Risk Management Plan
Health Network
2022

1.1 Introduction

Health Network and its senior officials have established a new Risk management plan, designed to reevaluate and reestablish a new security infrastructure for our organizations information systems. A risk management plan is needed to identify and evaluate risks to properly maintain the efficiency of our organization.

We encourage everyone, especially those in management, to be proactive instead of reactive. This risk management plan will help give an idea to those working with information systems here at Health Network, an approach to combat any threat or risk presented. Working at Health Network, we are committed to following security guidelines and protecting the confidentiality, integrity, and availability of our, and our customers' data.

1.2 Purpose

Our purpose for this plan is to encourage a lifestyle of managing risk here at Health Network. When all employees look at problems from a risk management approach, the better we are for protecting our critical data and also for our customers. We want to maintain all risks, internal and external, to provide better service to our partners. This risk management plan will examine risk assessments, risk mitigation plans, and business continuity plans.

1.3 Scope and Boundaries

After thorough review of Health Networks information systems and networks, we have found new risks that could potentially cause harm if not dealt with or mitigated. This risk management plan will cover the following details :

- **Identifying Compliance Regulations**
- **Identifying Risks and Threats including Risk Assessment**
- **Identifying Risk Mitigation Methods**
- **Business Impact Analysis and Business Continuity Plan**
- **Schedule of Risk Management Plan**
- **Key roles and responsibilities of Risk Management Plan**

The scope of this Risk management plan is to detail newly founded risks and to deal with them that will accumulate the least amount of risk. This risk management plan will also cover suggestions on what to do if/when a risk is imposed against Health Network systems. The risk management plan will detail Health Network Risk Assessments, Risk Mitigation Plan, Business Continuity Plan and the key roles and responsibilities of individuals as well as a schedule for the risk management process.

1.4 Governance and Compliance Regulations

Health Network aims to keep the confidentiality, integrity, and availability of critical data. As an organization dealing with healthcare information, we must provide secure handling of such information. Many governance and compliance regulations are put in place by our government to ensure that the health information being dealt with daily is properly maintained and secure. We seek to comply with such regulations, including :

- **HIPAA - Health Insurance Portability and Accountability Act**
    - **protect sensitive health information about people by not disclosing it to others without the patient's consent.**
- **PCI DSS - Payment Card Industry Data Security Standard**
    - **Protecting the data information of customer transactions including credit card data.**
- **FISMA - Federal Information Security Management Act**
    - **Complying with regular risk assessments, reducing risk of threats/vulnerabilities along with compromised data. Meeting FISMA requirements is essential in progressing the growth of Health Network.**
- **NIST SP 800-53**
    - **Established framework that most organizations have required. The NIST SP800-53 provides a great and useful framework for complying with, securing, and managing critical data.**

Working for an organization that primarily deals with healthcare data of individuals, it is crucial Health Network not only recognizes but conforms to these standards. These standards offer a variety of steps that will help maintain the core infrastructure of data security.

2.0 Risk Assessment

Risk assessment approaches consist of 3 different perspectives for how an organization may want to pursue their risk assessment. These include a quantitative, semi-quantitative, and qualitative approach. Qualitative approaches offer a more scaled, however subjective, approach to assessing risk which includes measurement of risk probability and impact. Quantitative covers more of the monetary side of things in a risk assessment such as single loss expectancy, annual rate of occurrence and control value. For this risk assessment, we will be conducting a qualitative approach.

Starting off, we will provide a basic guide for the overall outline of the risk assessment we have created. The risk assessment will start with an introduction, explaining the details of what a risk assessment is, what it carries out and how that is important to sustaining the daily operations here at HealthNetwork. Secondly, we will detail the overall scope and boundaries of this risk assessment. Next, we will lay out all of the assets and activities that lie within the scope of the risk assessment, its function and the manner we will go about assessing it. Following that, we will detail the threats and vulnerabilities and how we will go about assessing those found.

Next, we will assess the controls found at HealthNetwork that pertain to this risk assessment. After that, we will analyze and identify the roles of different members at HealthNetwork in accordance with the risk assessment. A proposed schedule for the risk assessment will be laid out with the overview of the assessment detailed at the end, which will include a table for referencing.

