

# America's Essential Hospitals

# Information Services & Technology

**CONTINGENCY PLAN**

## Purpose

The critical business processes of America’s Essential Hospitals (hereafter referred to as the Association) are heavily dependent upon its information technology resources. The Association recognizes the potential financial and operational losses and member impact from service interruptions and the importance of preparedness for disaster recovery operations.

The purpose of this Contingency Plan is to provide for business continuitywith a documented and detailed plan to ensure the successful continued operations and recovery of the network infrastructure and operations. This plan provides detailed procedures for handling a system outage in order to minimize any adverse impact on our ability to fulfill our mission. The following are the objectives of this plan:

* 1. Conduct and document a Business Impact Analysis (BIA) to identify the activities, resources, and procedures needed to carry out processing requirements during normal operations.
  2. Assign responsibilities to designated Association personnel and provide guidance for recovering the network during short-term periods of interruption to normal operations.
  3. Ensure coordination with other Association staff who will participate in the contingency planning strategies.

## Scope

This plan applies to the association network infrastructure, which is classified as a Low-Impact GSS based on FIPS 199 definitions (see the System Security Plan for more information).

## What to do In Case of an Emergency

* 1. Convene Contingency Plan Team, whose members include the Association leadership team, HR Director, and IT Director.
  2. Perform damage assessment and determine which Tier Action Plan to follow.
  3. Follow Contingency Plan Phase 1, 2, and 3 using specifics from the Tier Action Plan.

## Key Assumptions

* 1. Key Association personnel have been identified and will be trained regarding the activation of the Contingency Plan.
  2. Preventive controls, such as UPS devices, smoke detectors, fire extinguishers, and fire suppression systems will be fully operational at the time of an outage.
  3. The same incident that causes the outage has not affected those individuals responsible for executing the contingency plan.

## References/Requirements

* 1. Federal Information Security Management Act (FISMA) of 2002, Title III – Information Security.
  2. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.
  3. The current America’s Essential Hospitals System Security Plan.

## Data Center Location

The network information technology infrastructure resides in the corporate office, located in Washington DC. The office was constructed with building features that minimize the risk of fire and unauthorized entry. Protective measures include:

* 1. Office climate control for temperature and humidity control.
  2. Alarmed smoke and fire detection systems with fire suppression apparatus (sprinkler).
  3. Emergency exits with fire-resistive stairwells.
  4. Lobby 24 hour guard service.
  5. Servers are connected to Uninterruptible Power Supply (UPS).

## Emergency Relocation Options

In the event the Association must relocate all or part of its operations to an alternate facility, the following options will be considered by the Contingency Plan Team:

* 1. Other associations outside of the event area
  2. Holland and Knight
  3. Hotels we frequently use

## Business Impact Analysis (BIA)

|  |  |  |
| --- | --- | --- |
| **CRITICALITY CLASSIFICATION** | | |
| **Assessment** | | **Description** |
| **Rank** | **Classification** |
| 1 | Mission Critical | Can only be done by computers and must be restored between 1 hour and 30 work days. Key personal will be relocated to temporary space should this extend past 30 working days. |
| 2 | Critical | Can only be done by computers and must be restored between 1 hour and 30 work days. |
| 3 | Non-Critical | Can be delayed until damaged site is restored and/or a new computer system is purchased. |

|  |  |  |
| --- | --- | --- |
| **Critical Resource** | **Outage Impact** | **Recovery Priority** |
| Network | Mission Critical | 1 |
| Webinar Capability | Critical | 2 |
| Internet | Critical | 3 |
| Phones | Non-Critical | 4 |

