Halcyon

Contingency Response Plan

Version 1.0

May 9, 2019

Table of Contents

Section I: Introduction

A. Introduction

At Halcyon, information technology (IT) and automated information systems are vital elements to our business model and processes. Because these IT resources are so essential to the success of our organization, it is critical that the services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans and procedures and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster.

B. Purpose

This Contingency Plan establishes procedures to recover IT systems following a disruption. The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - Notification/Activation phase to detect and assess damage and to activate the plan
  - Recovery phase to restore temporary IT operations and recover damage done to the original system
  - Reconstitution phase to restore IT system-processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed to carry out IT system processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated Halcyon personnel and provide guidance for recovering IT systems during prolonged periods of interruption to normal operations.
- Ensure coordination with other Halcyon staff who will participate in the contingency planning strategies. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

C. Scope

Given the broad range of information system designs and configurations, as well as the rapid development and obsolescence of products and capabilities, the scope of the discussion is not intended to be comprehensive. Rather, the document describes technology practices to enhance an organization's information system contingency planning capabilities. These guidelines present contingency planning principles for the following common platform types:

- Client/server systems;
- Telecommunications systems; and
- Mainframe systems.

Various scenarios were considered to form a basis for the plan, and multiple assumptions were made. The applicability of the plan is predicated on two key principles:

- Halcyon's facility in Chicago, IL, is inaccessible; therefore, Halcyon is unable to perform functional IT operations
- A valid contract exists with the alternate site that designates that site in Poland, United Kingdom, South Korea, and Arkansas, U.S., as the Halcyon's alternate operating facility.
  - Halcyon will use the alternate site building and IT resources to recover system functionality during an emergency that prevents access to the original facility.

  - The designated computer system at the alternate site has been configured to begin processing system information.
  - The alternate site will be used to continue system recovery and processing throughout the period of disruption, until the return to normal operations.

Halcyon’s Contingency Plan does not apply to the following situations:

- Overall recovery and continuity of business operations.
- Emergency evacuation of personnel.

Section 2: Background

Information systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire). Much vulnerability may be minimized or eliminated through management, operational, or technical controls as part of the organization’s resiliency effort; however, it is virtually impossible to completely eliminate all risks. This plan is designed to mitigate the risk of system and service unavailability by providing effective and efficient solutions to enhance system availability.

A. Types of Plans

An organization would use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization’s information systems, mission/business processes, personnel, and the facility. Because there is an inherent relationship between an information system and the mission/business process it supports, there must be coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

a. Incident Response Plan

The IRP establishes a framework for quick, decisive, and appropriate responses to an incident.

b. Disaster Recovery Plan

The DRP applies to major, usually physical disruptions to service that deny access to the primary facility infrastructure for an extended period.

c. Business Continuity Plan

The BCP focuses on sustaining an organization’s mission/business processes during and after a disruption.

Plan	Purpose	Scope
Incident Response Plan	By establishing a framework for quick, decisive, and appropriate responses to an incident, we can limit the impact of an adverse event. This will be beneficial for the customers, resources, and the company. This is also intended to facilitate timely correction of any damage that comes as a result of	This policy applies to any established and defined business entity within Halcyon which includes associates, third-party service providers, and physical/electronic information systems.

	an incident and provide effective and efficient follow up actions. Anything that threatens the confidentiality, integrity, and availability of our services should have a proper response provided before an incident actually takes place. Responsibility and accountability for all steps in the process are also established within this policy.	
Disaster Recovery Plan	IT services are considered a critical component in the daily operations of Halcyon, requiring a comprehensive disaster recovery plan to assure that these services can be re-established quickly and completely, regardless of the magnitude and unpredictability of a disaster. This plan represents the requirements and the steps that will be taken in response to and for the recovery from any disaster affecting IT services at Halcyon, with the fundamental goal of allowing basic business functions to resume and continue until such time as all systems can be restored to pre-disaster functionality. Please note that no two emergencies are identical. Therefore, no single plan of action can anticipate and address every possible circumstance. The	Due to the uncertainty regarding the magnitude of any potential disaster, this plan will only address the recovery of systems under the direct control of Halcyon’s IT department and that are critical for business continuity. This includes the following major areas: • Authentication, single-sign-on, and network directory services • On-premises enterprise applications • Datacenters • On-premises website and services • Equipment (ex: work laptops) • Data networks and telecommunications (wired and wireless networks, file services) Other critical services such as hosted enterprise apps (payroll, records) and email will be addressed in terms of connectivity and integration of these services but the recovery

