

Disaster Recovery & Information Security Plan Outlines

A common best practice for any organization or IT department is to have plans in place which represent documented procedures and policies for both audiences with respect to how security is established and managed from a technology standpoint and what an expected response should be in preparation and response to a disaster incident and recovery to normal operations. These documents are typically robust and holistic in their approaches to each of these topics and developed for multiple internal audiences. Part of the District Technology Committee's agenda is to create these detailed plans over the course of the next few years, but has chosen to identify some of the core elements that will be included and/or integrated in other organizational planning moving forward.

Disaster Recovery Outline/Topics:

- Overview
- Incident History
- Plan Approval process
- Declaration of Disaster process
 - Authorized Personnel
 - Plan Activation step
 - Resumption of normal operations confirmation
- Disaster Recovery Phases
 - Disaster Assessment
 - Disaster Recovery Activation
 - Alternate Site/Data Center Rebuild
 - Return Home
- Key Activities
- Decision Tree
- Recovery Time Objectives (RTO)
- Recovery Point Objectives (RPO)
- Command Center Location
- Vital Records Identification & Retrieval
- Disaster Recovery Team & Responsibilities
 - Management Team
 - Technical Support Team
 - Hardware Responsibilities
 - Software Responsibilities
 - Network Responsibilities
 - Operations Responsibilities
- Sequence of Recovery Tasks
 - Application Recovery Priorities
 - Tier 0 Applications – No special disaster recovery plan needed
 - Tier 1 Applications – 5 days
 - Tier 2 Applications – 10 days
 - Tier 3 Applications – 15 days

- Tier 4 Applications – When possible
 - Application Details
 - Server Recovery
 - Rack layout
 - Server Details
 - Network Recovery
 - Recovery Procedures
 - Network Diagram
- Training Procedures for Disaster Recovery Team
- Testing the Disaster Recovery Plan
- Damage Assessment & Salvage Activities
- Emergency Phone Numbers

Information Security Outline/Topics:

- Scope of plan
- Information Security Organization
- Roles and Responsibilities
 - Information Security Officer
 - System owners/administrators
- Key Information Systems
- Physical Security
- Network Security
- Incident response procedure
- Policies and standards
- Risk Management
 - Assessment
 - Mitigation
- Security Awareness & Training
- Reporting Security Risks