON RESPONSIBLE: Primary: Director of Development
Secondary: Assistant Director of Development

Read completely through checklist before taking action

Be responsible for notifying personnel and pertinent stakeholders of plan activation.

Methods of communicating may include:
1. Employee/board call/e-mail tree.
2. Phone forwarding.
3. Employee hotline (1-800 or local number.)
5. Web site as information center.
6. Media contacts (See Appendix C.)

Be responsible for developing the media messages regarding any event.
1. Prepare initial communication materials for all pertinent stakeholders (obtain approval from the Incident Commander or Executive Director to distribute).

Be responsible for all stakeholder communications including the Board, employees, donors, grantees, suppliers/vendors, and media.
1. Prepare update for the employee emergency hotline.
2. Update web site
3. Prepare all communications for stakeholders.
4. Develop talking points for executives.
5. Record and update messages on the Emergency Hotline.
6. Maintain website with current disaster updates.
7. Gather information on the emergency situation and response actions and maintain status boards and maps.

Serve as the primary media contact.
1. Establish contacts with the media and The Arc of New Jersey.
2. Monitor television and radio reports.
3. Release "media only" telephone numbers and public number if appropriate.
4. Open media center if a number of reporters arrive in person. Maintain Media Center status boards and maps. Post hard copy of news releases.
5. Arrange media briefings/press conferences on a regular or "as needed" basis.
6. Receive and handle non-emergency media calls

Provide rumor control.

After the Event
Record "non-emergency message on the employee hotline
Gather all records kept during the emergency or disaster. Prepare a summary of events, actions taken, inquiries and responses. Collect media coverage (include TV videotapes as well as clippings)
APPENDIX B-10
IT & Telecom Coordination Checklist

PURPOSE:
PERSON RESPONSIBLE: Primary: Director of Information Technology
Secondary: Consultant

Read completely through checklist before taking action

This checklist makes the assumption that a Hot Site or alternative site has been selected as the recovery solution.

Recovery of the computer and telephone technology (hardware and software).

Activation Phase: Task List

- Place Primary Recovery Site (See Appendix A-2) and IT Personnel (See Appendix C-3) on notice of a potential disaster declaration.

Operational Phase: Task List

- Contact Jill Court to declare a disaster and reserve the space and equipment. If space is unavailable, have equipment shipped to alternate recovery location or enlist the mobile recovery unit.

- Contact Director of IT, Jill Court and dispatch disaster recovery kit (includes backup media and specific systems recovery procedures) to the recovery location.

- Go to the recovery location.

- Set up workspace and stage equipment for recovery of systems.

For server and server data recovery See IT Recovery Procedures Manual

- Recovery of desktops: Rebuild a desktop and use Ghost disk imaging to replicate the installation to other desktops.

- Setup shared, network printers.

- Setup additional phones for staff.
APPENDIX C-1
Communications Information

PURPOSE:
PERSON RESPONSIBLE: Primary: Director of Development
                           Secondary: Assistant Director of Development

Communication via Arc Emergency Hotline

Consider setting up a telephone calling tree, a password-protected page on the Arc website, an email alert or a call-in voice recording to communicate with personnel and or Board in an emergency or disaster.

Designate an out-of-town phone number where employees can leave an "I'm Okay" message in a catastrophic disaster.

The Emergency Hotline is available to provide Arc personnel with facility status information and business continuity plans during an emergency or disaster.

Text Message (SMS)

☐ Text messages can be sent to almost any wireless phone in the U.S. by addressing messages to the 10-digit wireless telephone number. The Arc should ensure each employee who has a cell phone, knows how to send and receive text messages.
☐ Numerous free SMS message sites can be located on the Web by doing a Google Search for "send text message".

Email

The ability to contact others via email will depend on the availability of power and the operation of the servers. If a recipient has different Internet Service Provider email addresses, use all of them. Those located off site may have the best chance of reaching the team member in a regional emergency or disaster.

Arc Phone Tree

A wallet card can provide Arc personnel with instructions on how to get information in an emergency situation, what numbers to call in-area for information, and what numbers to call out of area to report in and give an "I'm OK" message. A Phone Tree should show "who calls whom."

Communication via Arc Website

In the event of a widespread phone failure, a message with disaster updates will be placed on the Arc website.

Messages should be updated frequently during the business week.

Emergency Hotline – How to Change the Message

NOTE: The procedure outlined below may vary with the Arc's phone system. Use this as a template only.

Before you change the message:
• Listen to the existing message to be sure no one else has changed it.

To change the message:
• Dial ___________ , then press #.
• Press ___ to check messages
• Press ___ to hear more options
• Press ___ to change name and/or greeting

• When emergency messages are updated, always include the time and date of the update.
  For example: "You have reached the _________ Arc Emergency Hotline. This is the Monday, August 13, 4 p.m. update regarding the flooding."

The Arc of Somerset County – Disaster Recovery Administration Manual
Document Name: ARC DR - appendix C-1 Communications Information - Updated 1/5/2010
APPENDIX C-1
Communications Information

After you record the initial message:

- Send a broadcast email to all staff reminding them to check the Emergency Hotline for future updates.

Updates – Event in Progress
The Emergency Hotline message should be updated at a minimum every four (4) hours during business day even if there is no new information to report. This will ensure the message stays current and provide callers with the assurance that the information they receive is up-to-date.

Once the situation is resolved, change recording to report the time and date it was resolved.
Leave that message on for 24 hours.

Updates – Event is Over
Once the emergency or disaster is over, change the message to the “non-emergency message”.
(See next section for sample messages.)

Sample Messages

Non-Emergency Message
"You have reached The _______________ Arc Emergency Hotline. There are no emergencies to report at this time. If there were an emergency, this hotline would provide you with information regarding the affected site. After any major event, please call this number for instructions. If you are unable to reach this number, follow your department’s disaster plan. Thank you for calling The _______________ Arc Emergency Hotline."

Sample Message after an Emergency
"You have reached The _______________ Arc Emergency Hotline. Today is (today’s day, date and time). The Arc office is closed due to a building emergency. [You may or may not want to state the nature of the emergency.] The building is expected to reopen at (note time and date). This message will be updated, as new information becomes available. Thank you for calling the _______________ Emergency Hotline."

Call Forwarding the Main Phone Number
NOTE: The procedure outlined below may vary with the Arc’s phone system. Use this as a template only.

The main number has a (fill this space in with length of time the battery will last) UPS power supply. If power is not restored within that time frame, ..... (Name) ..... will call-forward the number to an alternate number.

This will be the new main number.

Voice mail  □WILL  □WILL NOT  transfer.

Forwarding main phone number on-site:
- Lift receiver
- Press ___________ #
- You will hear another dial tone
- Dial ___________
- If call is answered, call forwarding is working, if busy or no answer repeat steps

Forwarding main phone number remotely:
- Dial ___________, then dial prompts
- Enter ___________, then press # key
- Enter PIN ___________, then press # key
- Enter ___________, then press # key
APPENDIX C-1

Communications Information

- You will hear dial tone
- Dial __________.

Cancel call forwarding:
- Lift receiver for dial tone
- Press __________.#

Analog / Emergency Phone Locations
Following an emergency or disaster, analog phones (direct dial phone lines) may work even if the Arc phone switch has failed. An analog phone is located in the administration evacuation box. See Appendix F-1.

Nearby Pay Phones
Pay phones are part of the national emergency phone system and always get dial tone first. The following pay phones are located near the Arc offices.
<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Work Phone (M)</th>
<th>Email</th>
<th>Phone</th>
<th>E-mail</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amy Konowski</td>
<td>Director</td>
<td>N/A</td>
<td>419-906-8110</td>
<td>N/A</td>
<td>908-443-9167 (C)</td>
<td>Somerset NJ 08873 199 Front Street, #326</td>
</tr>
<tr>
<td>Anthony Pasek</td>
<td>Vice President</td>
<td>N/A</td>
<td>202-245-0513 (C)</td>
<td>N/A</td>
<td>908-220-8879 (C)</td>
<td>Somerset NJ 08873 79 Center Street, #326</td>
</tr>
<tr>
<td>Donna Pasek</td>
<td>President</td>
<td>N/A</td>
<td>202-245-0513 (C)</td>
<td>N/A</td>
<td>908-220-8879 (C)</td>
<td>Donny Pasek, IL 60036 77 Center Street, #326</td>
</tr>
<tr>
<td>Michael Stearn</td>
<td>President</td>
<td>N/A</td>
<td>732-377-9808</td>
<td>N/A</td>
<td>973-301-7600 (M)</td>
<td>Martinsville NJ 08826 77 Van Nest Dr</td>
</tr>
<tr>
<td>Yarin Patel</td>
<td>Director</td>
<td>N/A</td>
<td>257-996-6117</td>
<td>N/A</td>
<td>267-996-6117</td>
<td>Hilltop, IL 60880 808 18th Ave, Unit 211, Hilltop School</td>
</tr>
<tr>
<td>Josephine Cruz</td>
<td>Director</td>
<td>N/A</td>
<td>908-392-6379</td>
<td>N/A</td>
<td>908-392-6379</td>
<td>Somerville NJ 08873 250 Wood Drive 101, Somerville School</td>
</tr>
<tr>
<td>Erika Deisinger</td>
<td>Executive Director</td>
<td>N/A</td>
<td>732-713-2776</td>
<td>N/A</td>
<td>732-713-2776</td>
<td>Hilltop NJ 08844 81 Chicago Circle 301, Hilltop School</td>
</tr>
<tr>
<td>Kamikami</td>
<td>Executive Director</td>
<td>N/A</td>
<td>703-850-2179</td>
<td>N/A</td>
<td>703-850-2179</td>
<td>Clifton NJ 07012 10 Alexander Way 92, Clifton School</td>
</tr>
</tbody>
</table>