	instructions contained in this plan are intended to serve as guidelines only. They may not be appropriate in all cases. At no time should you risk your personal safety in complying with any of its provisions.	of the systems themselves is beyond the scope of this document. This plan covers Incident Response, Assessment and Disaster Declaration, Incident Planning and Recovery, and Post Incident Review.
Business Continuity Plan	The purpose is to coordinate recovery of critical business functions in managing and supporting the business recovery in the event of a facilities (office building or data center) disruption or disaster. This can include short or long-term disasters or other disruptions, such as fires, floods, earthquakes, explosions, terrorism, tornadoes, extended power interruptions, hazardous chemical spills, and other natural or man-made disasters. A disaster is defined as any event that renders a business facility inoperable or unusable so that it interferes with the organization's ability to deliver essential business services. The priorities in a disaster situation are to: 1. Ensure the safety of employees and visitors in the office buildings. (Responsibility of the ERT) 2. Mitigate threats or limit the damage that threats can cause. (Responsibility of the ERT)	The Business Continuity Plan is limited in scope to recovery and business continuance from a serious disruption in activities due to non-availability of Halcyon's facilities. The Business Continuity Plan includes procedures for all phases of recovery. This plan is separate from Halcyon's Disaster Recovery Plan, which focuses on the recovery of technology facilities and platforms, such as critical applications, databases, servers or other required technology infrastructure. Unless otherwise modified, this plan does not address temporary interruptions of duration less than the time frames determined to be critical to business operations. The scope of this plan is focused on localized disasters such as fires, floods, and other localized natural or man-made disasters. This plan is not intended to cover major regional or national disasters such as regional earthquakes, war, or nuclear holocaust.

	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. The Information Technology Business Continuity Plan includes procedures for all phases of recovery.	However, it can provide some guidance in the event of such a large-scale disaster.

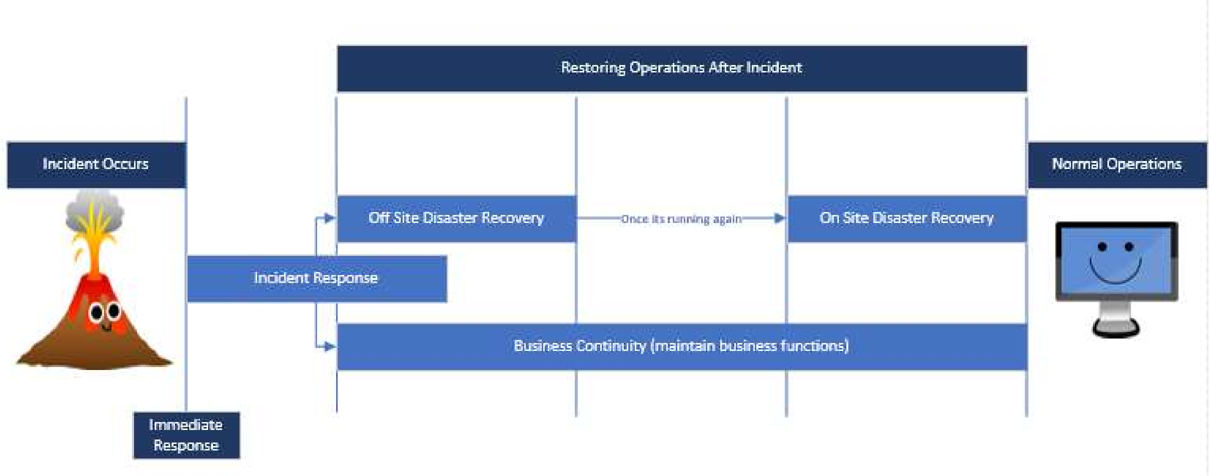

Restoring Operations After Incident
Incident Occurs
Normal Operations
Off Site Disaster Recovery
Once its running again
On Site Disaster Recovery
Incident Response
Business Continuity (maintain business functions)
Immediate Response