Here at HealthNetwork, we are dedicated to sending, receiving, and managing health information for many Americans in a secure and effective manner. In accordance with the Health and Safety at Work Act, we are required to perform regular risk assessments to maintain the confidentiality, integrity and availability of information by our customers and employees. Risk assessments are conducted by almost every company and it is crucial in cybersecurity. Risk assessments are often conducted due to new equipment, new software, new procedures, or during any big change in a company. Risk assessments identify which assets are crucial in protecting, give us insight to which controls provide the most value and help us determine the quantitative or qualitative value for risks.

2.1 Scope of Risk Assessment

The scope for this risk assessment will help establish what will be considered in the assessment. The scope of this risk assessment will include the following :

- Identification of key assets
- Identification of controls
- Identification of threats and vulnerabilities located inside of HealthNetworks' networks.
- Identification of roles and responsibilities pertaining to each risk
- Identifying risk likelihood and impact
- Proposed scheduling

The risk assessment must stay within the scope laid out to avoid any negative impacts on policy or operations here at HealthNetwork.

2.2 Identifying Data Center Assets and Activities

At HealthNetwork, we operate 3 different corporate locations, each operating in different locations which include Minneapolis (main headquarters), Portland, and Arlington. Each one supports a mix of corporate operations. With each corporate location, there is a nearby data center where production systems are located and are managed by third-party vendors. The data centers identified are crucial to keeping daily operations functioning and are considered assets to HealthNetwork. The data that is stored at our data centers are also very valuable assets and must be protected. Other assets include software, such as online directories/web portals, corporate-owned laptops/workstations, production systems, data storage, data servers, web servers/applications and IPS/IDS systems.

Data centers offer storage of highly critical information and operations. As a company in the healthcare industry, keeping this information confidential is very important for our company's reputation. Our data centers also provide us with availability of such sensitive information for our customers.

2.3 Identify Relevant Threats and Vulnerabilities

Risk assessments involve identifying current and possible future threats and vulnerabilities found within HealthNetworks' networks. Our team works to identify these threats and classify the overall likelihood and impact of these known threats. The list of threats identified include the following :

- Disgruntled employees
- Inclement Weather
- Internet Threats (Attackers)
- Possible insider threats
- Physical attacks (illegal entry, stealing corporate owned devices)

Vulnerabilities include any liability found in the security operations at HealthNetwork that can be attacked by a threat. Our security team works to find any known vulnerabilities and take the best course of action to mitigate them. Vulnerabilities not only exist in cyberspace, but also in the organizational/structural side. Such vulnerabilities found include :

- Lack of physical security on corporate owned laptops
- Customer security
  - Lack of information security on customer-side can potentially cause any threat to attack our networks.
- External service providers
- Human errors
  - Includes software errors/bugs, physical access controls, social engineering attacks, misclicks, organizational structure.
- Physical Data Centers
  - In the scenario of natural disaster or inclement weather, this could potentially have disastrous effects on operations.
- Lack of management/employees
- Hardware failure

2.4 Identifying controls

Risk assessments help identify which controls work best, given the scenario and infrastructure they are set in. Identifying controls with vulnerabilities and threats allows for management to get a better look at which controls can help mitigate risk and allow for safest operations. When an organization makes certain changes, some controls can become inadequate and thus require assessment. Security controls tend to lose their effectiveness over time which is why risk assessments must be done. Controls can include a range of proactive measures taken to accommodate or reduce risks, such as physical controls, technical controls or procedural controls. All controls laid out are relevant to our organization and will need to be assessed.

Physical controls include all controls that are used to help secure the physical environment. These include :

- Locked doors
- Security Guards

- Video cameras
- Access logs
- Circuit breakers

Technical controls involve any control that is implemented on a computer to help protect the confidentiality, integrity, and availability of information. These include :

- Firewalls
- Encryption
- Session time-out
- Input validation
- Log on access methods (Authentication)
- Monitoring

Procedural controls are controls implemented through organizational structure and management. These controls include :

- Policies/Procedures
- Training
- Insurance
  - Mostly for natural disasters such as fires and floods.
- Security plans

2.5 Key Roles and Responsibilities for Risk Assessment

Identifying the roles and responsibilities for individuals is important in conducting risk assessments. The roles are established to give guidance for what individuals should be focusing on. Without identifying roles, such policies, risk management plans, risk assessments and other organizational policies would be chaotic and would give threats a vulnerability to attack, as mentioned previously.