**Business Resumption and Emergency Contact List**

**Appendix C-2**
<table>
<thead>
<tr>
<th>Program</th>
<th>Alternate Location #1</th>
<th>Alternate Location #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respite</td>
<td>Ardsley</td>
<td>JCATC</td>
</tr>
<tr>
<td>748 Route 206 South</td>
<td>1 Ardsley Road</td>
<td>3 Jill Court, Bldg 15</td>
</tr>
<tr>
<td>Hillsborough, NJ 08844</td>
<td>Hillsborough, NJ 08844</td>
<td>Hillsborough , NJ 08844</td>
</tr>
<tr>
<td>Ardsley</td>
<td>Respite</td>
<td>JCATC</td>
</tr>
<tr>
<td>1 Ardsley Road</td>
<td>748 Rt. 206 South</td>
<td>3 Jill Court, Bldg 15</td>
</tr>
<tr>
<td>Hillsborough, NJ 08844</td>
<td>Hillsborough, NJ 08844</td>
<td>Hillsborough , NJ 08844</td>
</tr>
<tr>
<td>Rocky Hill</td>
<td>Ardsley</td>
<td>Respite</td>
</tr>
<tr>
<td>7 Young Drive</td>
<td>1 Ardsley Road</td>
<td>748 Route 206 South</td>
</tr>
<tr>
<td>Rocky Hill, NJ 08553</td>
<td>Hillsborough, NJ 08844</td>
<td>Hillsborough, NJ 08844</td>
</tr>
<tr>
<td>Warren</td>
<td>Old Stirling</td>
<td>Camp (when outfitted)</td>
</tr>
<tr>
<td>503 Warrenville Road</td>
<td>57 Old Stirling Road</td>
<td>51 Old Stirling Road</td>
</tr>
<tr>
<td>Mobus</td>
<td>OSGH</td>
<td>Camp (when outfitted)</td>
</tr>
<tr>
<td>305 Mobus Avenue</td>
<td>57 Old Stirling Road</td>
<td>51 Old Stirling Road</td>
</tr>
<tr>
<td>North Plainfield, NJ 07062</td>
<td>Warren NJ 07059</td>
<td>Warren, NJ 07059</td>
</tr>
<tr>
<td>OSGH</td>
<td>Shelter In Place</td>
<td>Camp (when outfitted)</td>
</tr>
<tr>
<td>57 Old Stirling Road</td>
<td>57 Old Stirling Road</td>
<td>51 Old Stirling Road</td>
</tr>
<tr>
<td>Steinmetz</td>
<td>Respite</td>
<td>JCATC</td>
</tr>
<tr>
<td>118 Steinmetz Road</td>
<td>748 Route 206 South</td>
<td>3 Jill Court, Bldg 15</td>
</tr>
<tr>
<td>Hillsborough, NJ 08844</td>
<td>Hillsborough, NJ 08844</td>
<td>Hillsborough , NJ 08844</td>
</tr>
<tr>
<td>SLP</td>
<td>Respite</td>
<td>Personal Arrangements</td>
</tr>
<tr>
<td>Various locations</td>
<td>748 Route 206 South</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hillsborough, NJ 08844</td>
<td></td>
</tr>
<tr>
<td>Commons</td>
<td>UA</td>
<td>Respite</td>
</tr>
<tr>
<td>18 4th Avenue</td>
<td>436 Union Avenue</td>
<td>748 Route 206 South</td>
</tr>
<tr>
<td>Bridgewater, NJ 08807</td>
<td>Bridgewater, NJ 08807</td>
<td>Hillsborough, NJ 08844</td>
</tr>
<tr>
<td>UA</td>
<td>Commons</td>
<td>Respite</td>
</tr>
<tr>
<td>436 Union Avenue</td>
<td>18 4th Avenue</td>
<td>748 Route 206 South</td>
</tr>
<tr>
<td>Bridgewater, NJ 08807</td>
<td>Bridgewater, NJ 08807</td>
<td>Hillsborough, NJ 08844</td>
</tr>
<tr>
<td>Franklin</td>
<td>Claremont</td>
<td>JCATC</td>
</tr>
<tr>
<td>37 Buffa Drive</td>
<td>75 Claremont Road</td>
<td>3 Jill Court, Bldg 15</td>
</tr>
<tr>
<td>Somerset, NJ 08873</td>
<td>Franklin Park, NJ 08823</td>
<td>Hillsborough , NJ 08844</td>
</tr>
<tr>
<td>Claremont</td>
<td>37 Buffa Drive</td>
<td></td>
</tr>
<tr>
<td>75 Claremont Road</td>
<td>Somerset, NJ 08873</td>
<td></td>
</tr>
<tr>
<td>Franklin Park, NJ 08823</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cedar Grove</td>
<td>Respite</td>
<td>JCATC</td>
</tr>
<tr>
<td>19 Cedar Grove Road</td>
<td>748 Route 206 South</td>
<td>3 Jill Court, Bldg 15</td>
</tr>
<tr>
<td>Branchburg, NJ 08876</td>
<td>Hillsborough, NJ 08844</td>
<td>Hillsborough , NJ 08844</td>
</tr>
<tr>
<td>Griggstown</td>
<td>Claremont</td>
<td>Franklin</td>
</tr>
<tr>
<td>7 Honeyman Street</td>
<td>75 Claremont Road</td>
<td>37 Buffa Drive</td>
</tr>
<tr>
<td>Griggstown, NJ 08540</td>
<td>Franklin Park, NJ 08823</td>
<td>Somerset, NJ 08873</td>
</tr>
<tr>
<td>Steven’s Lane</td>
<td>OSGH</td>
<td>Warren</td>
</tr>
<tr>
<td>39 Stevens Lane</td>
<td>57 Old Stirling Road</td>
<td>503 Warrenville Road</td>
</tr>
<tr>
<td>Martinsville, NJ 08836</td>
<td>Warren, NJ 07059</td>
<td>Warren, NJ 07059</td>
</tr>
<tr>
<td>Lindsley Road</td>
<td>UA</td>
<td>Respite</td>
</tr>
<tr>
<td>2711 Lindsley Road</td>
<td>436 Union Avenue</td>
<td>748 Route 206 South</td>
</tr>
<tr>
<td>Bridgewater, NJ 08807</td>
<td>Bridgewater, NJ 08807</td>
<td>Hillsborough, NJ 08844</td>
</tr>
</tbody>
</table>
Disaster Plans

- Create “addendums” for specific disasters
  - Terrorism
  - Floods
  - Active shooter
  - Pandemic
Pandemic Response Plan

An Example

Corona Virus Response Plan
The Arc of Somerset County

Coronavirus Response Plan

Introduction:

This interim response plan is based on what is currently known about the coronavirus disease 2019 (COVID-19) as of 3/9/2020. The Arc of Somerset County will update this interim guidance as needed and as additional information becomes available.

CDC is working across the Department of Health and Human Services and across the U.S. government in the public health response to COVID-19. Much is unknown about how the virus that causes COVID-19 spreads. Current knowledge is largely based on what is known about similar coronaviruses. This plan is based on the CDC most recent data and suggested guidelines.

Corona Virus Definition:

Coronaviruses are a large family of viruses that are common in humans and many different species of animals, including camels, cattle, cats, and bats. Rarely, animal coronaviruses can infect people and then spread between people, such as with MERS-CoV and SARS-CoV. The virus that causes COVID-19 is spreading from person-to-person in China and some limited person-to-person transmission has been reported in countries outside China, including the United States. However, respiratory illnesses like seasonal influenza, are currently widespread in many US communities.

The following interim response plan will be used to help prevent workplace exposures (both employees and program participants) to acute respiratory illnesses, including COVID-19, in non-healthcare settings. The guidance also provides planning considerations if there are more widespread, community outbreaks of COVID-19.