Fig 2-1: Contingency-Related Plan Relationships

Section 3: Policies/Testing Plans

This document provides the following sections to meet the requirements above:

- Business Impact Analysis
- In-depth Plan Policies
- Testing and Exercising Plan

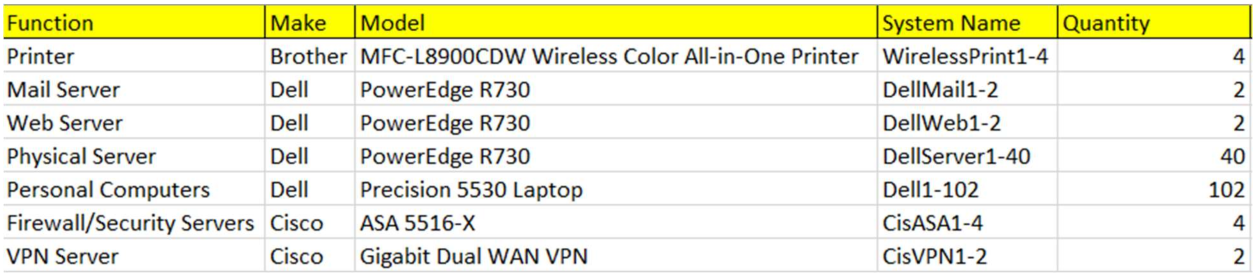
A. Business Impact Analysis

The Business Impact Analysis phase of Halcyon’s continuity planning process enables Halcyon to identify and prioritize essential functions, and then to conduct a systematic assessment of the resources (people, facilities, equipment, and records) required to support those functions.

The Business Impact Analysis focuses on identifying and evaluating key systems, data and infrastructure:

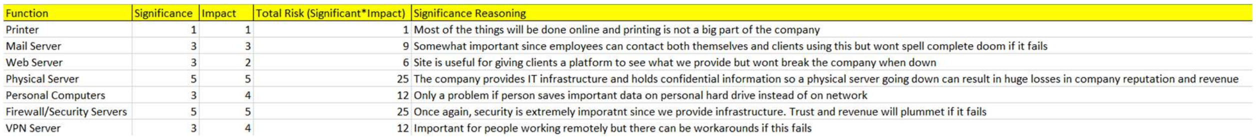
- Identify essential facilities, equipment, records, and other resources required to perform essential functions;

- Identify the vital records (files, documents, and databases) that must be protected and preserved; and
- The Recovery Time Objectives (RTOs) for each essential information technology system



