Greater Rochester Chamber of Commerce

(FKA: Rochester Business Alliance)

Disaster Recovery Plan/Security Incident Response Plan

Rev. 8/15/2017

Purpose:

The purpose of this plan is to document the process to recover from an incident which causes a disruption in service or services provided by the Greater Rochester Chamber of Commerce and also a security breach. The outline covers procedures to follow from a total loss or "facility destroyed" to computer server crash. The plan is designed in outline form with major category groups defined so the process can be initiated at any point and cover only the specific loss of service type. The basic categories are prioritized by relevance of need in a total loss scenario.

Required preprocess procedures:

- Data backups- The Rochester Chamber must continue to backup files, data and server configurations according to industry standards.
    - Weekly full backups
    - Daily incremental backups
    - Offsite storage
    - Encrypted data
- Staff lists – Up to date including home contact information. At minimum 2 senior staff members should store this information off site.
- Network Administrator - Computer login rights with administrator capabilities to be maintained by 2 separate user accounts with complex passwords.
- Bank Account access - Check signing rights to be maintained by 3 senior staff members and cannot include the accounting department staff. All checks over 5,000 require 2 signatures.
- Insurance company – The Rochester Chamber's insurance company contact and call escalation tree must be documented.
- Contact list – A call list of key function areas must be updated and maintained. This list is prioritized by first call and relevant situation.

Initial Steps:

Implement the disaster action team according to the following plan.

- Contact First Responders as defined by the DRP Contact list to determine scope of disaster.
- Contact Senior Staff (Disaster Recovery Team) to determine plan of action.
- Assign duties to recovery and determine communication message.
- Call insurance company to report and assess recovery.
- Contact appropriate governmental agency if sensitive personal information is compromised.

Process Tree:

1. Redirect phone system – Move main telephone number to designated contact – Director of Communications.
    a. Contact current phone vendor to forward main line to the designated contact
    b. Contact phone vendor
    c. Redirect other numbers to other locations/equipment using the following priority list of services
        i. Payroll
            1. Fax
            2. Call in
        ii. President – DID number
        iii. Health Insurance
            1. Fax
            2. Call in
        iv. Reference Checking
            1. Fax
            2. Call in
        v. Staffing
            1. Fax
            2. Call in

    d. Refer to list of #'s from disaster recovery file – Phone List to finalize transferred/forwarded phone number list. Disaster action team to determine additional phone system needs
2. Data breach- Shutdown firewall and secure access points.
    a. Lockdown network to close out breach.
    b. Review and save firewall log files to determine length of compromise.
    c. Save all server log files to common location for review.
        i. Review log file to determine source of breach.
        ii. Review and compare data to determine scope of breach.
    d. Contact appropriate governmental agency and report possible data loss.

3. Restore computer systems – Scope of disaster will determine whether to start at step "a" no workable server equipment or "b" internal server failure.
    a. Secure server space at local vendor according to "contact list"
    b. Install operating system (if needed)
    c. Restore data from back up tape
    d. Restore connectivity
        i. Internal client computers
        ii. External computers (if needed)
    e. Contact appropriate employees
    f. Contact customers affected by service disruption
    g. Order of significant process restoration
        i. Payroll services
        ii. Email
        iii. Reference Checking
        iv. Health Insurance
        v. Membership/Events
        vi. Accounting
        vii. Personal/Shared/Public files

4. Secure temporary office space for operations relocation
    a. Require 10,000 SF
        i. Contact current landlord from contact list
        ii. Other leasing companies
        iii. Convention Center
        iv. Local Hotels
    b. Secure Temporary Furniture and Fixtures
        i. 40 Cubicles

        ii. Adequate lighting
        iii. Chairs
        iv. Desks
    c. Secure Temporary Equipment
        i. Computers
        ii. Faxes
        iii. Copiers
        iv. Printers
        v. Phones

5. Secure or rebuild permanent location to house business
    a. Requires 18,000 SF
        i. Contact current landlord from contact list
        ii. Other leasing companies
    b. Secure permanent Furniture and Fixtures
        i. 40 employees
        ii. 3 tenants
    c. Secure Equipment
        i. Computers
        ii. Servers
        iii. Faxes
        iv. Copiers
        v. Printers
        vi. Phones
    d. Build out new space and move in

6. Reprint Materials
    a. Checks
    b. Timecards
    c. Brochures