For this risk assessment, Tier 1 is responsible for conducting risk assessments when needed, which will be mentioned later. Tier 1 is also responsible for evaluating information associated at organizational/architecture levels. Tier 2 will evaluate information associated with mission/business processes and funding for other information security resources. Tier 3 is responsible for implementation of controls, monitoring, and assessing risk.

Head of agencies, Chief executive officers and chief operating officers are responsible for authorizing and having oversight of risk assessments.

Information owners and authorizing officials are responsible for conducting mission/business functions pertaining to Tier 2 activities.

Program managers, information security architects and engineers are responsible for development and overall implementation of controls.

2.6 Scheduling for Risk Assessment

For this risk assessment, a good time-frame for implementation of said procedures should depend on the underlying risk involved. For higher overall probability risks, these should be implemented within weeks to prevent any unwarranted attack on our networks. Other controls, such as certain physical controls, can and may take a few months to implement.

- Risk assessments should be conducted quarterly, if no controls and/or business functions have been changed.
- Controls should be regularly monitored to determine the impact it has on business operations.
- Newer controls should be monitored for 60 days before any decision is made on implementation.
- Risk assessments must be produced and conducted 30 days after presentations.
- Decisions made about the risk assessment must be made within 21 days following the presentations.

2.7 Risk Assessment Report

It is in our best interest here at HealthNetwork, to find the best practices for maintaining the confidentiality, integrity, and availability of data to maintain normal business operations. In this risk assessment, we have found different threats, vulnerabilities, controls as long as recommendations to those findings. The table below gives us a scale on the vulnerabilities, showing the probability and impact of each.

Probability	Impact				
	Very Low	Low	Moderate	High	Very High
Very Likely	High	High	Very High	Very High	Very High
Likely	Moderate	High	High	Very High	Very High
Moderate	Low	Moderate	High	Very High	Very High
Unlikely	Low	Low	Moderate	High	Very High
Very unlikely	Low	Low	Moderate	High	High

Threat Source	Vulnerability
Hacker	Open Ports/ Bad Firewall Configuration
Insider Threat	Lack of Access Controls
Inclement Weather	Backups/Power Outages
Hacker	Vendors/Customers
Attacker	Employee using laptop
Employee	Misclicks/Software errors

Such vulnerabilities can be mitigated by implementing certain controls. Starting off, we can make sure that employees at Tiers 2 and 3 level use access control methods, such as password policies and ID cards to ensure that employees only have access to things they need. Second, make sure that unused ports are closed to prevent any attacker from trying to attack those ports. Ensure hardening of all firewalls and workstations. As a healthcare company, we must ensure that data is being transmitted securely and that data is encrypted at all times. We can also implement spam detection in our networks to prevent any malware or virus intrusion in our systems from an employee. This will drastically reduce the chance of a social engineering attack on our employees. Next, we can institute input validation on our software and systems to ensure that accidental human errors are accounted for, thus resulting in no risk from employees. Natural weather conditions disrupting our operations may be something upper management would like to discuss as to what to do with it.

3.0 Risk Mitigation Plan

Risk mitigation plans seek to identify risks associated with data, networking, and physical risks (including natural disasters). This risk mitigation plan will cover all risks and/or vulnerabilities identified in the risk assessment report that was released earlier this year. The risk mitigation plan also looks to dampen or lessen the impacts associated with each risk. Although it is important for our organization to cover specific elements associated with IT security, such a plan must also commit to broadening the scope of security at an organizational level (e.g. physical access controls).