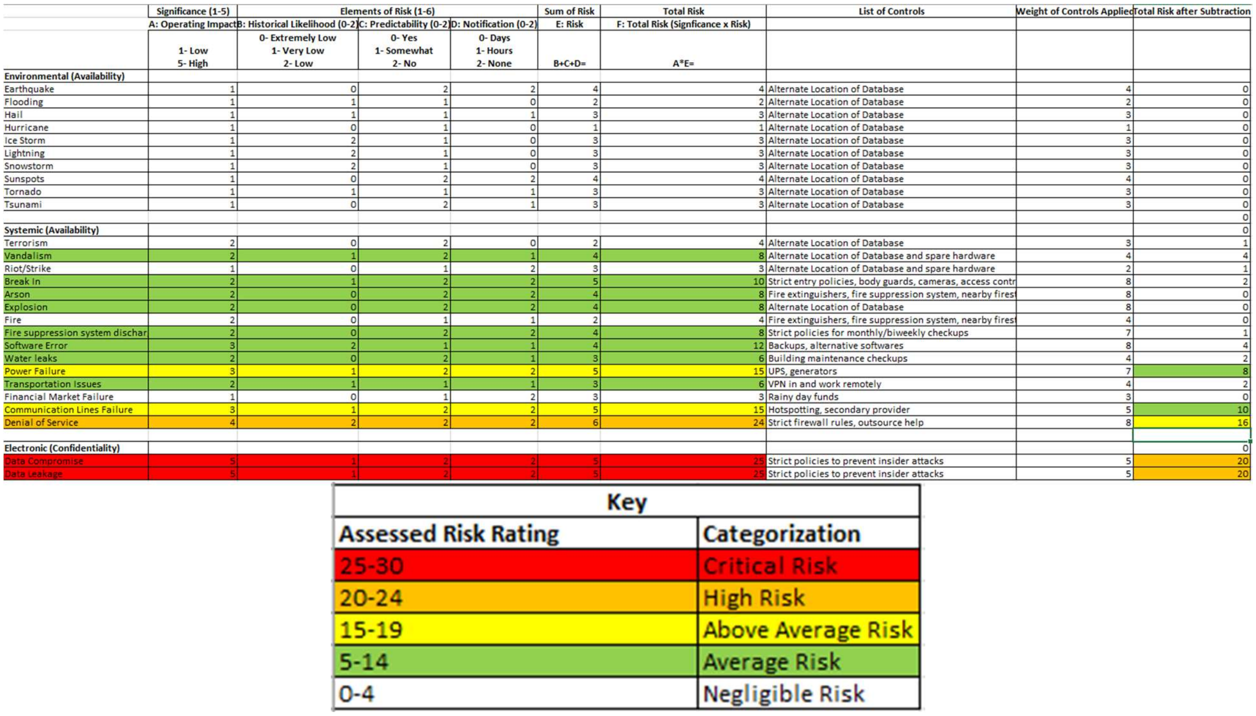
Function	Make	Model	System Name	Quantity
Printer	Brother	MFC-L8900CDW Wireless Color All-in-One Printer	WirelessPrint1-4	4
Mail Server	Dell	PowerEdge R730	DellMail1-2	2
Web Server	Dell	PowerEdge R730	DellWeb1-2	2
Physical Server	Dell	PowerEdge R730	DellServer1-40	40
Personal Computers	Dell	Precision 5530 Laptop	Dell1-102	102
Firewall/Security Servers	Cisco	ASA 5516-X	CisASA1-4	4
VPN Server	Cisco	Gigabit Dual WAN VPN	CisVPN1-2	2

Fig 3-1: Asset Inventory



Function	Significance	Impact	Total Risk (Significant*Impact)	Significance Reasoning
Printer	1	1	1	Most of the things will be done online and printing is not a big part of the company
Mail Server	3	3	9	Somewhat important since employees can contact both themselves and clients using this but wont spell complete doom if it fails
Web Server	3	2	6	Site is useful for giving clients a platform to see what we provide but wont break the company when down
Physical Server	5	5	25	The company provides IT infrastructure and holds confidential information so a physical server going down can result in huge losses in company reputation and revenue
Personal Computers	3	4	12	Only a problem if person saves important data on personal hard drive instead of on network
Firewall/Security Servers	5	5	25	Once again, security is extremely imporatnt since we provide infrastructure. Trust and revenue will plummet if it fails
VPN Server	3	4	12	Important for people working remotely but there can be workarounds if this fails