To prevent stigma and discrimination in the workplace, use only the guidance described below to determine risk of COVID-19. The Arc does not make determinations of risk based on race or country of origin, and be sure to maintain confidentiality of people with confirmed COVID-19. There is much more to learn about the transmissibility, severity, and other features of COVID-19 and investigations are ongoing. Updates are available on CDC’s web page at www.cdc.gov/coronavirus/covid19

Coronavirus Response Plan

1
Current strategies for The Arc of Somerset County:

- **We will actively encourage sick employees to stay home:**
  - Employees who have symptoms of acute respiratory illness are recommended to stay home and not come to work until they are free of fever (100.4°F [37.8°C] or greater using an oral thermometer), signs of a fever, and any other symptoms for at least 24 hours, without the use of fever-reducing or other symptom-altering medicines (e.g. cough suppressants). Employees should notify their supervisor and Human Resources and stay home if they are sick.
  - Our sick leave policies are will be flexible and consistent with public health guidance and we will communicate to ensure employees are aware of these policies. We will NOT require employees to find their own coverage if home sick with a fever.
  - Temp agencies that provide the Arc with contract or temporary employees will be contacted to reinforce the need for their employees to stay home if sick.
  - We will request a healthcare provider’s note for employees who are sick with acute respiratory illness to validate their illness or to return to work. It is understood however, that healthcare provider offices and medical facilities may be extremely busy and not able to provide such documentation in a timely way.
  - The Arc will maintain flexible policies that permit employees to stay home to care for a sick family member. Employers should be aware that more employees may need to stay at home to care for sick children or other sick family members than is usual.

- **Separate sick employees:**
  - CDC recommends that employees who appear to have acute respiratory illness symptoms (i.e. cough, shortness of breath) upon arrival to work or become sick during the day should be separated from other employees and be sent home immediately. Sick employees will be instructed to cover their noses and mouths with a tissue when coughing or sneezing (or an elbow or shoulder if no tissue is available). They will also be instructed to wash their hands frequently.

- **Emphasize staying home when sick, respiratory etiquette and hand hygiene by all employees:**
  - Posters that encourage staying home when sick, cough and sneeze etiquette, and hand hygiene at the entrance to your workplace and in other workplace areas where they are likely to be seen have been posted in each program location.
  - The Arc will provide tissues and no-touch disposal receptacles for use by employees. As well as hand sanitizer and ample amounts of soap. Employees will be instructed to wash their hands for 20 seconds, often.
  - Hand sanitizer is located in multiple locations in the facilities and in conference rooms to encourage hand hygiene.
  - Visit the coughing and sneezing etiquette and clean hands webpage for more information.

- **Perform routine environmental cleaning:**
  - Employees will be reminded to routinely clean all frequently touched surfaces in the workplace, and program locations; such as workstations, countertops, and doorknobs using the cleaning agents (disinfectant wipes, etc) that have been provided.
  - No additional disinfection beyond routine cleaning is recommended at this time.
  - The Arc will provide disposable wipes so that commonly used surfaces (for example, doorknobs, keyboards, remote controls, desks) can be wiped down by employees before each use.
Cleaning contractor will be reminded to train all of their employees on the best practices when disinfecting agency work space and bathrooms.

- **Advise employees before traveling to take certain steps:**
  - Employees with be provided with the [CDC’s Traveler’s Health Notices](https://www.cdc.gov/travel/) for the latest guidance and recommendations for each country to which someone will travel. Specific travel information for travelers going to and returning from China, and information for aircrew, can be found at on the [CDC website](https://www.cdc.gov).
  - When known to us, we will advise employees to check themselves for symptoms of [acute respiratory illness](https://www.cdc.gov) before starting travel and notify their supervisor and stay home if they are sick.
  - Employees who become sick while traveling understand that they should notify their supervisor and the Human Resources department and should promptly call a healthcare provider for advice if needed.
- If outside the United States, sick employees should follow obtain medical care or contact a healthcare provider or overseas medical assistance company to assist them with finding an appropriate healthcare provider in that country. The Human Resources department should be notified so that they can work with our Health benefits provider. A U.S. consular officer can help locate healthcare services.

- **Additional Measures in Response to Currently Occurring Sporadic Importations of the COVID-19:**
  - Employees who are well but who have a sick family member at home with COVID-19 should notify their supervisor and the Human Resources Department and refer to CDC guidance for [how to conduct a risk assessment](https://www.cdc.gov) of their potential exposure.
  - If an employee is confirmed to have COVID-19, employers should inform fellow employees of their possible exposure to COVID-19 in the workplace but maintain confidentiality as required by the Americans with Disabilities Act (ADA). Employees exposed to a co-worker with confirmed COVID-19 should refer to CDC guidance for [how to conduct a risk assessment](https://www.cdc.gov) of their potential exposure. For program staff, guardians of individuals served will also be provided with information about the possible exposure to their loved one. All information related to individuals and their health status is considered confidential and must be protected under HIPPA regulations. No HIPPA information is to be shared.

**Planning for a Possible COVID-19 Outbreak in the US**

The severity of illness or how many people will fall ill from COVID-19 is unknown at this time. If there is evidence of a COVID-19 outbreak in the U.S., The Arc will plan to be able to respond in a flexible way to varying levels of severity and be prepared to refine their business response plans as needed. For the general American public, such as workers in non-healthcare settings and where it is unlikely that work tasks create an increased risk of exposures to COVID-19, the immediate health risk from COVID-19 is considered low. The CDC and its partners will continue to monitor national and international data on the severity of illness caused by COVID-19.
19, will disseminate the results of these ongoing surveillance assessments, and will make additional recommendations as needed.

**Planning Considerations**

**Communication:** The Executive Director and /or The Associate Executive Director will be the ONLY staff members to communicate with employees and program participants regarding the COVID-19 Virus. These communications will be frequent and based on information received from either the Department of Health and/or the CDC. Communications will include:

(a) reducing transmission among staff,
(b) protecting people who are at higher risk for adverse health complications (including program participants)
(c) maintaining business operations,
(d) minimizing adverse effects on other entities in their supply chains.

Some of the key considerations when making decisions on appropriate responses are:

- Disease severity (i.e., number of people who are sick, hospitalization and death rates) in the community where The Arc is located;
- Impact of disease on employees/program participants that are vulnerable and may be at higher risk for COVID-19 adverse health complications. Inform employees that some people may be at higher risk for severe illness, such as older adults and those with chronic medical conditions.
- Prepare for possible increased numbers of employee absences due to illness in employees and their family members, dismissals of early childhood programs and K-12 schools due to high levels of absenteeism or illness:
  - The Arc will monitor and respond to absenteeism at the workplace. Essential employees will be identified as those who can maintain the core/essential functions of the department.
  - Director level staff will Cross-train department staff personnel to perform essential functions so that the workplace is able to operate even if key staff members are absent.
  - Essential functions and the reliance on vendors and others and the community will be assessed. Alternative suppliers will be pursued.

- Program Directors (Residential and Employment) will provide Asst. Directors and managers with the authority to take appropriate actions outlined in their business infectious disease outbreak response plan based on the condition in each locality.
- Coordination with Somerset County Department of Health and Office of Emergency Management has been established. In addition, The Arc is a fixed facility medication distribution location- in the event that mass distribution of medications is required for program participants and employees.
**Important Considerations for Creating an Infectious Disease Outbreak Response Plan**

All employers should be ready to implement strategies to protect their workforce from COVID-19 while ensuring continuity of operations. During a COVID-19 outbreak, all sick employees should stay home and away from the workplace, respiratory etiquette and hand hygiene should be encouraged, and routine cleaning of commonly touched surfaces should be performed regularly.

**The Arc will:**

- Ensure the response plan is flexible and involve your employees in developing and reviewing your plan.
- Conduct a focused discussion (with all Director level staff) or exercise using your plan, to find out ahead of time whether the plan has gaps or problems that need to be corrected.
- Share our plan with employees and explain what human resources policies, workplace and leave flexibilities, and pay and benefits will be available to them.
- Share best practices with other businesses in your communities (especially those in your supply chain), chambers of commerce/business partnerships, and associations to improve community response efforts.

**Infectious Disease Outbreak Response Plan:**

- For program participants and employees who have increased risk are those who have underlying respiratory issues and/or compromised health; In the event of an outbreak, these individuals will be separated from others. Employees will be asked to self quarantine, Program participants will be isolated in their bedrooms unless other guidance from health practitioners is provided. If needed our “Alternate Locations” and “Shelter in Place” policies will be activated to separate individuals who are symptomatic, from those who are not.
- Employees who work in a home with symptomatic individuals will be quarantined along with the individuals; unless transported to the hospital.
- Human resources policies will be reviewed to ensure policies and practices are consistent with public health recommendations and are consistent with existing state and federal workplace laws. Non Exempt will be paid for hours worked and/or PTO can be used, if there is a need to be absent from work.
- Policies and practices, such as flexible worksites (e.g., telecommuting), conference calling and flexible work hours (e.g., staggered shifts), to increase the physical distance among employees and between employees and others will be observed - if state and local health authorities recommend the use of social distancing strategies.
- For employees who are able to telework, supervisors will be encouraged to have employees to telework instead of coming into the workplace until symptoms are completely resolved. Information Technology Department will assist to ensure that the information technology and infrastructure needed to support multiple employees who may be able to work from home.
- Identify essential business functions include:
  - Finance, managing cash and reserves in the event that there is a financial need
  - Billing - to ensure ongoing financial resources
  - Purchasing – to ensure adequate supplies and food for programs
o Maintenance – only priority projects will be completed (those projects that must be completed to ensure the health, safety and welfare of individuals served and employees)

o Programs – If needed, Employment programs will close and employment staff will be reassigned to support group homes

o Technology – ongoing monitoring to ensure infrastructure intact

o Human Resources – will monitor the health of employees and provide guidance on sick/leave policies

- Our Disaster plan will be set into motion as per that plan. Sheltering in place and alternate location schedule policies will be activated as needed. The Executive Staff will trigger this response. Executive Staff will maintain contact with local health officials to identify these triggers.