3.1 Identifying Assets

One of the fundamental steps of building a proper risk mitigation plan is to start off by identifying our organizations assets. Listing off assets helps value our assets on a low-medium-high scale. Identifying assets also helps to provide a guideline of which assets to protect in the organization. Assets found here at Health Network include :

- Data servers/data storage **- High**
- Application servers **- High**
- Online directories and web portals **- High**
- Corporate owned laptops/workstations - **Medium/low**
- IPS/IDS **- High**
- Off-site data centers **- High**
- Third-party vendors **- High**
- Corporate locations **- High**
- Personnel - **Medium/High**

These assets identified are critical in maintaining the security operations here at Health Network. We can see that many Health Network assets possess a high value that is crucial in performing daily security operations. Although assets such as workstations and laptops aren't high in monetary value, protecting these will help keep the CIA triad for protecting data. Certain assets not located on company premises, such as off-site data centers and vendors are very important to protect to keep data protected.

3.2 Identifying vulnerabilities for Each Asset

According to NIST SP 800-53, different questions should be asked for each asset regarding the threats and vulnerabilities pertaining to each. We can also look at each control family given to us by NIST to further examine how and what control to implement. It is important to first identify the risks imposed by each asset to get a better look at what controls to implement regarding each risk.

- Data servers/storage and Application servers
    - Potential hardware failure resulting in server downtime.
    - Attacks on data servers which could lead to loss of confidential information
- Corporate owned laptops
    - Lack of physical security
- Corporate workstations
    - Software/Human errors
    - Open unsecure/unused ports
- IPS/IDS
    - Improper configuration
    - Hardware failure
    - Backups to use in a case of emergency
- Data centers
    - Physical security
    - Inclement weather or natural disasters
    - IT security

- Vendors
    - Lack of security
    - Product failure
- Corporate locations
    - Physical security
    - Natural Disasters
    - Organizational structure
    - Disgruntled employees/Insiders attacks
    - Social Engineering attacks
- Personnel
    - Malicious employee
    - Lack of personnel
    - Human errors (misclicks, software bugs, victim to social engineering attacks)

This list of vulnerabilities for each asset will help provide an idea for a list of controls to implement for each asset. It is very important for Health Network to keep these assets safe and secured as well as running to prevent serious loss. We can see here that vulnerabilities do not only refer to the IT side of our organization, however, they present themselves in physical form as well.

3.3 Control Evaluation and Implementation

NIST SP 800-53 gives us a list of different security control families pertaining to the security of Information Systems. In order to attain our security operations, controls must be implemented to lessen the impact of the risks/vulnerabilities listed earlier. After thorough review of risks/vulnerabilities associated with each asset, the following controls will be implemented :

Data servers/storage and Application servers

- Maintenance - Schedule, document and review all records of maintenance for the servers and storage devices to ensure that they work properly.
- Systems and Information Integrity - provides malicious code protection, software protection and firmware integrity across data servers to provide a more enhanced security to keep these servers running.
- System and Communications protection - serves to provide protection for information at rest.

Corporate Laptops

- Physical and Environmental Protection - provide laptops with physical securities such as tracking devices so that devices stolen can be traced and reported.

Corporate Workstations

- Access Control - this control family consists of providing forms of access controls to prevent unauthorized use of corporate workstations.
- Risk assessment - provides controls used for vulnerability scanning and measures in-place controls to see the impacts they make for information systems.
- Audit and Accountability - provides workstations with sets of controls used for auditing, audit reports and protection of audit information.
- Configuration Management - configuring workstations to close or open ports, encryption.

IPS/IDS

- Configuration Management - provides controls specific to those that are listed in the configuration management policies.
- Audit and Accountability - will help utilize the ability to audit for IPS and IDS systems
- System and Information Integrity - will provide security alert controls and system monitoring.

Data centers and Vendors -

Since 3rd party vendors and data centers are not part of our organization's policies, our team has managed other ways to provide certain controls to make sure that the organizations we work with are self-sustaining in security. Tools such as Black Kite allow us to get ratings for other organizations' security. Other things we can and will do is get audits, compliance regulations and security checks from these companies to make sure that they do not present a weak link in our security.

Corporate Locations

- Physical and Environmental Protection - physical controls such as locked doors, security cameras and access logs.
- Identification and Authentication - doors will be equipped with card readers like biometrics or keycards in order to access rooms or buildings.

Personnel

- Awareness and training - personnel must be equipped with proper training to enhance security culture at Health Network.