Fig 3-2: Significance, Impact, Reasoning for each



	Significance (1-5)	Elements of Risk (1-6)			Sum of Risk	Total Risk	List of Controls	Weight of Controls Applied	Total Risk after Subtraction
	A: Operating Impact	B: Historical Likelihood (0-2)	C: Predictability (0-2)	D: Notification (0-2)	E: Risk	F: Total Risk (Signficance x Risk)			
	1- Low 5- High	0- Extremely Low 1- Very Low 2- Low	0- Yes 1- Somewhat 2- No	0- Days 1- Hours 2- None	B+C+D=	A*E=			
Environmental (Availability)									
Earthquake	1	0	2	2	4	4	Alternate Location of Database	4	0
Flooding	1	1	1	0	2	2	Alternate Location of Database	2	0
Hail	1	1	1	1	3	3	Alternate Location of Database	3	0
Hurricane	1	0	1	0	1	1	Alternate Location of Database	1	0
Ice Storm	1	2	1	0	3	3	Alternate Location of Database	3	0
Lightning	1	2	1	0	3	3	Alternate Location of Database	3	0
Snowstorm	1	2	1	0	3	3	Alternate Location of Database	3	0
Sunspots	1	0	2	2	4	4	Alternate Location of Database	4	0
Tornado	1	1	1	1	3	3	Alternate Location of Database	3	0
Tsunami	1	0	2	1	3	3	Alternate Location of Database	3	0
									0
Systemic (Availability)									0
Terrorism	2	0	2	0	2	4	Alternate Location of Database	3	1
Vandalism	2	1	2	1	4	8	Alternate Location of Database and spare hardware	4	4
Riot/Strike	1	0	1	2	3	3	Alternate Location of Database and spare hardware	2	1
Break In	2	1	2	2	5	10	Strict entry policies, body guards, cameras, access contr	8	2
Arson	2	0	2	2	4	8	Fire extinguishers, fire suppression system, nearby firest	8	0
Explosion	2	0	2	2	4	8	Alternate Location of Database	8	0
Fire	2	0	1	1	2	4	Fire extinguishers, fire suppression system, nearby firest	4	0
Fire suppression system dischar	2	0	2	2	4	8	Strict policies for monthly/biweekly checkups	7	1
Software Error	3	2	1	1	4	12	Backups, alternative softwares	8	4
Water leaks	2	0	2	1	3	6	Building maintenance checkups	4	2
Power Failure	3	1	2	2	5	15	UPS, generators	7	8
Transportation Issues	2	1	1	1	3	6	VPN in and work remotely	4	2
Financial Market Failure	1	0	1	2	3	3	Rainy day funds	3	0
Communication Lines Failure	3	1	2	2	5	15	Hotspotting, secondary provider	5	10
Denial of Service	4	2	2	2	6	24	Strict firewall rules, outsource help	8	16
Electronic (Confidentiality)									0
Data Compromise	5	1	2	2	5	25	Strict policies to prevent insider attacks	5	20
Data Leakage	5	1	2	2	5	25	Strict policies to prevent insider attacks	5	20

Key	
Assessed Risk Rating	**Categorization**
25-30	Critical Risk
20-24	High Risk
15-19	Above Average Risk
5-14	Average Risk
0-4	Negligible Risk

Fig 3-3: Threat Assessment and Key

B. Incident Response Plan

An Incident Response Team will be implemented with defined rules and responsibilities to make necessary decisions if an incident were to occur. The reason for the defined rules and responsibilities is to ensure that these responsibilities take priority over their normal duties during an emergency. A classification system will also be implemented to categorize incidents and their severity to ensure proper responses and possible need for actions to be escalated.

Lastly, all parties that are covered by the policy should act accordingly and follow directions given by the Incident Response Team.

The term “incident” should be properly defined to put everyone on the same page. This is defined as any event that can be seen as adverse/irregular and involves the confidentiality, integrity, and availability of our systems and services. It is impossible to have one list to include all possible scenarios but some examples would include: attempts for an unauthorized user trying to get access to our systems or data, malware that can negatively impact our network, and attacks such as a DDoS attack.

The members of the Incident Response Team will include a chief risk officer, chief administrative officer, systems manager, operations officer, risk officer, information security officer, and corporate security officer. When reporting an incident, the level of security should be decided by either the information security or corporate security officer. They are also responsible for deciding if the severity level at any point should be elevated or downgraded. The three categories are listed below:

High level events can cause significant damage, corruption, or loss of confidential information, services, and infrastructure. Both public image and monetary loss can be experienced. Examples would include a DDoS attack, widespread virus infection, and unauthorized computer intrusions.

Medium level events would have a moderate impact on operations and reputation but still cause damage, corruption, or loss of replaceable information without compromise. Examples would include confined virus infection, unusual after-hour activities, and abuse of authorized access. Lastly, low level events simply cause inconveniences and minor costs to recover from. There is little to no impact on the operations and reputation. Examples would include sharing of passwords and simple policy violations.

All associates and third-party service providers are responsible for reporting any security problem in a timely manner. An Incident Event Form is available as a part of our Ticketing System.