- As directed by The Executive Director, the Foundation Director will communicate information to business partners on our infectious disease outbreak response plans and latest COVID-19 information. We will anticipate employee fear, anxiety, rumors, and misinformation, and plan communications accordingly. Our Employee Assistance Program will be readily available to our employees.

- In the event that local, early childhood programs and K-12 schools are dismissed, particularly if COVID-19 worsens. The Jerry Davis Center will also close their program. Center Employees will be encouraged to stay home, until the center resumes operations.

- Local conditions will influence the decisions that public health officials make regarding community-level strategies; The Arc will take the time now to learn about plans in place in each community where they have a business.

- If there is evidence of a COVID-19 outbreak in the US and or in NJ, The Arc will cancel all business travel to additional countries per travel guidance on the CDC website.
  - Travel restrictions may be enacted by other countries which may limit the ability of employees to return home if they become sick while on travel status.

Screening and Protection:

- As per agency policy, employees must be physically able to perform their job functions and must be free of communicable diseases.

- If there is evidence of a COVID-19 outbreak in the Somerset County or adjacent Counties, The Arc will screen employees prior to entering the work site and at the end of their work shift. This will include at a minimum, taking each employees temperature and screening for coughing and shortness of breath. Each screening will be recorded and maintained in the Human Resources department. Any Employee with any of the (3) symptoms screened will be asked to go home immediately and contact their health provider. Any individual served that displays any of the (3) symptoms, will be quarantined in their bedroom while further instruction from their health care providers and The Somerset County Department of Health and The Somerset Office of Emergency Management are contacted for guidance.

- For employees working with quarantined individuals, The Arc will provide personal protective equipment (PPE) along with instructions on how to use/wear the PPE.

- To reduce exposure to the COVID-19 virus, new admissions to Arc programs will be suspended.

If the there is evidence of an outbreak in the immediate area (Somerset and the adjacent Counties), group events, gatherings and meetings will be reassessed and possibly cancelled.
This plan and related policies will be updated as new information is gathered. Updates to this plan will be highlighted to ensure changes are easily identified.

Plan date: 3-9-2020

Revision dates: ______________
Business/Financial Planning

• Consider Four Key areas
  • Loss/reduction of revenue
  • Potential/real increase in expenses
  • All sources of revenue/ reduction of expenses
  • Other considerations
Consider:

- Loss/reduction of billing (FFS or other)
- Loss/reduction of Tuition
- Loss/reduction of program income due to suspension/closure
Reduction/Loss of Revenue (2 of 2)

• Consider:
  • Loss of fundraising due to cancellation of events or donor hardship
  • Loss of grant funding due to lower LOS/service provision
  • Calculate the RANGE of loss from best case scenario to worst case scenario
<table>
<thead>
<tr>
<th>Revenue Source</th>
<th>Impact Weekly</th>
<th>Status</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medicaid – loss of billing</td>
<td>65K</td>
<td></td>
<td>State provides some gap funding</td>
</tr>
<tr>
<td>Day Care/ PS Tuition – loss from program closure</td>
<td>14K</td>
<td>Off set by staff furlough</td>
<td></td>
</tr>
<tr>
<td>EI Reimbursement – reduction due to movement to tele-health</td>
<td>25K</td>
<td>Therapist costs match reimbursement – break even program</td>
<td></td>
</tr>
<tr>
<td>Camp Tuition – loss due to suspension of program</td>
<td>13K</td>
<td>Off set by staff furlough</td>
<td></td>
</tr>
<tr>
<td>College Tuition – loss due to reduction of class size/ virtual learning</td>
<td>8K</td>
<td>Offer additional courses</td>
<td></td>
</tr>
<tr>
<td>Fundraising – in person events changed to virtual</td>
<td>Reduce fundraising goal by 30%</td>
<td>Ask previous attendees to crowd fund</td>
<td></td>
</tr>
</tbody>
</table>
Potential Increase in Expenses

1 of 3

• Consider:
  • Increased over time costs for remaining programs
  • Increased cost of employee incentives
  • Cost of additional supplies
  • Cost related to cleaning/ preparing facilities (shelters)
Potential Increase in Expenses (2 of 3)

Consider:

- Fixed costs of facilities that may not be utilized
- Increased insurance premiums/bank fees
- Increased cost of technology for work at home/virtual programs
- Calculate the RANGE of increase expenses from best case scenario to worst case scenario
<table>
<thead>
<tr>
<th>Expense item</th>
<th>Amount of impact weekly</th>
<th>Progress/status</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Over time costs for staff remaining in programs</td>
<td>42K</td>
<td></td>
<td>Some gap funding from state, PPP, other grants</td>
</tr>
<tr>
<td>Additional supplies needed (PPE, etc)</td>
<td>5K</td>
<td></td>
<td>Donations/fundraising</td>
</tr>
<tr>
<td>Professional cleaning/sanitizing</td>
<td>3K per program</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee incentive/Bonus</td>
<td>$120.00 per week per employee</td>
<td></td>
<td>Limited to 12 weeks</td>
</tr>
<tr>
<td>Additional IT needed for work from home/ZOOM</td>
<td>$20K one-time costs</td>
<td></td>
<td>IT grants?</td>
</tr>
</tbody>
</table>
Sources of Revenue to Consider (1 of 3)

• Agency operating and agency reserves (do you have three months of operating?)

• Other reserves? (maintenance/IT, etc.)

• Bank balances

• Line of credit
Sources of Revenue to Consider (2 of 3)

- Foundation / investment accounts
- Fund raising / Crowd funding
- Calculate all potential revenue sources and how they will offset the loss of revenue/ increase in expenses
<table>
<thead>
<tr>
<th>Revenue Source</th>
<th>Amount available</th>
<th>Status/progress</th>
<th>Notes/priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency operating</td>
<td>1 month operating</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agency Reserves</td>
<td>2 weeks operating</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other reserves (Maintenance/IT)</td>
<td>200K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Foundation/ Investment account</td>
<td>2 weeks operating</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bank balances</td>
<td>2 weeks operating</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line of Credit</td>
<td>1.5 M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fund Raising/ crowd funding</td>
<td>15K for Covid-19 appeal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Private Foundations</td>
<td>various</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grants – FEMA, CARES, PPP, etc.</td>
<td>1.8 M for PPP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• Delay payables (without harming the business relationship)

• Furlough non-essential employees (use of PTO time to reduce the liability on your books)

• Reduction of non-essential employees

• Staffing exodus

• Insurance costs (reduce/spread out payments)
Other Consideration (2 of 3)

- Insurance programs (offering discounts; suspension of premium?)
- Reach out to grantor to ask for extension of grant period
- Advocacy with local/state legislators
- Disaster funding or specialized grants
<table>
<thead>
<tr>
<th>Proposed initiative</th>
<th>Amount</th>
<th>Progress/Status</th>
<th>Notes</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay payables</td>
<td></td>
<td></td>
<td>Harm to the business relationship?</td>
<td></td>
</tr>
<tr>
<td>Furlough non-essential employees</td>
<td></td>
<td></td>
<td>Cross train other employees</td>
<td></td>
</tr>
<tr>
<td>Reduction of hours</td>
<td></td>
<td></td>
<td>With preservation benefits</td>
<td></td>
</tr>
<tr>
<td>Property sales/eliminate lazy assets</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>County/CDBG grant preservation</td>
<td></td>
<td></td>
<td>Alternate methods to meet grant goals?</td>
<td></td>
</tr>
<tr>
<td>Advocacy</td>
<td></td>
<td></td>
<td>Local and state</td>
<td></td>
</tr>
<tr>
<td>Insurance</td>
<td></td>
<td></td>
<td>Suspension/reduction of premiums</td>
<td></td>
</tr>
<tr>
<td>Increase “cost of care”</td>
<td></td>
<td></td>
<td>As cost rises – contribution rises</td>
<td></td>
</tr>
</tbody>
</table>
✓ Add risk management/mitigation to your annual strategic planning process

✓ Create an annual routine regarding risk assessment

✓ Cultivate and Steward all donors/volunteers

✓ Establish working relationships with local and State OEM, FEMA, Red Cross and other First Responders
Important Steps to Remember (2 of 2)