- Identification and Authentication - personnel must be equipped with a keycard that identifies themselves.
- Personnel Security - controls implemented from this family will consist of background screening, transfers and terminations.

3.4 Final Report for Risk Mitigation Plan

To start off, we have presented our list of assets that pertain to our Information Technology operations. Such assets include our data servers, data storage, file servers, application servers, laptops and workstations, IPS/IDS systems, data centers and 3rd party vendors, our own corporate centers and our personnel team. These assets identified present a huge role in keeping the data being traveled through and from our networks safe.

Secondly, we have identified vulnerabilities, threats and risks pertaining to each asset. In order to keep the normal security operations at Health Network, we must be able to have the risks for each asset set to a minimum as much as we can.

Asset	Risk	Threat	Vulnerability
Data Servers/Storage	Loss of confidential information	Attackers Disgruntled employee Natural events	Misconfiguration in firewalls, IPS or IDS systems, hardware failure or outage
Laptops/Workstations	Loss of information, leaked information. Can lead to loss of other assets inside of network	Physical Attackers or hackers	Lack of physical security on laptops
IPS/IDS	No incident response or detection	Attackers, power outages/natural events	Misconfiguration, hardware failure
Data Centers and Vendors	Can pose as a weak link in our security	Attackers	Lack of security on customer or client-side
Health Network Locations	Downtime on our servers, insider	Natural events Physical attackers	Lack of physical access controls

Asset	Risk	Threat	Vulnerability
Data Servers/Storage	Loss of confidential information	Attackers Disgruntled employee Natural events	Misconfiguration in firewalls, IPS or IDS systems, hardware failure or outage
Laptops/Workstations	Loss of information, leaked information. Can lead to loss of other assets inside of network	Physical Attackers or hackers	Lack of physical security on laptops
	attacks, social engineering		
Personnel	Errors can present flaws in security operations	Attackers, disgruntled employees	Human errors Misclicks Misconfigurations

This table lists off some of the threat/vulnerability pairs for each asset along with the risk it poses on our daily functions and what we want to keep protected. For this risk mitigation plan, we have come up with a list of security controls, as provided by NIST SP 800-53 for each asset. Each control will be carefully monitored and assessed periodically. If the control does not provide enough protection, nor show any improvement from previous controls, we can reassess the controls for the asset. Our security team has gone through each risk posed by the vulnerabilities and has detailed how to mitigate those with different controls.

For our data, file and application servers, we can mitigate a lot of the risk by having near constant maintenance for the physical servers, along with encrypting nearly all data located on the file servers. We can also implement a secure firewall between each server from the LAN and WAN so that any attacker will have trouble gaining access to these servers. We can also implement power generators so that in any case of power outages, our servers don’t suffer much downtime.

The laptops and workstations owned by our organization do not present a high monetary value, however, they are valuable to our operation. Laptops given to remote employees have significant vulnerabilities, such as being stolen. Physical controls, such as locks or trackers can help locate the stolen device. Our workstations also need controls, that being access controls, configuration management, and auditing. These are all crucial in preventing unauthorized access to machines and networks owned by Health Network.

Intrusion Prevention Systems help prevent an attacker from making their way into our networks. Intrusion Detection systems only alert when an attacker is trying to get in. These systems are crucial for our security at Health Network. In order for these systems to work the way we would like them to, these systems must be configured properly. Having a group or small team of people to configure these IPS and IDS systems will be more effective in reducing the errors of misconfiguration, misclicks and other modes of human error.

Health Network uses multiple data centers and 3rd party vendors. These other organizations can present themselves as weak links to our security so it is important to make sure these data centers and vendors have up-to-date security placed into their infrastructure. Tools such as Black Kite can provide organizations with ratings of another organizations security.

Our corporate locations are all located in areas where inclement weather, power outages, and natural disasters are all possible. It is also to have physical access controls, such as locks, security cameras, guards and key card readers for certain personnel. We must also put in place other forms of control to help mitigate natural disasters like generators and storage back-ups.