There are four phases to incident response and escalation: identification, assessment, response, and follow-up. The first step is to recognize, report, and confirm an incident. The next step is to evaluate it by categorizing it with one of the severity ratings. The next step is to execute appropriate strategies. The last step is to correct damages, find vulnerabilities, mitigate/remedy them, and write a summary report. The information security officer and corporate security officer are responsible for initiating, completing, and documenting the incident response with the help of the Incident Response Team. The final report should include type of incident, response strategy, how it occurred, and recommendations for further prevention. If needed, cooperation with law enforcement is possible for certain events.

C. Disaster Recovery Plan

The incident commander is the Chief Information Officer and will be leading the Incident Command Team alongside the managers of all IT-related personnel that have been assigned to be a part of the team.

The Incident Command Team is in charge of the Datacenter Recovery Team which is composed of personnel within the IT department that supports the company’s central computing environment and primary datacenters where all central IT services, the Networks Operation Center, and other central computing resources are located. This team also supports the other datacenters outside the main headquarters. The primary function of this working group is the restoration of the existing datacenter or the activation of the secondary datacenter depending on the severity of the disaster. This team's role is to restore the datacenter to a condition where individual recovery teams can accomplish their responsibilities with regard to server installation and application restoration. The team lead has the responsibility to keep the IT Incident Commander up to date regarding the nature of the disaster and the steps being taken to address the situation.

The Work Equipment and Hardware Recovery Team is composed of personnel within the Information Technology department that support desktop hardware for associates and client applications. The primary function of this working group is the restoration of any systems and devices under their care. During the initial recovery effort, the team is not responsible for restoration of any data the user may have on their desktop computer. Halcyon recommends all users store data files on the file servers, which are backed up nightly, to support data recovery. The team lead has the responsibility to keep the IT Incident Commander up to date regarding the nature of the disaster and the steps being taken to address the situation.

The Enterprise Systems Recovery Team is composed of personnel within the Information Technology department that support the enterprise systems. The primary function of this working group is the restoration of all enterprise applications to the most recent pre-disaster configuration in cases where data or operational loss is significant. In less severe circumstances the team is responsible for restoring the system to functional status as necessitated by any hardware failures, network outages, or other circumstances that could result in diminished system operation or performance. The team lead has the responsibility to keep the IT Incident Commander up to date regarding the nature of the disaster and the steps being taken to address the situation.

The Infrastructure and Web Recovery Team is composed of personnel within the Information Technology department that support Halcyon's network infrastructure, including Active Directory, DHCP, DNS, email, file servers, network applications, network storage, server virtualization, and web services. The primary function of this working group is the restoration of our network infrastructure and servers to their most recent pre-disaster configuration in cases where data and operational loss is significant. In less severe circumstances, the team is responsible for restoring the system to a functional status as necessitated by any hardware failures or other circumstances that could result in diminished operation or performance. The team lead has the responsibility to keep the IT Incident Commander up to date regarding the nature of the disaster and the steps being taken to address the situation.

The Telecommunications, Network, and Internet Services Recovery Team is composed of personnel within the Information Technology department that support the organization's voice and data networks including cable plants, switches, and routers. The primary function of this working group is the restoration of our voice and data networks and Internet services to the most recent pre-disaster configuration in cases where operational loss is significant. In less severe circumstances, the team is responsible for restoring the voice and data networks and Internet services to a functional status as necessitated by any failures or other circumstances that could result in diminished operation or performance. The team lead has the responsibility to keep the IT Incident Commander up to date regarding the nature of the disaster and the steps being taken to address the situation.

D. Resource Requirements

A critical requirement for disaster recovery is ensuring that all necessary information is available to assure that hardware, software, and data can be returned to a state as close to "pre-disaster" as possible. This section covers the preparations required to ensure that recovery is possible. Backup/Recovery files are required to return systems to a state where they contain the information and data that was resident on the system shortly prior to the disaster. The following table shows the type of backups and where it will be stored.