✓ Create a global disaster plan
✓ Add specific addendums for various scenarios
✓ Create a Financial /business plan for disasters
✓ Share – test – revise the plan annually
Conclusion

• Planning should be an ongoing activity

• The financial impact of a disaster can be challenging

• The financial impact of poor or no planning prior to a disaster can be catastrophic

• Be safe, be well and plan to protect your organizations future!
Contact Information

• Lauren Frary, MA, LRC, CSW

• Phone: 908-725-8544 X604

• Email: LaurenF@thearcofsomerset.org
Other Supporting Documents
# INDEX

## IT Operations Disaster Recover Overview

### Section A – Disaster Preparedness

- Virtualizing Servers: A-1
- Section Removed: A-2

### Section B – Recovery of Servers and Restoration of Data

- Installing VMware Workstation: B-1
- Installing Backup Exec: B-2
- Section Removed: B-3
- Section Removed: B-4
- Recovering FINANCE2 Server: B-5A
- Restoring FINANCE2 Data: B-5B
- Recovering MAN-EXCH: B-7A
- Restoring MAN-EXCH Data: B-7B
- Recovering MAN-SVR: B-8A
- Restoring MAN-SVR Data: B-8B
- Changing Public DNS: B-10

### Section C – Common Procedures

- Installing VMware Tools: C-1
- Installing the DAT Tape Drive and Driver: C-2A
- Installing the Tandberg SCSI Tape Driver: C-2B
- How to Inventory and Catalog a Tape in Backup Exec.: C-3

### Section D – Special Procedures

- Resolving Trust Relationship Error: D-1
- Backup Exec Tape Drive not found: D-2
- Installing Backup Exec Agents: D-3
- Media not found error: D-4

### Section E – Post Recovery Procedures

### Section F - Hardware Requirements

- Recovery Server Requirements
- Tape Backup Requirements

### Section G - Site information

### Section H - Supporting Documentation
Preparation before the fact is the first step in successful disaster recovery. Advance planning is particularly important in making the IT recovery process easier and faster. This thinking has been taken into consideration when determining what gets backed up, where it gets backed up to, as well as where the media is stored.

Every computer system the agency operates that stores user data is backed up regularly. The backup media for each of these systems is relocated to an off-site storage area where there is a high probability that the media will survive in the event a disaster strikes. The offsite location currently being used:

Jill Court

All media is stored in a secure fireproof cabinet.

Data Backup

The Data being backed up consists of databases, emails and user files.

Primary Data has been identified as the following:

- MIP, ADP, Abra & Donor Perfect databases
- Email
- Network files
- Shared documents

All data is backed up to disk and duplicated to tape, with the tapes being stored offsite. This process provides redundancy to the backups and provides the ability to recover data faster by not having to go offsite to retrieve a tape.

There are 5 remote locations with servers that have their data replicated daily to our Manville server over a secure VPN connection so their data can be backed up to tape.

*Backups are scheduled and tapes taken offsite according to the current Arc backup policy.*

Recovery

In the event of a disaster, the IT department has designed a recovery plan that will allow complete recovery of all critical servers and the data stored on those servers up to the point of the last backup available. The IT recovery plan is designed to use off the shelf hardware that is not vendor specific in order to reduce recovery time. This plan includes the use of the following hardware/software that has been purchased and is stored offsite with the backup tapes:

- External Tape drive that can read DAT backup tapes currently in use
- External Hard drives that are used to store server images of all critical servers
- Virtualization software that allows the server images to be restored and run

The recovery process is detailed in the IT Disaster Recovery Processes and Procedures manual.
Time to recovery
Once a disaster is declared, the amount of time it will take the first user to access recovered data will vary depending on many factors, most of which are beyond anyone’s control. Keeping this in mind the IT department will give their best effort to meet the following goals:

- Day 1 – Assess disaster, obtain and prepare all equipment required for recovery
- Day 2 – Recover primary servers and critical databases. User files, folders and Financial Data (MIP) should be accessible on Day 2. Email should be partially restored (Ability to send and receive new emails).
- Day 3 – Recover non primary servers and user files. User emails should be restored by day 3.
Section A - Preparing for a Disaster

This topic explains what is required to prepare for a successful disaster recovery. Preparing the servers to be used during a disaster requires minimal work. The designated servers are virtualized to a removable external hard drive and stored offsite with the backup tapes.

Pre-Requisites
These procedures should be performed anytime there are changes made to a designated servers operating, such as service packs or hot fixes being applied. They should also be performed anytime changes are made to the applications running on those servers, such as service packs, hot fixes or version upgrades.

See individual processes for specific requirements

Steps to prepare:

1. Virtualize Servers
2. Backup Virtual Server Images to tape for redundancy
3. Store External Drive and Tapes in offsite secure location

Documents included:
ARC DR – Section A-1 - Virtualizing a Server
ARC DR – Section A-2 - Backing up the DR images

Notes:
Servers should be virtualized Quarterly to ensure we have up to date images

NOTE: While all efforts have been made to ensure the accuracy of this manual, the pictures shown may be different than what is shown on the computer. Please do not rely on the pictures – ALWAYS read the text.
This topic explains how to Virtualize a server using VMware Converter. This process will take several hours and can be run during the day or overnight.

**Pre-Requisites**

VMware Converted Version 5 is installed on the server
External USB disk is connected and is accessible to the server
A network share with R/W access has been created on the external disk and is accessible from the server to be converted.

**Procedure**

1. Double click on the VMware Convert Icon to run the program.

2. Click Convert Machine

3. At the Source System type screen, select **Powered on machine**, select **A Remote Computer**, enter required information and click **Next**
Section A-1 - Virtualizing a Server using VMware converter version 5

4. If the agent has not been previously deployed, you will be prompted to uninstall the agent when finished. Select “I will manually uninstall the files later” and click Yes.

The Agent will deploy

If you have previously installed the agent, you may receive a Converter Security Warning. Click the “Do not display security warning” check box and click the Ignore button.
5. At the Destination System screen, change destination type to VMware Workstation, product to **Workstation 10.0.x**. Under Virtual machine details, the name will automatically populate. Enter the path to the network share where the files will be created, enter the user credentials and press the next button.

6. At the Options screen, Next to the Networks setting, click the Edit button, for ALL Nic’s select Host-only, then click the edit next to the Advanced item.
7. Click the Post-conversion tab, then check the Install Vmware Tools box and click next.

8. Review the summary page to make sure everything is correct and click the Finish button.
9. You can view the progress in converter. DO NOT close the window or the conversion will stop.

The conversion will be marked as Completed if it completes successfully.

<table>
<thead>
<tr>
<th>Destination</th>
<th>Status</th>
<th>Start</th>
</tr>
</thead>
<tbody>
<tr>
<td>\MAN-DC.thear...</td>
<td>Completed</td>
<td>10/16</td>
</tr>
</tbody>
</table>

Estimated times to Virtualize each server:

- MAN-DC – 1 Hour
- MAN-EXCH – 3 hours
- MAN-SVR – 2.5 hours
- FINANCE2 – 1 hour

Note that the conversion will impact system and network performance and key servers should be converted during hours when impact to users would be minimized.
Steps to Recovery of Servers and Restoration of Data

This topic explains what is required to recover servers and restore data.
Recovering the designated servers brings the server back online with data from the date the server was last 'virtualized'. Restoring data brings the user data back from the last available backup. The procedures are outline below and detailed in the listed documents.

Pre-Requisites
See individual procedures for specific requirements

Steps to Recovery of Servers:

1. Install VMware Workstation on the Recovery System
   a. See Document ARC DR – Section B-1 - Installing VMware Workstation

2. Install Backup Exec on the Host server

3. Recover server FINANCE2
   a. See Document ARC DR - Section B-5A - Recovering Finance2
      i. See section C-5 for Trust Relationship Errors
   b. See Document ARC DR - Section B-5B - Restoring Data - FINANCE2 Data
      i. Upon completion of this step, Financial data will be available

4. Recover server MAN-EXCH (Email)
   a. See Document ARC DR - Section B-7A - Recovering MAN-EXCH
      i. See section C-5 for Trust Relationship Errors
   b. See Document ARC DR - Section B-7B - Restoring MAN-EXCH Data
      i. Upon completion of this step, user emails will be available

5. Recover server MAN-SVR (User Files)
   a. See Document ARC DR - Section B-8A – Recovering MAN-SVR
      i. See section C-5 for Trust Relationship Errors
   b. See Document ARC DR - Section B-8B – Restoring MAN-SVR Data
      i. Upon completion of this step, user files will be available

6. Change the Public DNS (Restores inbound email)
   a. See Document ARC DR - Section B-10 - Changing Public DNS

NOTE: While all efforts have been made to ensure the accuracy of this manual, the pictures shown may be different than what is shown on the computer. Please do not rely on the pictures – ALWAYS read the text.
Section B-1 - Installing VMware Workstation Version 10

Have VMware Software?

Download VMware Workstation from Www.vmware.com

Install VMware Workstation on “Server”

See License and Password document for License Key

Complete
Section B-1 - Installing VMware Workstation Version 10

This topic explains how to install VMware Workstation on the Recovery Desktop.