## Contingency Plan Team

| **Role** | **Responsibility** | **Name** |
| --- | --- | --- |
| **System Owner (SO)** | The SO is responsible for ensuring that the IT Security Program, to include contingency planning, is appropriately developed and implemented within the Association. They work with the CPC and Facilities Manager to ensure facility availability and safety of employees. The SO also coordinates with leadership team. | Rhonda Gold  CFO  America’s Essential Hospitals  1301 Pennsylvania Avenue, NW, Suite 950  Washington, DC 20004  (202) 585-0109  [rgold@essentialhospitals.org](mailto:rgold@essentialhospitals.org) |
| **Backup System Owner** | The Backup System Owner is responsible for executing the System IT Contingency Plan in the event that the System Owner is unable to execute this plan. | Bruce Siegel  President and CEO  America’s Essential Hospitals  1301 Pennsylvania Avenue, NW, Suite 950  Washington, DC 20004  (202) 585-0115  [bsiegel@essentialhospitals.org](mailto:rgold@essentialhospitals.org) |
| **Contingency Planning Coordinator (CPC)** | The CPC works with the Facilities Manager in overseeing all contingency planning responsibilities. The System Owner will receive notification of all system outages and recoveries.  The CPC is responsible for ensuring the Contingency Plan is fully executed in the event of an outage. The CPC is also responsible for coordinating and facilitating communications among various responsible parties. | Mark Campbell  Director of Information Technology  America’s Essential Hospitals  1301 Pennsylvania Avenue, NW, Suite 950  Washington, DC 20004  (202) 585-0553  [mcampbell@essentialhospitals.org](mailto:mcampbell@essentialhospitals.org) |
| **Facilities Manager** | The Facilities Manager works with the CPC to ensure facility availability and safety of employees. The Facilities Manager coordinates with building management, the CPC, and the SO. | Alan Burk  Director of Human Resources  America’s Essential Hospitals  1301 Pennsylvania Avenue, NW, Suite 950  Washington, DC 20004  (202) 585-0129  aburk@essentialhospitals |
| **Contingency Planning Coordinator Backup** | The CPC backup is responsible for executing the System IT Contingency Plan in the event that the CPC is unable to execute this plan. | Frank Neuner  Absolute Computer Solutions  2831 Gallows Rd., Suite 135  Falls Church, VA 22042  (703) 981-4784  [fneuner@abs-com.com](mailto:fneuner@abs-com.com) |
| **Facilities Manager Backup** | The Facilities Manager backup is responsible for executing the System IT Contingency Plan in the event that the Facilities Manager is unable to execute this plan. | Rhonda Gold  CFO  America’s Essential Hospitals  1301 Pennsylvania Avenue, NW, Suite 950  Washington, DC 20004  (202) 585-0109  [rgold@essentialhospitals.org](mailto:rgold@essentialhospitals.org) |
| **Network Consultant** | Assist as needed with all aspects of the contingency plan. | Frank Neuner  Absolute Computer Solutions  2831 Gallows Rd., Suite 135  Falls Church, VA 22042  (703) 981-4784  [fneuner@abs-com.com](mailto:fneuner@abs-com.com) |
| **Team Member** | Assist as needed with all aspects of the contingency plan. | America's Essential Hospital Leadership Team |

## Tier Action Plan Overview

Below are 2 Action Plans (Tier 1 and Tier 2) determined by a damage assessment. The first step in any disaster is to identify its severity.

## Tier 1 Action Plan—Must Permanently Relocate

* + 1. Damage Assessment
       - 1. Cannot renter building again.
    2. Action Plan
       - 1. All employees work from home until notified otherwise.
         2. Notify members.
         3. Secure temporary office space.
         4. Secure permanent office space.
         5. Contract with network host.
         6. Host builds network.
         7. Host recovers from backups.
         8. Install Internet access to office space.
         9. Install PRI phone circuits to office space.
         10. Purchase, install, and configure workstations, printers, copiers, and phones.

## Tier 2 Action Plan—Key Staff Relocate for 30 Work Days/Weeks

* + 1. Damage Assessment
       - 1. Cannot enter offices for up to 30 business days.
         2. Building is sound, but more than 75% of all resources and utilities are too damaged for on-site restoration.
    2. Plan Type

Off-site plan

* + 1. Action Plan
       - 1. Resume all critical operations at alternate site.
         2. All employees work from home until alternate site is identified.
         3. Need a building/place for network.
         4. Need authorization for purchasing equipment and Internet access.
         5. Rebuild network off site.
         6. Establish Internet access.
         7. Install firewall, router, switches, and cabling
         8. Install servers.
         9. Recover from backups.
         10. Configure and attach workstations.

## Contingency Plan Phases Overview

The 3 Contingency Plan Phases outlined below explain in greater detail what should happen when a disaster occurs.

## Contingency Plan Phase 1: Notification/Activation Phase

The Notification/Activation Phase defines the initial actions that should be taken once a system disruption or emergency has been detected or appears to be imminent. During this phase, if a service/system disruption or emergency occurs, or is imminent, the Association employees take the actions required to preserve life, coordinate notifications, assess damages, and initiate the plan.

### Outage Notification

Employee safety is the first priority of the Association; therefore, it is paramount that all employees follow the established evacuation procedures, should the need arise. Once all employees are safe and accounted for, the contingency process may begin with notifications. Events requiring activation of the IT Contingency Plan may occur with or without prior notification. In either situation, the notification procedures in this IT Contingency Plan should be followed. If the outage is not planned, the individual that notices a system outage should call the Contingency Planning Coordinator (CPC). If the CPC is not available, the backup CPC should be notified.

