America’s Software Corporation

Business Continuity Plan

Version 3.0

1/6/2019

The priorities in a disaster situation are to:

1. Ensure the safety of employees and visitors in the office buildings.
2. Mitigate threats or limit the damage that threats can cause.
3. Have advanced preparations to ensure that critical business functions can continue.
4. Have documented plans and procedures to ensure the quick, effective execution of recovery strategies for critical business functions.

Emergency management is responsible for:

1. Periodically reviewing the adequacy and appropriateness of its Business Continuity strategy.
2. Assessing the impact on the EMERGENCY MANAGEMENT Business Continuity Plan of additions or changes to existing business functions, EMERGENCY MANAGEMENT procedures, equipment, and facilities requirements.
3. Keeping recovery team personnel assignments current, taking into account promotions, transfers, and terminations.
4. Communicating all plan changes to the Business Continuity Coordinator so that the organization’s IT master Disaster Recovery Plan can be updated.

Facilities Management Department management is responsible for:

1. Maintaining and/or monitoring offsite office space sufficient for critical EMERGENCY MANAGEMENT functions and to meet the EMERGENCY MANAGEMENT facility recovery time frames.
2. Communicating changes in the “Organization IT Disaster Recovery Plan” plan that would affect groups/departments to those groups/departments in a timely manner so they can make any necessary changes in their plan.
3. Communicating all plan changes to the Business Continuity Coordinator so that the master plan can be updated.

The Business Continuity Coordinator is responsible for:

1. Keeping the organization’s IT Recovery Plan updated with changes made to EMERGENCY MANAGEMENT facilities plans.
2. Coordinating changes among plans and communicating to EMERGENCY MANAGEMENT when other changes require them to update their plans.

A. Recovery Plan Phases

The activities necessary to recover from a AMERICA'S SOFTWARE CORPORATION facilities disaster or disruption will be divided into four phases. These phases will follow each other sequentially in time.

1. Disaster Occurrence

This phase begins with the occurrence of the disaster event and continues until a decision is made to activate the recovery plans. The major activities that take place in this phase includes: **emergency response measures, notification of management, damage assessment activities, and declaration of the disaster.**

2. Plan Activation

In this phase, the Business Continuity Plans are put into effect. This phase continues until the alternate facility is occupied, critical business functions reestablished, and computer system service restored to AMERICA'S SOFTWARE CORPORATION's Departments. The major activities in this phase include: **notification and assembly of the recovery teams, implementation of interim procedures, and relocation to the secondary facility/backup site, and re-establishment of data communications.**

3. Alternate Site Operations

This phase begins after secondary facility operations are established and continues until the primary facility is restored. **The primary recovery activities during this phase are backlog reduction and alternate facility processing procedures.**

4. Transition to Primary Site

This phase consists of any and all activities necessary to make the transition back to a primary facility location.

5. Communication. Customers

Customers are the life of a business, so contact with customers is a top priority. Customers may become aware of a problem as soon as their phone calls are not answered or their electronic orders are not processed. Our business continuity plan includes action to redirect incoming telephone calls to a second call center (if available) or to a voice message indicating that the business is experiencing a temporary problem. The business continuity plan should also include procedures to ensure that customers are properly informed about the status of orders in process at the time of the incident. Customer service or sales staff will be assigned to communicate with customers if there is an incident.

B. Vital Records Backup

All vital records for EMERGENCY MANAGEMENT that would be affected by a facilities disruption are maintained and controlled by either EMERGENCY MANAGEMENT or Disaster Recovery/IT. Some of these files are periodically backed up and stored at an offsite location as part of normal EMERGENCY MANAGEMENT operations.

When EMERGENCY MANAGEMENT requires on-site file rooms, scanning, and organization offsite storage locations, best practices advise using one near-by Records Warehouse and another secure site for vital records and data back-up. All vital documents are typically located in files within the office complex and the most current back-up copies are in a secure off-site storage facility.

C. Restoration of Hardcopy Files, Forms, and Supplies

In the event of a facilities disruption, critical records located in the EMERGENCY MANAGEMENT Department may be destroyed or inaccessible. In this case, the last backup of critical records in the secure warehouse would be transported to the secondary facility. The amount of critical records, which would have to be reconstructed, will depend on when the last shipment of critical records to the offsite storage location occurred.

EMERGENCY MANAGEMENT will arrange the frequency of rotation of critical records to the offsite storage site.

The following categories of information can be exposed to loss:

1. Any files stored on-site in file cabinets and control file rooms.
2. Information stored on local PC hard drives.
3. Any work in progress.
4. Received and un-opened mail.
5. Documents in offices, work cubes and files.
6. Off-site records stored in the Records Warehouse (if this is not a secure, hardened facility).

D. On-line Access to AMERICA'S SOFTWARE CORPORATION Computer Systems

In the event of a facilities disruption, the IT Disaster Recovery Plan strategy should be to assist in re-establishing connectivity to the AMERICA'S SOFTWARE CORPORATION departments and to establish remote communications to any alternate business site location. If the data center is affected by a disaster or disruption, the IT Disaster Recovery Plan should include recovering processing at a pre-determined alternate site. Services covered would include; phones, cellular phones, pagers, communications, and all other services required for restoring limited emergency service to the organization.