The virtualized servers will all run on a single desktop. This requires installing VMware workstation.

It is recommended that you download the latest version from www.vmware.com

Pre-Requisites

A desktop that meets the hardware and software requirements
VMware Workstation Version 10 software
VMware Workstation license key

Procedure

1. On the desktop that is the recovery system, download the latest release of VMware workstation V10.x from http://www.vmware.com/download/ws/
Section B-1 - Installing VMware Workstation Version 10

2. Enter the **username** and **password** and click Login.

![](image)

3. This will bring you to a License Agreement page. Scroll to the bottom and Click Yes

4. Click on the appropriate link to download the program to the local disk.

5. After downloading, open the program by double clicking on it.

![](image)
Section B-1 - Installing VMware Workstation Version 10

6. At the Open File Security Warning, click RUN

7. At the Installation Wizard, click Next
8. At the Setup Type screen, select Typical and click Next

![Setup Type Screen](image1.jpg)

9. At the Destination Folder screen, accept the default and click Next

![Destination Folder Screen](image2.jpg)
Section B-1 - Installing VMware Workstation Version 10

Click Next at the next series of screens

![Image of VMware Workstation Setup window showing Software Updates and User Experience Improvement Program]

- **Software Updates**: When would you like to check for updates of your software?
  - Check for product updates on startup
    - When VMware Workstation starts, check for new versions of the application and installed software components.

- **User Experience Improvement Program**: Would you like to send feedback to VMware?
  - Help improve VMware Workstation
    - Send anonymous system data and usage statistics to VMware.
10. At the Configure Shortcuts screen, accept the default and click Next.

![Configure Shortcuts screen](image1)

11. At the Ready to Install the Program screen, click Install

![Ready to Perform the Requested Operations](image2)
VMware Workstation installs

12. At the Registration Information Screen, enter the appropriate information and click .

See License and Password document for License Key
13. At the **Installation Wizard Completed** screen, click **Finish**

![VMware Workstation Setup](image)

14. You will be prompted to reboot. Click **Yes**.

![VMware Workstation](image)

VMware Workstation is now ready to use
Section B-5 - Recovering the FINANCE2 server

External Hard Drive should already be connected

Copy FINANCE2 VM from External drive to local hard drive

Room for this VM on Disk?

YES

NO

Open FINANCE2 VM with VMware Workstation

Recover System has Second Disk?

YES

NO

Change allocated memory to 512mb
Change NIC to Bridged

Change allocated memory to 512mb
Change NIC to Bridged

Start Virtual Machine, Install VMware tools & Configure Video Acceleration

Configure Network Setting (IP Address)

Stop Services that are not required. Start Required Services.

Test Connectivity (Ping ARC-SVR3)

Restore Data from backup tapes

Process Complete

ARC of Somerset
IT Disaster Recovery Flowchart
Recovery steps for Manville NJ Main office
Rev 1 – August 28, 2008

Recovering FINANCE2

IP = 192.168.1.5
Mask = 255.255.255.0
Gateway = 192.168.1.1
DNS1 = 192.168.1.4
DNS2 = 192.168.1.3
Section B-5 - Recovering the FINANCE2 server

This topic explains how to prepare the FINANCE2 virtual server for use.

Before the FINANCE2 Virtualized server can be used, there are several steps that must be completed. This document details those steps. Note that while the following procedure has been tested, there may be occasions where undocumented dialog boxes may appear. Typically, you can cancel out of them to continue onto the next step.

Pre-Requisites

The ARC-SVR3 Virtual server MUST be running.

If Possible, copy the Virtual Machine folder with the files to the local hard drive. Note – If copying to a local disk, it MUST be NTFS format, NOT FAT32.

Procedure

1. Browse to the location of the Virtual Server files and Open the FINANCE2 Folder. Find the vmx file and Double Click on it. This will open the FINANCE2 Virtual Machine in VMware Workstation.
Section B-5 - Recovering the FINANCE2 server

2. In the FINANCE2 Device window, Double click on Memory.

3. In the Memory Dialog box, change the memory size to 512 MB and click OK.
4. In the FINANCE2 Device window, if **Ethernet** is NOT set to **Bridged**, Double click on it.

5. In the Ethernet Dialog box, select **Bridged** and click **OK**
Section B-5 - Recovering the FINANCE2 server

6. In the FINANCE2 Command windows, click on **Start this virtual machine**.
Section B-5 - Recovering the FINANCE2 server

7. Login as Administrator

8. At the Service Control Manager dialog box, click the OK button
9. If prompted with a Shutdown Event Tracker box, select **Power Failure: Environment** and click **OK**.

10. After logging in, windows will identify new devices. Wait for this to finish,
Section B-5 - Recovering the FINANCE2 server

11. When prompted to install drivers, click Cancel – We will install these shortly.

12. When prompted to restart - Select NO. Then Wait - The server WILL automatically reboot anyway.
13. After the server reboots, Login as Administrator.

14. Ignore the Display Settings – Click on the X

15. Install VMware Tools – See **Installing VMware Tools** document

16. After installing VMware tools, the server reboots. Once it’s back up, login as Administrator

17. On the desktop, find My Network Places, right click on it and select Properties.
Section B-5 - Recovering the FINANCE2 server

18. In the Network connections windows, right click on Local Area Connection 2 and select properties

19. In the Local Area Network Connection 2 Properties box, select Internet Protocol (TCP/IP) and click Properties.
20. In the Internet Protocol (TCP/IP) Properties screen, select **Use the Following IP address** and **Use the following DNS server addresses**. Enter the information provided and click the **OK** button.

![Internet Protocol (TCP/IP) Properties screen]

**FINANCE2 IP Information**
- **IPAddress**: 192.168.1.5
- **Subnet mask**: 255.255.255.0
- **Default Gateway**: 192.168.1.1
- **Preferred DNS**: 192.168.1.4
- **Alternate DNS**: 192.168.1.3

21. At the Microsoft TCP/IP Warning, click **NO**. NOTE: You MUST select NO!

![Microsoft TCP/IP Warning]

The IP address 192.168.1.5 you have entered for this network adapter is already assigned to another adapter 'Generic Marvell Yukon Chipset based Ethernet Controller'. 'Generic Marvell Yukon Chipset based Ethernet Controller' is hidden from the Network Connections folder because it is not physically in the computer. If the same address is assigned to both adapters and they both become active, only one of them will use this address. This may result in incorrect system configuration.

Do you want to enter a different IP address for this adapter in the list of IP addresses in the Advanced dialog box?
Section B-5 - Recovering the FINANCE2 server

22. In the Local Area Network Connection 2 Properties box, click **OK** (or **Close**) button.

![Local Area Network Connection 2 Properties window](image)

Restart the server (Be Patient – It take a while 5+ minutes)

The FINANCE2 Server is now up and running and ready to restore data from the backups.
Restoring FINANCE2 Data

Install Tape Driver

Tape Drive and Driver Installed?

Yes

Insert most recent backup tape.

Has tape been catalogued?

YES

Stop MIP and ADP Database Services

Select files from last NORMAL backup to be restored and Click Restore Data

Restore ALL Incremental backups

Process Complete
This topic explains how to restore the MIP and ADP data from the backups.

MIP and ADP data is stored in SQL Databases. Restoring is simple as stopping the SQL services and restoring the data. You must restore the latest NORMAL backup tape first and all subsequent INCREMENTAL tapes.

Pre-Requisites

Tape drive and tape driver MUST already be installed.
FINANCE2 Server must have been ‘recovered’ according to Server Recovery steps.

Procedure

1. Stop the MSSQL$MIP_Engine Service by right clicking on it and selecting STOP.
2. Stop the **Gupta SQLBase SQL9SVR** Service by right clicking on it and selecting **STOP**.

3. Run NTBACKUP by Clicking **Start**, click **Run**, type **NTBackup**, and then click **OK**.
4. Insert the latest FINANCE2 backup tape into the tape drive. NT Backup should find the tape. If prompted, Select **Allow Backup Utility to use the media** and click **OK**.

5. Click on the tape you inserted and select the last **NORMAL** backup.
6. Select C: and D:\SHARES to restore MIP data

7. Select D:\ADP and D:\SQLBASE to restore ADP data. After selecting what to restore click the Start Restore button.
8. At the **Confirm Restore** box, click the **OK** button.

9. The Restore starts. This should take less than 30 minutes.
10. When the restore is done, verify the status is completed and then click **OK**

11. Repeat steps 1 to 10 for all subsequent **INCREMENTAL** tapes

12. Exit **NTBACKUP**.

13. Start the **$MIP_Engine** and **SQLBase SQLB9SVR** Services.

ADP and MIP are now ready to use.
Section B-7A - Recovering MAN-EXCH

This topic explains how to restore and prepare the Virtual Server MAN-EXCH for use.