The caller should provide the CPC with detailed information such as:

* + 1. Component affected (workstation or server).
    2. Location of the outage.
    3. Type of outage (e.g., power or hardware or software failure).
    4. Result of outage (e.g., compromise of system information).
    5. Criticality of the outage to the business.

### Damage Assessment Procedures

Upon notification of a system outage or emergency, the CPC or alternate conducts a damage assessment to identify the major problem areas, assess the damage, and determine the estimated time required to restore the IT infrastructure and resume business activities. Based on the type of event that has occurred, the CPC determines the appropriate corrective measures to ensure successful recovery of the Association's operations.

### Outage/Escalation Notification

Events requiring activation of the plan may occur with or without prior communication. Planned events are coordinated by management, and the employees are notified via email and/or cell phone. If an unplanned event occurs, use the following guidelines:

### Employees

Use the Emergency Procedures, if needed. For example, if the building is evacuated. Contact your manager.

### Contingency Plan Team

* + - * 1. Assess the situation. Determine if the problem is isolated to a single user or if it is affecting multiple users.
        2. Gather information. Write down specific facts like warnings or error messages.
        3. Acquire resources. Contact the appropriate party for assistance with resolving the issue. For example, contact the CPC and your VP.
        4. CPC determines next steps. If the CPC is not available, contact the Alternate.

### Plan Activation

Based on the results of the damage assessment the CPC recommends a plan of action to the Association Systems Owner for approval. Unless otherwise noted, the CPC determines whether or not restoration should take place on-site or off-site to expedite recovery.

### Plan Notification

The CPC provides the nature and impact of the event and an estimated time for recovery to all members of the Contingency Plan Team.

## Contingency Plan Phase 2: Recovery Phase

During the Recovery phase, activities focus on the contingency measures that are required for repairing and restoring the Association IT infrastructure so that critical operations may resume. These activities include:

* 1. Arranging for the repair and/or purchase of replacement resources.
  2. Setting up a command center, preparing an alternate site (resumption center), and restoring data to recover from a disaster.
  3. Arranging for daily status meetings using teleconferencing.
  4. Resuming critical operations and business activities, either on-site or off-site.

### Sequence of Recovery Activities

Upon activation of the plan, the CPC is responsible for overseeing the recovery of the Association Operations, monitoring the Recovery Team so that all necessary tasks are performed expeditiously, and regularly communicating situation updates to the Contingency Plan Team and other appropriate personnel.

### Prerequisites

Before starting the recovery activities, the following tasks should already be completed:

* + 1. Damage assessment.
    2. Tier Action Plan selection.

### Activity Sequence Outline

Use the following high-level activity sequence to coordinate and control the recovery operation:

* + 1. Establish a command center and resumption site, which will be determined at the time of the emergency.
    2. Assemble Team Members. Brief them on the current situation and provide resumption/recovery task assignments.
    3. Repair or purchase essential replacement computer equipment and verify that is it installed/setup and operational.
    4. Arrange for telephone communications and internet connectivity, if not already working through communication vendor.
    5. Get network operational.
    6. Restore accounting functions.
    7. Determine time frames and follow-up with clients and vendors to help ensure that all tasks are completed as promptly as possible.
    8. Advise appropriate personnel of current statuses.
    9. Provide a list of purchase requirements to the System Owner for purchase approval.
    10. Activate resumption site if needed. If using the alternate site.
    11. Maintain an Activity Log.
    12. Arrange for a site survey with a damage adjustor and/or insurance assessor.

### Recovery Procedures

During the recovery process, the CPC supervises and assists all parties so that all procedures are followed appropriately and expeditiously.

Additionally, the CPC works with the appropriate personnel to determine some general factors, which are reported to the Team and used throughout the recovery process. These factors are:

* + 1. Actual versus projected collection capacity—is the Association able to serve its members as efficiently as predicted?
    2. Effects of the interruption on the amount of work in progress—how much work time and productivity is lost or not lost.
    3. Skill set and number of employees needed to maintain membership support levels—ascertain who has the best abilities and are they available.

The following scenarios were developed for recovering the Association after an interruption. The instructions for each scenario are high-level and intended for technical individuals who have a clear understanding of the Association Operations and are at a high level.