4.0 Business Impact Analysis / Business Continuity Plan

4.1 Purpose of Business Impact Analysis (BIA)

The Business Impact Analysis (BIA) is a big part of contingency planning for Health Networks data center. This specific BIA will focus on all components and systems with Health Networks data center.

The purpose of conducting a BIA is to identify and highlight the system components that play a critical role in Health Networks mission/business processes. BIA’s also use that information to create impact values on the processes if the identified components were not available. Most BIA’s follow 3 steps which include :

- **Determining mission/business processes and recovery criticality.** In this step, system resources/components that help with the mission/business processes are identified. Impacts of system disruption on those processes are identified and values are determined depending on severity. Other details in outage impacts are included, such as MTD, RTO and RPO.

- **Identifying requirements for resources.** Resources required to resume the mission/business processes are identified.
- **Prioritizing recovery for system resources.** After identifying required resources to restart the mission/business processes, the resources are then allocated to more prioritized/critical processes.

4.2 Critical Business Functions

Health Network has 3 operable data centers all located next to each one of our corporate facilities. Each data center hosts production systems that are all managed by third-party data center hosting vendors. Including all 3 data centers, there are roughly 1000 production systems in total. These data centers play a huge role in Health Network mission/business processes. Some critical business functions of these data centers are :

Mission/Business Process	Description
Maintaining HNET products	The process of keeping the availability of HNet products available for its customers.
Securing medical messages	HNetExchange is the primary source of revenue, which involves securing medicale messages that come from hospitals and clinics.
Securing and processing payments	HNetPay is used to accept forms of payments and interacts with credit-card processing organizations

Table 1-1

4.2.1 Identifying Critical Resources

The following table lists resources that are needed and used in order for data centers to perform their role in Health Networks mission/business processes.

Table 1-2

Resource/Component	Description
Routers/Switches	These devices are important for connecting to other data centers, corporate locations, other devices within

	the data center and internet connectivity.
Web Servers	Hosting websites/portals for Health Network customers to use.
Storage Systems	Storage of critical files including health and credit card information.
Firewalls	Uses rules to keep certain internet addresses from being able to connect with systems located inside of data centers.

4.2.2 Identifying Outage Impacts

The following impact categories were created to represent areas of consideration in the event of a disruption.

Impact Categories :

- Cost - this impact category refers to costs that Health Network needs to make based on the event.
  - Severe - costs of repairing, replacing, rebuilding and fees are projected to total over $1 million.
  - Moderate - all costs associated with the disruption total to $500,000.
  - Minimal - costs associated with the disruption total to $100,000 or under.
- Safety - refers to the overall safety of medical and financial information that hospitals and clinics use.
  - Severe - loss of multiple customer files and/or loss of confidentiality of those files.
  - Moderate - loss of a singular file. Some impact to overall confidentiality, integrity, or availability of other files.
  - Minimal - no data loss. Minimal impact overall of the confidentiality, availability, and integrity of files.

The table below refers to the impact of each process if, for example, storage systems unexpectedly malfunctioned.

Table 1-3

Mission/Business Process	Impact Category		Impact
Maintaining HNet Products	Cost	Safety	Severe
Securing Medical Messages	Cost	Safety	Severe
Securing Payments	Cost	Safety	Severe

The impacts could be severe depending on how long the storage systems are down for, which will be covered later. Storage systems play a very big role in the processes that Health Network provides to hospitals and clinics throughout the country. Newer files being put into the system while it is down would not be found and this could end up costing Health Network lots due to fines from regulatory violations or intangible values from things like losing customers due to bad service.

4.2.3 Estimated Downtime

Estimated Downtime refers to the goals and objectives that our organization gives the mission/business processes to get back up and running after a disastrous event. Things like MTD, RTO, and RPO correlate directly with downtime.

Maximum Tolerable Downtime (MTD) - Maximum tolerable downtime refers to the total amount of time that business leaders/managers are willing to accept for a mission/business process outage.

Recovery Time Objective (RTO) - refers to the maximum amount of time that a mission/business resource is allowed to be down until it starts unacceptably impacting other resources.

Recovery Point Objective (RPO) - refers to point in time, prior to an outage, to which mission/business process data must be restored after an outage.