Before the MAN-EXCH server can be used, there are several steps that must be completed. This document details those steps. Note that while the following procedure has been tested, there may be occasions where undocumented dialog boxes may appear. Typically, you can cancel out of them or click next to continue onto the next step.

Pre-Requisites

VMware Workstation installed on recovery server, MAN-DC recovered and running.
If Possible, copy the Virtual Machine folder with the files to the Recovery Systems local hard drive. Note – If copying to a local disk, it MUST be NTFS format, NOT FAT32.

Procedure

Estimated time to completion – 45 minutes

1. Click on the Open a Virtual Machine link.

2. Browse to the location of the Virtual Server files, appropriate Vmware Configuration File (.vmx), highlight it and click open.
3. Under Devices, click on Memory

4. Change the memory to 2048, make sure the Network adapter is set to Bridged and press OK
5. Click the ‘Power on this Virtual Machine’ link.

6. On the first start up, you may receive notices about devices not being available. Click the NO button for each one you receive.
7. When the Log on page is displayed, press the CTRL + ALT + DELETE icon at the top left.

8. If you are prompted to log onto the local computer (man-exch instead of thearcofsomerset.org), click the Switch User button. Otherwise log in and skip to step 11.

9. Click Other User

10. Enter arc\administrator in the username box, the current password and click the Blue arrow.

Be patient – It can take more than 10 minutes to get logged in the first time.

11. If you are prompted to install Tools, click Remind Me Later.
Section B-7A - Recovering MAN-EXCH

12. After you login, the server will install VMware Tools and drivers. Do not do anything until this completes. To monitor the status, click the Devices icon in the task bar.

13. After drivers are installed the server will reboot. If prompted, click Restart Now.

Again, be patient, it can take 20+ minutes to get a log in prompt.

If you get “The trust relationship between this workstation and the primary domain failed”, go to D-1

Log back in as the administrator

14. Set the Static IP address. Right click on the Network icon at the bottom right and click on Open Network and Sharing center
Under the Internet click on Local Area Connection X

Click on Properties

Select Internet Protocol Version 4 (TCP/IPv4) and click Properties.
Set the IP address as per server requirements and click OK

Click the Close button twice and the IP address should be set

15. Make sure you can Ping the domain Controller. Open a CMD prompt and type ping jc-svr. You should get 4 responses.
16. Make sure Exchange Services have started. There will be 2 that will be stopped – this is normal.
Section B-7B – Restoring MAN-EXCH Data

This topic explains how to restore Data (Emails) on MAN-EXCH.

This procedure explains how to emails to the MAN-EXCH email server.

Pre-Requisites

- MAN-EXCH has been recovered and all exchange services are running.
- Symantec Backup Exec 2010 software has been installed and working properly.
- The Backup Exec Agent can communicate with the exchange server.
- Backup tapes to be used have been inventoried and cataloged.

This procedure requires disk space greater in size than the size of the Exchange databases. Be prepared to have at least 400GB of temporary space available, which can reside on an external USB disk is necessary.

Procedure

Clink on the Devices tab, select the tape drive, right click on the tape and select restore data.
Section B-7B – Restoring MAN-EXCH Data

On the Selections item, expand the date of the backup and select the files you want to restore.
Now select the Advanced option and under GRT, select the location of the temp files. This space needs to be greater than the size of the Exchange Information store databases and log files.

Now go to the Microsoft Exchange option and again set the location for the temp files. Then click Run Now.
Section B-7B – Restoring MAN-EXCH Data

The backup job properties widow is displayed, click OK.

You can monitor the status of the backup job in the Job Monitor. Right click on the job and select Properties.
The Job Activity window will display and you can monitor the status.

The job should display as Successful upon completion.
This topic explains how to prepare the Virtual Server MAN-SVR for use.

Before the MAN-SVR server can be used, there are several steps that must be completed. This document details those steps. Note that while the following procedure has been tested, there may be occasions where undocumented dialog boxes may appear. Typically, you can cancel out of them or click next to continue onto the next step.

Pre-Requisites

VMware Workstation installed on recovery server
MAN-DC Recovered and working
If Possible, copy the Virtual Machine folder with the files to the Recovery Systems local hard drive. Note – If copying to a local disk, it MUST be NTFS format, NOT FAT32.

Procedure

Estimated time to completion – 20 minutes

1. Click on the Open a Virtual Machine link.
2. Browse to the location of the Virtual Server files, appropriate Vmware Configuration File (.vmx), highlight it and click open.

3. Under Devices, click on Memory
4. Change the memory to 768, make sure the Network adapter is set to Bridged and press OK.

5. Click the ‘Power on this Virtual Machine’ link.
6. On the first start up, you may receive notices about devices not being available. Click the NO button for each one you receive.

7. The Virtual Machine will start.
8. When the Log on page is displayed, press the CTRL + ALT + DELETE icon at the top left.
Section B-8A – Recovering MAN-SVR (File & Print Server)

9. Click the Change User Icon.
10. Click the Other User icon
Section B-8A – Recovering MAN-SVR (File & Print Server)

Enter the Domain\username and password and press the Blue Arrow button
11. After you login, the server will install VMware Tools and drivers. Do not do anything until this completes. To monitor the status, click the Devices icon in the task bar.

12. After Drivers are installed, you will be prompted to restart.
13. After the server restarts, log in as Administrator, go to the task bar, click on the Network icon and click on the “Open Network and Sharing Center” link.

14. Find the Local Area Connection and click on it.

15. On the Status page, click on the Properties button.
16. On the Properties page, find the TCP/IPv4 item, click on it (DO NOT Uncheck it!) and click the Properties Button.

![Image of Properties page]

17. Select “Use the following IP Address” and enter the server’s IP address and the DNS Server information.

- IP = 192.168.1.6
- Mask = 255.255.255.0
- Gateway = 192.168.1.1
- Preferred DNS = 192.168.1.11
18. You will receive a message about the IP being assigned to another adapter. Click the Yes button.

MAN-SVR is now running and ready for data to be restored from backup tapes.

Please refer to document located in Section B-8B for detailed instructions.
Section B-8B - Restoring MAN-SVR Data - DRAFT

This topic explains how to restore the User data on MAN-SVR

In order to get the most recent user data back to the recovered server, you must restore the latest NORMAL backup tape and all subsequent INCREMENTAL tapes. This document explains how to restore that data.

Pre-Requisites

MAN-BACKUP Server must be restored and able to access the tape drive. MAN-SVR Must be restored and accessible from MAN-BACKUP (Able to Ping)

Procedure

Log onto MAN-BACKUP server and start Backup Exec. Insert the latest LTO-4 backup tape into the drive.

Inventory the device (Make sure the tape moves).

Catalog the tape (See BACKUP Exec – Catalog tape) – If the catalog fails, make sure the tape drive is connected – restart BE Services.

Select the last Full backup for MAN-SVR and the last Differential backup

Important Message from Backup Exec

Reminder: In order to fully back up or restore a remote computer, the appropriate Backup Exec Remote Agent must be installed and running.

Please refer to the documentation or online help for more information.

[Image of Backup Exec interface showing backup history and options]

[Image of Backup Exec interface showing restored data properties]
Section B-10 - Changing the Public DNS Records

This topic explains how to change the public DNS records. Public DNS records tell computers on the how to find your servers. The records that need to be changed will redirect email Email and Webmail to the new location. Because Network Solutions may change the web site without notice, these instructions and pictures might not be accurate.

Pre-Requisites
A computer with internet access
The username and password for the DNS site
DO NOT perform this procedure until the Microsoft Exchange Databases have been restored and Exchange is working

Procedure

1. Open internet explorer and Go to http://www.networksolutions.com/
2. Find the Login link and click on it.
3. At the Login screen, enter the User ID and Password and click the Log in button.

See License and Password document for Password
4. Find the **Account Manager** link and click on it.

5. **Under Domain Details**, find the section titled **Domain currently points to**, and click the **Edit** link.

6. **Go to Advance DNS Manager** and click on **Manage DNS Records**
Section B-10 - Changing the Public DNS Records

7. At the Domain Screen, Scroll down to the **Mail Servers** section and click the **Add/Edit** button.

8. Find the entry titled mail.thearcofsomerset.org and change to new location.

9. Scroll to the bottom of the page and click Save.

10. Confirm the change. Then logout.
Section C - Common Procedures

This topic explains common procedures.
Some procedures require common steps, such as installing software or drivers. These steps have been isolated and placed in separate documents to be used are required.

Pre-Requisites
See individual processes for specific requirements

Documents included in this section:

ARC DR - Section C-1 - Installing VMware Tools
ARC DR - Section C-2A - Installing the DAT Tape Drive and Driver
ARC DR - Section C-2B - Installing the LTO Tape Driver
ARC DR - Section C-3 – Inventory and Catalog a tape before restoring data

NOTE: While all efforts have been made to ensure the accuracy of this manual, the pictures shown may be different than what is shown on the computer. Please do not rely on the pictures – ALWAYS read the text.
Section C-1 - Install VMware Tools on virtual servers

This topic explains how to install VMware Tools on virtual servers

VMware tools should be installed on all virtual servers. This will allow better controls of the mouse and is a required to use the external tape drive.