### IT Recovery Priority Sequence

* + 1. Network backbone.
    2. Internet service.
    3. Workstations and access.
    4. Accounting system.
    5. Membership system.
    6. Phone and voicemail service.

## Contingency Plan Phase 3: Reconstitution Phase

During the reconstitution phase, once critical business operations that support time-sensitive operations are recovered, the Association re-establishes all operations using two stages: restoration (if needed) and resumption.

### Restoration Stage

This stage is used if the affected location requires repairs that cannot be made with staff on site, or if the location is damaged beyond repair and a new site is chosen.

During the restoration stage the following tasks are accomplished:

* + 1. The affected office is returned to a working state; if the affected office cannot be repaired, a new location is acquired, either permanently or temporarily..
    2. Personnel and equipment are transported to either the restored or new location.
    3. The System Owner and Contingency Plan Team are notified that normal operations have recovered (declaration of full recovery).
    4. If a new office is acquired, the new address and move-in date are provided to the Association members by the System Owner, along with any other pertinent information.

### Building Repairs or Acquisition

Depending on the type and severity of damage incurred, the Facilities Manager is responsible for several tasks to help ensure that the site is repaired within a period of time specified by the System Owner. If that timeline cannot be completed, or the building is beyond repair, the System Owner and Facilities Manager shall coordinate the acquisition of a new location.

Items to consider:

* + 1. Establish what items were salvaged and can be re-used.
    2. Decide which damaged equipment should be immediately repaired and which items can wait for repair.
    3. Contact insurance company.
    4. Create authorizations for replacement items and repair estimates for damaged items.

Work with the CPC to:

* + 1. Either organize repair/maintenance projects and timelines with the building management, or coordinate with the System Owner regarding leasing a new site.
    2. Obtain vendor quotes for the repair and/or replacement of vital resources.
    3. Create a timetable schedule of building repair timeline, delivery dates, vendor/product availability, etc.
    4. Prepare a budget.
    5. Present quotes, budget, and timetable to the System Owner for approval.
    6. Submit the orders for fulfillment.
    7. Follow-up on all statuses (building maintenance, purchases, repairs, etc.).
    8. Update the System Owner and other key personnel as needed.

### Building Occupancy (Re-entry or Move-in)

Once the primary site is repaired and safe for re-entry, or the new location is ready for occupants, the Facilities Manager:

* + 1. Inspects the facility to ensure that it meets the Association standards and that all restoration is complete (primary site repair only).
    2. Sets the move-in date with the System Owner and notifies other key personnel of the date.
    3. Works with the CPC to arrange for any equipment transportation from storage and/or the resumption site, if applicable.
    4. Supervises the delivery, arrangement, and setup of new and salvaged equipment and supplies.
    5. Updates System Owner of any problems with accomodations or lack of equipment.

### Resumption Stage

This is the final stage of restoration and begins once the following tasks are complete:

* + 1. Critical business operations are recovered, either on- or off-site.
    2. Any building repairs (except minor and/or cosmetic fixes) are finished.

All equipment and personnel are either re-established in the office or are moved into a new location.  
During the resumption stage the following tasks are accomplished:

* + 1. All business operations are resumed and verified as operative.
    2. Recovery activities are terminated by deactivating the plan.

### Operations Verification

Before officially deactivating the plan, the CPC must verify that all business operations are re-established and working properly at the affected site. This verification process applies to all types and tiers of the plan, even if minimum recovery was performed on-site.

To complete the verification process, the CPC coordinates with the appropriate personnel to verify that the following operations are running:

* + 1. IT connectivity.
    2. Accounting functions.
    3. Membership system functions.
    4. Phone Service.
    5. Mail delivery.

### Plan Deactivation

Once operations are successfully verified, the CPC does the following:

* + 1. Declares the plan deactivated.
    2. Completes any outstanding paperwork (checklists, logs, and so on).
    3. Updates the System Owner.

## Contingency Plan Testing

The Association reviews and tests the plan annually to help ensure the accuracy of the Plan and identify deficiencies before the need to execute a Contingency Plan occurs.

During the review process, a table top test is performed where all key participants review virtual plan scenarios that cover each element of the Plan. This helps verify priority levels, update old data, correct mistakes, identify anomalies, and rewrite confusing procedures. This can also meet the training requirement.

## Training

All personnel involved with the plan (planning and execution) review the plan annually and sign a statement acknowledging they understand the contents of the plan.