Type:	Location:
Daily Backup	Datacenter, Cloud Provider
Weekly Backup	Datacenter, Cloud Provider
Monthly Backup	Cloud Provider, Off-site storage/datacenter
Annual Backup	Cloud Provider, Off-site storage/datacenter

Only the servers located in the datacenter are backed up; as such, only data resident on these systems will be able to be recovered. In the event that a disaster occurs onsite which destroys personal computers, the information located on these computers will be extremely difficult or impossible to recover. If recovery is possible, it will require outside vendor involvement at great expense to the user.

The Information Technology department recommends and encourages the use of network drives (on servers) to store all important files. The recovery of data not backed up to a network drive and/or full system backups are not covered under this plan.

In the event of any disaster which disrupts the operations in the datacenter, reestablishing the datacenter will be the highest priority and a prerequisite for any IT recovery. As such, the Information Technology department is required to have detailed information and records on the configuration of the datacenter and all servers and equipment located in the datacenter. Detailed information is documented in our monitoring system and infrastructure website.

In the event of any disaster which disrupts the network and/or telecommunications, reestablishing the connectivity and telephony will be a high priority and a prerequisite for any IT recovery. Recovery of these services will be accomplished in parallel or immediately following recovery of the datacenter. As such, Information Technology is required to have detailed information and records on the configuration of the networking equipment. Detailed information of switches and routers is documented in our monitoring system and infrastructure website.

Information necessary for the recovery and proper configuration of all application software located on the central servers is critical to assure that applications are recovered in the identical configuration as they existed prior to the disaster. Detailed information on critical central applications will be documented in our monitoring system and infrastructure website.

The infrastructure staff is responsible for keeping the hardware and software inventory up to date.

E. Business Continuity Plan

The strategy is to recover critical IT business functions at the alternate site location. This can be possible if an offsite strategy has been put into effect by Office Services and Disaster Recovery/IT Teams to provide the recovery service. Information Systems will recover IT functions based on the critical departmental business functions and defined strategies.

In the event of a disaster or disruption to the office facilities, the strategy is to recover operations by relocating to an alternate business site. The short-term strategies (for disruptions lasting two weeks or less), which have been selected, include:

Primary Location	**Alternate Business Site**
Chicago, IL	Downers Grove,IL or Conway, Arkansas
United Kingdom	Poland
Poland	United Kingdom

For all locations, if a long-term disruption occurs (i.e. major building destruction, etc.); the above strategies will be used in the short-term (less than two weeks). The long-term strategies will be to acquire/lease and equip new office space in another building in the same metropolitan area.

The activities necessary to recover from a Halcyon 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 Halcyon'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.

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

In the event of a facilities disruption, critical records located in the IT 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. IT 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. Testing and Exercising Plan

Regularly scheduled exercises are critical to ensure that the Contingency Plan can be executed in times of an emergency. Exercising is one of the most effective ways to discover and document necessary modifications. The testing and exercise plan will be progressive, building from simple, individual tests to complex, functional exercises. The plan will include activities that build on training and improve capabilities through a series of tests and exercises.

Testing is required to demonstrate the correct operation of all equipment, procedures, processes and systems that support the organization's essential functions. Test exercises are conducted to validate elements of the Contingency Plan, both individually and collectively. Exercises should be realistic simulations of an emergency, during which individuals and agencies perform the tasks that are expected of them in a real event. Exercises should promote preparedness; improve the response capability of individuals and participating agencies; validate plans, policies, procedures, and systems; and verify the effectiveness of command, control, and communication functions. Exercises may vary in size and complexity to achieve different objectives.

Halcyon's testing and exercising plan will follow the schedule and adjust accordingly based on needs and schedules of all staff involved:

Type:	Schedule:
Tabletop	1st Wednesday every month
Functional	2nd Tuesday every 3 months
Full-Scale Functional	3rd Thursday every 6 months

Section 4: Revision History

Date	Version	Requester	Tech. Writer	Change/Review
5/9/19	1.0	Tim Kang	Timothy Kang	

Modified by: _____________Timmy Kang_____________________________ ______5__/__9__/_19____

Reviewed by: ____________Timoteo Kang____________________________ _____5__/__9__/_19____

Approved by: ____________Definitely not Tim Kang___________________ ______5__/__9__/_19____