Pre-Requisites

None

Procedure

1. In the VMware Workstation Menus, click the VM menu and select **Install VMWARE TOOLS**
2. At the Dialog box, click **Install**
3. In the VMware Tools dialog box, click **Next**
Section C-1 - Install VMware Tools on virtual servers

4. In the Setup Type screen, select **Typical** and click **Next**

5. In the Ready to Install the Program screen, click **Install**
Section C-1 - Install VMware Tools on virtual servers

6. At the VMware Tools Installation dialog box you will be prompted to enable hardware acceleration, click **Yes**

7. VMware will open Display Properties, Got to the **Settings** Tab and click **Advanced**
Section C-1 - Install VMware Tools on virtual servers

8. In the Advanced Properties screen, select the Troubleshoot tab and change Hardware Acceleration to Full. Click OK.

9. At the Installation Completed Screen, click Finish.

10. VMware prompts you to restart. Click Yes.
Section C-2A - Installing the DAT Tape Drive and Driver

This topic explains how to install the DAT Tape Drive and Driver.

Before you can use the external tape drive, you must download and install the tape driver.

Pre-Requisites

The tape driver downloaded onto the system where the tape driver will be used.

Procedure

1. Download the tape driver. The tape drive is a DAT 160 and can be downloaded from www.quantum.com. A copy is also located on the External ARC-DR Drive.
2. Extract the drivers – Note the path they were extracted to. You will need this information later.

3. AFTER the driver is downloaded and extracted, make sure the system (Virtual or Physical) is running and you are logged in, then plug in and power on the USB tape drive. The system will find the new device and launch the Hardware Wizard.

4. At the Found New hardware screen, Select **No, not this time** and click **Next**
Section C-2A - Installing the DAT Tape Drive and Driver

5. Select **Install from a list or Specific Location** and click **Next**

![Image of Found New Hardware Wizard]

6. Select **Include this location in the search** and click **Browse**

![Image of search options for found hardware]
7. In the **Browse For Folder** dialog box, browse to the location you extracted the drivers. Install the appropriate driver for the operating system the tape drive is connected to:
   a. Windows Server 2003 – Use the Windows 2003, i386 folder
   b. Windows XP – Use the Windows XP folder.

8. Click **Next**
9. At the Hardware Installation warning, click **Continue Anyway**

10. When it completes click **Finish**
This topic explains how to install the Tandberg SCSI tape driver.

Before you can use the external tape drive, you must download and install the tape driver.

Pre-Requisites

The tape driver downloaded onto the system and the tape drive connected to the SCSI controller.

Procedure

1. Download the tape driver. The tape drive is a Tandberg LTO-4 HH and can be downloaded from http://www.tandbergdata.com/us/. A copy is also located on the External ARC-DR Drive.

2. Extract the drivers – Note the path they were extracted to. You will need this information later.

3. Right click on My Computer and select Manage
4. Select Device Manager and in the Center pane, expand other devices, right click on the LTO-4 tape drive and select Update Driver Software

5. Select Browse my computer
6. Browse to the folder where the extracted driver files are located, select the appropriate driver and click Next.

7. At the Security Warning, click “Install this driver anyway”

8. After the driver installs, click Close

9. When prompted, restart the computer
Section C-3 – Inventory and Catalog a tape before restoring data

This topic explains how to Inventory and Catalog a tape before restoring data.

Backup tapes must be inventoried and the contents cataloged to the Backup Exec database before data can be restored. This procedure explains how to do both.

Pre-Requisites

Backup Exec can access the tape drive to be inventoried and cataloged.

DAT Tapes from FINANCE2 should take less than 5 minutes to catalog.

LTO Tapes take over 3 hours to Catalog the First tape and XX Hours for the 2nd tape.

**Before Cataloging an LTO Tape, ensure you have set the “Use storage media based catalogs” option in Backup Exec. See corresponding document to verify this setting.**

Procedure

Write Protect the Tape to be inventoried and put into the tape drive.

Open Backup Exec, go to Devices, right click on the tape drive and select Inventory

Click the Run Now Button. The tape drive will show as “In use” while it inventories the tape. This should only take a minute or two.

Now Right click on the tape drive and select Catalog

Click the Run Now button
Section C-3 – Inventory and Catalog a tape before restoring data

You can monitor the status of the Catalog job by going to Job Monitor

Upon completion it will show as Successful

You should now be able to restore data from that tape.
Section D – Special Procedures

This topic describes Special Procedures. Special Procedures are to be run ONLY if you are told to run them.

Pre-Requisites
All previous procedures have been performed.

Documents included in this section:

NOTE: While all efforts have been made to ensure the accuracy of this manual, the pictures shown may be different than what is shown on the computer. Please do not rely on the pictures – ALWAYS read the text.
Section D-1 – Resolving Trust Relationship Errors

Summary
When restoring older images of a sever image, you may receive a
“The trust relationship between this workstation and the primary domain failed” error message.

Before You Begin
You will need to know the servers local Administrator username and password. This will be listed in the Master Password list.
Section D-1 – Resolving Trust Relationship Errors

Procedure

Log onto the server getting the error message using the local administrator account and password.

For the username enter .\administrator and the local administrator password, then click the Blue arrow.

1. Right click on computer and select Properties.

2. Click on Advance System Settings
3. Select the Computer Name tab and click on the Change button.
4. Under Member of, change from ARC to WORKGROUP and click OK

5. You will be prompted about knowing the local administrator password – be sure you know it and click OK.
6. When prompted, enter the domain administrator name and password and click OK
Section D-1 – Resolving Trust Relationship Errors

7. Click OK and close the window and when prompted, reboot.
Section D-1 – Resolving Trust Relationship Errors

After the computer restarts, log in with the local administrators account

Now rejoin the domain. Repeat steps 1 to 3. When you get to step 4, select Domain and enter ARC

Repeat steps 5 to 7. After you reboot, you should be able to log onto the domain without any errors
Section D-2 – Backup Exec Tape Drives

Summary
When running Backup Exec the tape drive may be displayed as offline. Resolving this requires removing the existing drive and restarting the backup exec services. This will most likely happen when attempting to restore data on FINANCE2 server.

Procedure
Start Backup Exec

Put Existing Backup jobs on hold
Delete the existing tape drive
Section D-2 – Backup Exec Tape Drives

Restart the Backup Exec Services

![Backup Exec Services Manager](image)

![Stopping Backup Exec Services](image)
The tape drive should now be found
Section D-3 – Install the Backup Exec Agents on recovered servers

Summary
Before you can restore data to the recovered servers, the Backup Exec Agents on each server need to be connected to the ‘new’ backup exec server. This requires removing the existing drive and restarting the backup exec services. This procedure needs to be done to MAN-EXCH and MAN-SVR before data can be restored.

Procedure
Start Backup Exec. Go to File, Select New and click on backup Selection List.

Click Selections, right click on Windows Systems and select Add Windows System
Section D-3 – Install the Backup Exec Agents on recovered servers

Type the name of the server, click the pulldown under Logon Account and enter arc\administrator. Click OK.

Click the Yes button

Click the OK button

Repeat for all other servers that need data restored.
Section D-4 – Media not found error

Summary
After cataloging a tape you get a media not found error.

Procedure
In the Backup Exec Tools menu, select Options.
Select Catalog from the right side, uncheck the Use storage media based catalogs and click OK.

Re-catalog the tape and the problem should be fixed.
Section E - Post Recovery Steps

This topic Describes what needs to be done after everything is complete. After performing the recovery and restoration procedures, certain things will need to be done in order for things to runs normally.

Pre-Requisites
All previous procedures have been performed.

Additional Procedures

Install any required software on desktops.
- MIP Client
- ADP Client
- Abra Client

Install Printer drivers for printer types located at recovery site.

Disable scheduled backups on all recovered servers
- Failure to do this will result in a conflict between servers and the external tape.
- Failure to do this could result in needed backup tapes being overwritten.

NOTE: While all efforts have been made to ensure the accuracy of this manual, the pictures shown may be different than what is shown on the computer. Please do not rely on the pictures – ALWAYS read the text.
Section F-1 – Recovery Server Hardware Requirements

This topic explains the Hardware and Software requirements to recover the servers in case of a disaster.

In order for this disaster recovery plan to be implemented successfully, Hardware and Software must be obtained that meets or exceeds the minimum requirements. These requirements are listed and explained below.

Recovery Server

- Intel Quad Core Processor or Higher
- System MUST support VT Technology
- 8 GB System Memory or higher (16gb or more preferred)
- 1 Terabyte Hard drive or Higher – Prefer dual disks configured with Raid 1 for redundancy, however it is not required.
- Gigabit Network Card
- DVD/CD Drive
- LTO5 Tape Drive – SCSI or SATA with compatible interface card
- 64bit edition of a Windows Server 2008R2 with Service Pack 1
- VMware Workstation Version 8