## APPENDIX 1: External Contacts

| **Name, Title** | | **Contact Option** | | **Contact Number** |
| --- | --- | --- | --- | --- |
| **Property Manager** | | Quadrangle HQ | | 202.662.1200 |
| Loading Dock | | 202.662.1222 |
| Guard Desk | | 202.393.3271 |
| **Phone/Internet Broker** | | ARG | | 703.770.2400 |
| Email Address | | support@myarg.com |
| **Avaya Phone Equipment** | | E-Tel | | 703.904.1700 |
| Email Address | | bburris@e-telsystems.com |
| **IT Hardware Supplier** | | Absolute Computer Solutions | | 703.242.8331 |
| Mobile | | 703.981.4784 |
| Email Address | | fneuner@abs-com.com |
| **IT Hardware Supplier** | | B&H | 800.606.6969 | |
| Website | www.bhphotovideo.com | |
| **Insurance** | | Rust Insurance | 202.776.5000 | |
| Broker | Dave Riley | |
| Email Address | driley@rustinsurance.com | |
| **Off-Site Storage** | | Bank of America Safety Deposit Box | 700 13th St  202.624.4413 | |
| IBackup for Windows | https://www.ibackup.com/ibackup-for-windows/ | |
| **Police** | Phone | | 911 | |
| **Fire** | Phone | | 911 | |
| **Police Non-Emergency** | Phone | | 202.727.9099 | |

## APPENDIX 2: Contingency Plan Team Contact Information

| **Name, Title** | **Phone Numbers** | **Emails** |
| --- | --- | --- |
| **Siegel, Bruce** | 202.585.0115 (W) 301 775.2585 (C) 301.897.5398 (H) | [bsiegel@essentialhospitals.org](mailto:bsiegel@essentialhospitals.org) [bsiegel1804@gmail.com](mailto:bsiegel1804@gmail.com) |
| **Gold, Rhonda** | 202.585.0109 (W) 301 840.5476 (H) 301 233.3743 (C) | [rgold@essentialhospitals.org](mailto:rgold@essentialhospitals.org) [Rgold61@verizon.net](mailto:Rgold61@verizon.net) |
| **Burk, Alan** | 202.585.0129 (W) 443.812.4019 (C) 410.461.2809 (H) | [aburk@essentialhospitals.org](mailto:aburk@essentialhospitals.org) [alanjburk@verizon.net](mailto:alanjburk@verizon.net) |
| **Campbell, Mark** | 202.585.0553 (W) 301.770.0934 (H) 240-731-6138 (C) | [mcampbell@essentialhospitals.org](mailto:mcampbell@essentialhospitals.org) llebpmacm@gmail.com |
| **Feldpush, Beth** | 202.585.0111 (W) 703.403.0785 (C) 703.243.6341 (H) | [bfeldpush@essentialhospitals.org](mailto:bfeldpush@essentialhospitals.org) [bcfeldpush@hotmail.com](mailto:bcfeldpush@hotmail.com) |
| **Metter, Kristine** | 202.585.0573 (W) 703.405.7727 (C) | [kmetter@essentialhospitals.org](mailto:kmetter@essentialhospitals.org) [kjmetter@gmail.com](mailto:kjmetter@gmail.com) |
| **Engler, David** | 202.585.0125 (W) 614.764.4937 (C) | [dengler@essentialhospitals.org](mailto:dengler@essentialhospitals.org) davidengler@me.com |

## APPENDIX 3: Sample Scenarios

## Scenario 1: Server Outage

**Event:** During business hours, the Association Main Servers powers off for an unknown reason. All other devices in the server room have power and are working normally. Employees cannot access critical account and member data.

**Action:** Use the steps below to resolve this event (on-site or off-site is yet to be determined).

* 1. Respond to the situation by notifying the appropriate personnel.
  2. Assembly the team members whose expertise best fits the situation.
  3. Notify all users of the situation.
  4. Determine if the server can be recovered on-site within a reasonable yet limited time frame.
  5. Reboot server and assess if power is present. Check outlets for power.
  6. Verify that server data is now accessible
  7. Check the data’s integrity by reconciling it against reports.
  8. Notify all users that the situation is resolved.

## Scenario 2: Voice Communications Failure

**Event:** During business hours, the phone service is inactive. Incoming calls cycle through a message stating that the operator is unable to take calls. Dialing a specific extension takes the caller directly to voicemail. the Association users can make outgoing calls without encountering a problem.