The table below shows the MTD, RTO, and RPO for each mission/business process found in **Table 1-1.**

Mission/Business Process	MTD	RTO	RPO
Maintain HNet Products	18 hours	8 hours	6 hours
Securing medical messages	18 hours	8 hours	6 hours
Securing payments	18 hours	8 hours	6 hours

4.3 BCP

Business Continuity Plans can be thought of as a guide to follow if an organization were to face something catastrophic. Such catastrophes can include:

- Winter snow storms
- Power Outages
- Lack of employees being able to get into the offices

4.3.1 Planning

As snow storms continue to ramp up in the east coast, we can safely assume that such storms can cause serious damage over the period of a week. For a period of a week, Health Network will need necessary supplies so that our organization can continue to operate for a week period in the worst case scenario.

4.3.2 Incident Response/Strategy

Snow storms in America are often recognized quickly and weather reports are able to guide judgment on how harsh and when a snow storm may come. Depending on severity and how quick it may come, Health Network BCP coordinators should start preparing in response to a snow storm. Any storm that is likely to accumulate over 1 foot of snow will allow BCP coordinators to enact the BCP plan. Coordinators should contact Health Network’s transportation to shuttle employees.

First, all employees will be notified of the response to the storm. Employees in the offices will be notified. All employees should be allowed to return home while other higher levels of management should be in charge of the building, power, and their own department. Groups of IT employees will stay to prepare for disastrous events that may occur in the organization's networks. All work will be shifted to an online setting until the snow storm resides, unless otherwise stated. Other works that are needed in-person must resume regular schedules. If driving conditions are poor, groups of employees will be set to stay in the building.

Critical resources mentioned in the BIA, noted above, will be carefully examined by officials. IT personnel will respond accordingly to the incident. Backups should be done every 6 hours.

4.3.3 System Description and Architecture

Health Network consists of 3 different corporate locations each with a nearby data center consisting of nearly 1,000 production systems. The Arlington location is the primary location for business units. Each corporate location is able to connect to the other 2 locations. Each corporate location center is able to communicate with their nearby data center via VPN. There are currently no locations making backups.

4.3.4 Phases

96 hours before	Notify all personnel that a snowstorm is likely to hit within the next couple of days. Review BCP.

72 hours before	Review supply list. Gather all supplies necessary stated in the BCP. Review steps and responsibilities of BCP.
48 hours before	Release all employees that are non-essential. All work activities will resume online. Test backup generators. Notify employees that will be working on-call in the snowstorm.
24 hours before	Bring in the group of employees including all team members. Follow BCP.

The first phase will consist of activation of the BCP and notifying team members and leaders. Depending on how quickly and how bad the snowstorm is, DAT and EMT members will be located in the building and carefully assessing any damages to resources.

The second phase will occur after a majority of the storm has passed. This will be the recovery phase. All damage assessed will be taken care of by the TRT, in which they will respond according to the resources mentioned in the BIA.

Lastly will be the reconstitution phase in which all operations will return to normal. This phase will be implemented after the storm has completely resided and all employees are able to return to work.

4.3.5 Plan Training, testing and exercises

Testing is an important aspect of BCP's to get a look at exactly how the flow of the BCP will work. If the plan isn't tested, it could cause even more disaster than the disaster itself. The BCP will be tested, at least 3 months prior to the latest update made. To plan, IT members will shift the work online to ensure that services and connections can remain stable even in a simulated setting where certain servers can go down. This will ensure that even in snowstorms, work can remain to get done. Other team leaders and coordinators will continue to work as they would during an event and plan things accordingly. Any personnel assigned a responsibility who fails to be able to keep up will be released from the role and assigned a different position that is better fit for them. Every once in a while, certain employees can volunteer or will be asked to participate in testing to see who is best fit for the role. Any negative aspects of the plan should be reviewed and assessed carefully and changes should be made.

4.3.6 Plan Maintenance

Revisions and updates on the BCP should be done twice a year. All changes should be documented by the BCP coordinator. Every few months, the BCP should be reviewed and likewise, training and testing should be conducted. Always review the BCP after any substantial change in the IT department and depending on the change, make adjustments that are needed.