**Action:** Use the steps below to resolve this event (on-site or off-site is yet to be determined).

* 1. CPC should ensure Operations and facilities Manager and system owner are aware of phone outage
  2. Determine if outage is internal or external
  3. Contact internet vendor if external issue
  4. Contact phone vendor if internal phone panel issue
  5. Keep plan team updated regarding status

## Scenario 3: Power Outage

**Event:** After 3:00 p.m. the entire building loses power for 45 minutes. Most devices are connected to an Uninterruptible Power Supply (UPS) or laptop battery.

**Action:** Use the steps below to resolve this event.

* 1. Respond to the situation by notifying the appropriate personnel.
  2. Assembly the team members whose expertise best fits the situation.
  3. Contact Electric Company to determine outage period and for updates.
  4. If the power outage is estimated to last at least 24 hours, activate the Plan.
  5. Perform a proper shutdown for each of the servers in the data center.
  6. Walk the floor and turn off office equipment, such as copiers, printers, and fax machines and shutdown any office workstations to help prevent a power surge.
  7. When the power is restored, turn on all servers and workstations in the server room.
  8. Verify that each device starts properly and that you can access the Association Network.

## Scenario 4: Building Evacuation

**Event:** During business hours, a tornado occurs. Some visible building damage is present and the power to the entire area is out. All tenants are requested to evacuate the building for damage assessment. There is some structural damage and tenants are not allowed to re-enter the building until repairs are made. The repair completion is estimated at three weeks.

**Action:** Use the steps below to resolve this event.

* 1. Evacuate the building and proceed as instructed in the Association Emergency Procedures.
  2. Respond to the situation by notifying the appropriate personnel.
  3. Assembly the IT Restoration Team.
  4. Contact the alternate location, update them on the situation, and setup a command and resumption center.
  5. *Client Coordinator:* Communicate the situation to the Association clients.  
     *Facilities Manager:* Work with the Project Managers to staff the alternate site as directed by the System Owner.  
     *Operations Manager:* Notify all employees of the situation and provide them with scheduling information.
  6. From the alternate site recover the following:
     1. P1 resources within 24 to 48 hours.
     2. P2 resources within 5 business days.
     3. P3 resources within 14 business days.
  7. Continue working from the alternate site or at home until the primary location is accessible.
  8. Upon re-entering the primary location, perform a damage assessment to determine if any resources need repair or replacement before resuming normal operations.
  9. Verify that the resources are working and “tear down” the alternate site.
  10. Notify all parties that normal operations have resumed.

## APPENDIX 4: Hardware Inventory

|  |  |  |
| --- | --- | --- |
| **Server Name** | **Operating System** | **Server Role** |
| NAPH2 | Windows Server 2008 | Avaya IP Office 9.0 |
| NAPH-ACCOUNTING | Windows Server 2008 R2 | Microsoft Dynamics SL version 8.01 (MSSQL 2008)  FRx 6.7 |
| NAPH-DOMAIN2 | Windows Server 2003 | Primary Domain Controller |
| NAPH-DPS | Windows Server 2008 R2 | Microsoft Data Protection Mgr 2010 |
| NAPH-EXCHANGE | Windows Server 2008 R2 | Microsoft Exchange 2010  Active Directory |
| NAPH-FILES | Windows Server 2008 R2 | File Server |
| VS1 | Windows Server 2008 R2  Hyper V | Remote Virtual Desktops |
| VS2 | Windows Server 2008 R2  Hyper V | APPSRV. iMIS 15 application server (2008 R2)  DBSRV. iMIS 15 SQL database server (2008 R2/MS SQL 2008)  DC1. Backup domain controller (2003 SP2)  ISGWEB. ISG web server (2003 SP2) |
| VS3 | Windows 2008 R2 | Remote Virtual Desktops |
| VS4 | Windows 2008 R2 | Remote Virtual Desktops |

## APPENDIX 5: Software Inventory

| **Name** | **Description** |
| --- | --- |
| Microsoft Server 2010 | Microsoft Operating System |
| Microsoft SQL Server 2008 | Microsoft SQL |
| Microsoft Exchange 2010 | Microsoft Exchange |
| iMIS 15 | SQL database and front end to manage association records. |
| Dynamics 8 | SQL database and front end to manage association accounting records. |
| FRx 6.7 | Report writer for accounting package. |
| Office Professional 2010 | Microsoft Office Professional (Outlook, Word, Excel, Power Point, Access, One Note) |
| Crystal Reports | Report writer for SQL databases |

# Receipt and Acknowledgement

# Information Services & Technology

# CONTINGENCY PLAN

My signature below affirms that I have read and will adhere to this policy. I understand that I am a member of the Association Contingency Plan Team

**Employee Signature**

**Date**

**Print Name**