1.5 Key Roles and Responsibilities

Identifying key roles and responsibilities in the infrastructure is just as crucial as having a plan. Without proper tasks being managed correctly, we reduce our security and increase our chance of being attacked. Proper duties will be assigned to groups of employees, depending on the tier they are in.

Tier 3 employees, those working with information systems directly, will be tasked to follow the decisions of upper management, Tiers 1 and 2. These individuals may be responsible for :

- Deploying Risk Methods
- Identifying Risks
- Reporting Risks
- Assessing the risks

Tiers 1 and 2 will work together to come up with the best route, in terms of security and cost, to lead Health Network to acceptable amounts of risk. Tier 2 will be more responsible for budgeting, BCP's, and other tasks pertaining to business financials. Tier 1 will be primarily responsible for enforcing the structure outlined in this Risk Management Plan, along with other policies, guidelines and rules. Tier 1 officials may also be responsible for accepting any risk, as all plans are passed to Tier 1 officials for permission.

1.6 Schedule for Risk Management Plan

Scheduling for variations of tasks is important for having a smoother and more reliable Risk Management Plan. If tasks weren't done in a specific period, our risk levels could potentially increase. We want to mitigate and lessen the chance of risk around the board.

- **Compliance Laws : Regularly train employees on the list of Compliance Regulations Health Network is subject to. Training can be completed after 45 days.**
- **Identifying and Reporting Risk : It is important that communication between all levels is held. Identification and reporting of risks are important for keeping our risk levels acceptable. 24/7 monitoring is important for identifying. Report all found risks immediately.**
- **Risk Management Plan : It is important as an employee at Health Network that you are constantly following the RMP. If RMP were to pass, this would be effective immediately.**

- **Risk Mitigation : Following new reports, upper levels are responsible for making the decisions. New recommendations and controls following a report should be conducted 5 days after. It is important to take a proactive measure for assessing and mitigating risk.**
- **Business Continuity Plan : Coordinators for this plan must test the plan at a minimum of once a month. Any problems noted after testing must be brought to management. BCP's should be reviewed every 6 months and should be updated after review.**

Works Cited

- [0]Darell Gibson, Andy Igonor. 2010. Managing Risk in Information Systems.(September 02, 2010). Retrieved November 30, 2022 from Jones & Bartlett Learning Navigate 2 (jblearning.com).
- [1]National Institute of Standards and Technology. NIST. Contingency Planning Guide for Federal Information Systems. (May, 2010). Retrieved December 2, 2022 from SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems | CSRC (nist.gov).
- [2]National Institute of Standards and Technology. NIST : Security and Privacy Controls for Information Systems and Organizations. (September 2020). Retrieved November 10, 2022 from Security and Privacy Controls for Information Systems and Organizations (nist.gov)
- [3] Justin Peacock.CyberSaintIO : NIST SP 800-53 Control Families Explained. Retrieved November 10, 2022 from NIST SP 800-53 Control Families Explained (cybersaint.io)
- [4]Haspod. 2019. Are Risk Assessments a Legal Requirement? (June 19, 2019). Retrieved October 08, 2022 from Are Risk Assessments A Legal Requirement? - HASpod
- [5] National Institute of Standards and Technology. NIST : Guide for Conducting Risk Assessments. (September, 2012) Retrieved October 07, 2022 from NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments

- [6] Heather Devane. 2021. The Complete Guide to Data Security Compliance Laws and Regulations. (June, 2021). Retrieved September 19, 2022 from https://www.immuta.com/blog/the-complete-guide-to-data-security-compliance-laws-and-regulations/#:~:text=Common%20 Compliance%20Laws%201%20 GDPR%20The%20European%20Union,4%20HIPAA%20...%205%20FISMA%20...%20More%20items
- [7] Incorporated Zone. 2020. What is Data Compliance (Regulations and Standards)? Retrieved from https://incorporated.zone/data-compliance/#:~:text=What%20are%20some%20data%20compliance%20laws%20and%20regulations%3F,stands%20for%20the%20California%20Consumer%20Privacy%20Act.%20
- [8] National Institute of Standards and Technology. NIST: Risk Management Framework for Information Systems and Organizations. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf