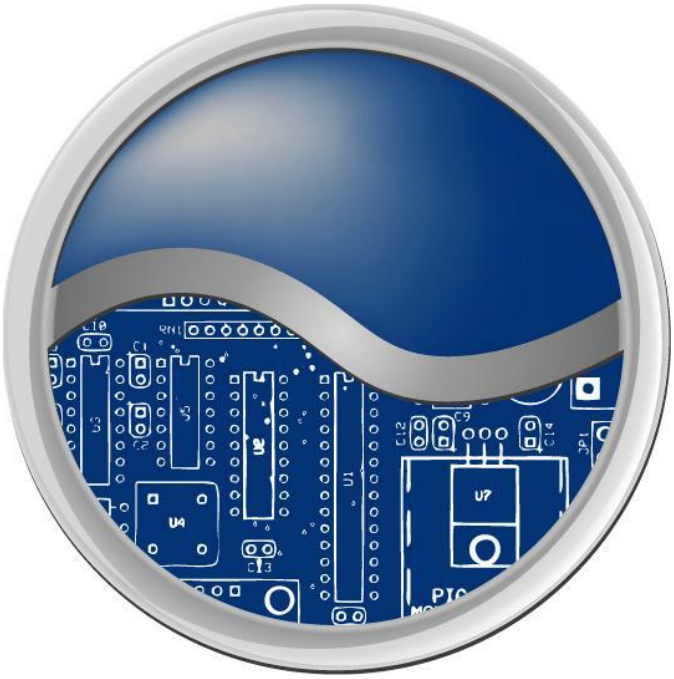

Information Security & Disaster Recovery Plan For Happy Haven Daycare Centers, LLC

Presented by; Norm Coleman

Network Solutions, Inc.

COMN-228 –Winter 2012

Table of Contents

Introduction –Risk Statement

Network Solutions has created this Risk Statement for Happy Haven Daycare Center as a guide to assist in the establishment of a Network Security Management policy. Happy Haven Daycare Center is the brain child of Owners Kim & Dean Doane offering state of the art care and security for Pre-School and latchkey age children. (Ages; Newborn to 5 year old +)
The daycare facility is a new build with only outer walls at the time of this writing. The owners plan to install a small (less than 100 nodes (workstations)) network and with the backbone (basic) network components (wiring, etc.) going in prior to building out the space. The purpose of this report is help the owners evaluate their security needs and put into place systems and policies which relate to the security of its employees, Clients, and company assets.

With this information Mr. & Mrs. Doan should be able to govern their company's information security policies with strategic planning and assess, plan and implement measures and policies to protect valuable company assets and information in digital and paper forms.

Desired Outcome

The desired outcome of information security governance according to the authors of "Management of Information Security" Third Edition, would be as follows

1. Strategic alignment of information security with business strategy to support organizational objectives
2. Risk Management by executing appropriate measures to manage and mitigate threats to information resources.
3. Resource management by utilizing information security knowledge and infrastructure efficiently and effectively.
4. Performance measurement by measuring, monitoring, and reporting information security governance metric to ensure that organizational objectives are achieved.
5. Value delivery by optimizing information security investments in support of organizational objectives.

The National Association of Corporate Directors (NACD), the leading membership organization for boards and directors in the United States, recognizes the importance of information security. It recommends four essential practices for boards of directors:

1. Place information security on the boards Agenda.
2. Identify information security leaders, hold them accountable, and ensure support for them.
3. Ensure the effectiveness of the corporation's information security policy through review and approval.
4. Assign information security to a key committee and ensure adequate support for that committee[i]

Benefits [ii]

- Increase in Share Value for organizations
- Increased predictability and reduced uncertainty of business operations by lowering information security related risks to definable and acceptable levels
- Protection from the increasing potential for civil or legal liability as a result of information inaccuracy of the absence of due care.
- Optimization of the allocation of limited security resources.
- Assurance of effective information security policy and policy compliance
- A firm foundation for efficient and effective risk management, process improvement and rapid incident response.
- A level of assurance that critical decisions are not based on faulty information.
- Accountability for safeguarding information during critical business activities such as mergers and acquisitions, business process recovery, and regulatory response.
-

The Threat Assessment

Aside from the fact that the care and protection of the children which are in the care of a daycare facility, is the most important concern of the facility, is the fact that in the childcare industry the most valuable "information" a day care facility would have may just be the "Confidential" information of the parents and their Children, both of which were placed in your trust. Equally important to you, the organization is the information concerning the business, its operations, and its employees. For these reasons, it is imperative that an organization makes and assessment of possible threats not only to the organization's Information but to the organization's assets as well. Here we will talk about threats to the organizations Information assets.

System Components

The network installed for Happy Haven will consist of the following components

Hardware	**(Assets)**	
1. Firewall	2. Router	3. Switch
4. Patch Panel	5. Server	6. Workstations
7. Wireless Access points	8. Laptop	9. Printers
Software	**(Assets)**	
1. Word[1]	2. Outlook[1]	3. Access[1]
4. Excel[1]	5. Publisher[1]	6. Powerpoint[1]
7. Onenote[1]	8. Child Care Manager	9. QuickBooks Pro
Information	**(Assets)**	
1. Stockholder Names	2. Social Security Numbers	3. Address & Phone Numbers
4. Employee Names	5. DOB & Social Security Number	6. Address & Phones Numbers

[1] Word, Outlook, Access, Excel, Publisher, PowerPoint & OneNote are part of the Microsoft Office suite. Macros are a part of the features which come with these programs.

7. Parents Names	8. DOB & Social Security Number	9. Address & Phones Numbers
10. Children's Names	11. DOB & Social Security Number	12. Address & Phone Numbers
13. Schedules of employees	14. Schedules of Children	15. Parents Checking & Credit Card Numbers
16. Company financials	17. Bank Account information	18.

Table 1

Threat Categories and examples

So let's take a look at some of the possible threats for Happy Haven Daycare Center.

Category	Example
Human Error	Accidents or mistakes
Compromise of intellectual property	Piracy, copyright infringement
Espionage or trespass	Unauthorized access and/or data collection
Acts of information extortion	Blackmail of information disclosure
Acts of sabotage or vandalism	Destruction of systems or information
Theft	Illegal confiscation of equipment or information
Software attacks	Viruses, worms, macros, denial of service
Deviations in quality of service from service providers	Power and wan service issues
Forces of nature	Fire. Flood. Earthquake, lightning
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Table 2

Vulnerability Identification

Human Error

People are human and humans make mistakes. Chalk it up to improper training, no training, inexperience, making assumptions, either intentionally or un-intentionally failing to follow policy, whatever the cause, such failures threaten an organization's information assets.

Compromise of Intellectual Property

I am not sure if this applies at this point to Happy Haven at this time. However, should the company ever obtain a copyright to something or a patent Network Solutions would suggest revisiting this section.

Espionage or Trespass

Although this covers a broad category of activities which may include theft (covered later in this report) When an unauthorized individual gains access to information an organization is trying to protect, the act is categorized as a deliberate act of espionage or trespassing.ii

Acts of Information Extortion

Common in credit card theft, this act occurs when an attacker or insider steals information from a computer system and demands compensation for it return or for a non-disclosure agreement.

Sabotage or Vandalism

When an individual or group of individuals intend to sabotage to operations of a computer system or business or deliberately destroy an asset or damage the image of an organization.

All the items in table 2 may be established as attacks against the assets of the organization. A threat Agent often referred to as a hacker, identifies vulnerability and exploits that vulnerability in the form of an attack on the assets of an organization or even an individual. Sometimes for financial gain and other times just to prove, they could do it.

Theft

Simply the taking of another’s property whether physical, electronic, or intellectual.

Software Attacks

Malicious code, software, or malware (often these terms are used interchangeably) which are deliberately designed to attack a vulnerable system are forms of “software attacks”. Malicious code would include viruses, worms, Trojan horses, logic bombs, and back doors.

Deviations in Quality of Service

If a product or service is not delivered as expected, it is referred to as a deviation in the quality of service. The Happy Haven Daycare Center’s network depends on the successful operation of many interdependent support systems, i.e. Power grids, telecommunications networks, parts

suppliers, and service providers. The threat of power outages are common, when it happens it can cause voltage spikes, power surges, a momentary or prolonged dip in voltage (referred to as Sags and Brownouts), faults (a momentary complete loss of power), or even a blackout.

Forces of Nature

Sometimes referred to as "Force Majeure", these are "acts of God" and pose some of the most dangerous threats as they can occur without warning. These include fire, flood, earthquake, lightning, and even insect infestation.

Technical Hardware Failures or Errors

When a piece of hardware fails or errors occur because of a manufacturer's known or unknown flaw, it's called a "Hardware Failure".

Technical Software Failures or Errors

Similar to a hardware failure but with software and can include "Bugs" or untested failure conditions.

Technical Obsolescence

When network system infrastructure becomes antiquated and/or outdated, it can lead difficulties in maintaining reliable and trustworthy system operation, which can lead to erroneous data or a loss of data.

Control Analysis

Many of the systems, processes, hardware pieces, and software put into place in the Happy Haven Local Area Network are put there to protect from all these risks. Of course there is the more obvious methods used to protect an organizations assets like security doors and locks, security alarms on doors windows and motion sensors, fire alarms, and devices which you might normally find in any place of business. In a network environment however there is a need for additional security devices to protect against the "online" predator. Network Solutions, Inc. will put systems in place in an effort to minimize such risk, where appropriate details are provided in the sections, which follow below.

Minimizing Human Errors

There isn't much you can do about intentional or deliberate attacks against your organization except to treat people as fairly as you possibly can. Un-intentional acts or accidents however, could be minimized with proper training and education on the use of company assets and

having policies in place laying down rules and guidelines and making the review of such policies part of the training process. This process not only minimizes risk of a loss by human error but also the risk of successful litigations against an organization and financial loss therefrom.

Protecting Intellectual Property

Network Solutions, Inc. at the time of this writing is not aware of any such assets and therefore will not cover this in much detail. If however, there should come a time that an organization has such assets this topic should be re-visited and addressed. That being said, having in place the proper documentations and filings with the copyright and patent offices is the best place to start.

Espionage or Trespass

A hardware firewall which operates much like a security guard at the front door checking employee ID to ensure proper individuals enter the premises, the firewall checks the packets which arrive via the network medium (Cable, satellite, fiber optics), allowing access to only the packets which have proper credentials.

A hardware Router will protect internal IP Addresses for the Local Area Network of Happy Haven Daycare Center by offering a public IP address which gains access to the network as a gate would to a community. When a packet arrives to router, which is destined for a workstation within the organization, the router will “route” the packet toward the workstation with the IP address to which the packet was directed. You could say it is like having your mail delivered to a post office box, instead of your business or home. It adds a layer of security to your network.

Deterring Acts of Information Extortion

A server will be set up, which will establish a domain within the network, and a database, which will store and protect information regarding the operations of the organization. Part of the security provided by this process is an access control system, which stores user names and passwords, which require a user to “log in” to gain access. Policy should be in place regarding the use of user names and passwords.

Sabotage, Vandalism, or Theft

The aforementioned systems will also deter acts of sabotage and/or vandalism by making it more difficult to penetrate the network to carry out such attacks.

Safeguards against Software Attacks

Network Solutions, Inc. will install the most recent version of Norton Internet Security Suite, which adds a software firewall, Antivirus, Intrusion Detection, Browser Protection, Inbound Email Scanning, Outbound Email Scanning, Anti Phishing Protection, Identity Protection,

Automatic Back up, Automatic Updates to these services and more. Most of these processes are put in place to protect from Software Attacks. Some however are put in place to cover attacks outside of this category, i.e. Intrusion Protection could be an act of sabotage, vandalism or theft.

Guards against the Quality of Service or Forces of Nature

Part of the System put into place is a UPS (Un-interruptible Power Supply) which protects against these threats by providing stable voltages and currents so your system does not see the surges, spikes, sags, etc. In the event of a brownout or blackout, the system can be shut down without the loss of important company data.

Technical Hardware or Software Failures or Errors

Systems and policies will be installed which will allow for these potential losses by providing backup of important and/or vital company information and data.

As previously suggested in the process of proposing these systems, Network Solutions, Inc. advised procedures and policies be in place regarding usage of off-site backups to company information and data assets.

Technical Obsolescence

Keeping systems up to date and replacing antiquated, old and aging equipment if vital to the preservation of important and vital company information assets. As equipment ages and becomes antiquated, the risk of loss from equipment failure becomes far greater. For this reason, Network Solutions, Inc. recommends keeping systems up to date and maintained.

Likelihood of Loss from an Assessed Threat

Threat	Likelihood of loss
Human Error	Medium
Compromise of Intellectual Property	n/a
Acts of Espionage or Trespass	Low
Acts of Information Extortion	Low
Acts of Sabotage or Vandalism	Low
Acts of theft	Low
Software Attacks	Medium
Deviations in Quality of Service	High
Forces of Nature	Low
Hardware Failure or Errors	Medium
Software Failure or Errors	Medium
Technical Obsolescence	Low (higher as equipment ages)

Table 3

Impact Analysis

Threat	Impact
Human Error	Medium
Compromise of Intellectual Property	n/a
Acts of Espionage or Trespass	Low
Acts of Information Extortion	Low
Acts of Sabotage or Vandalism	Low
Acts of theft	Low
Software Attacks	Medium
Deviations in Quality of Service	Low
Forces of Nature	High
Hardware Failure or Errors	High
Software Failure or Errors	Medium
Technical Obsolescence	Medium

Table 4

TOP RecoveryTeam

Risk Determination

Threat	Risk Level (High; >50 to 100, Med; >10 to 50, Low 1 to 10)
Human Error	(25) Medium
Compromise of Intellectual Property	n/a
Acts of Espionage or Trespass	(1) Low
Acts of Information Extortion	(1)Low
Acts of Sabotage or Vandalism	(1)Low
Acts of theft	(1)Low
Software Attacks	(25)Medium
Deviations in Quality of Service	(10)Low
Forces of Nature	(10)High
Hardware Failure or Errors	(50)Medium
Software Failure or Errors	(25)Medium
Technical Obsolescence	(5)Low

Table 5

Control Recommendations

Network Solutions, Inc. has included in the proposed network systems to help keep these threat to a minimum. These systems include the following hardware, software and policies, which help to make the assets of Happy Haven Daycare Center, more secure.

Hardware		
Firewall	Router	Domain Control Server
Wireless Access points		
Software		
Access control Lists	Hard/Software Firewalls	Antivirus Software
Anti-Phishing Software	Backup Software	Active Directory Service
Policies	Covered more in next section	
Employee Training	Network Access	User Accounts
Backup	Off-site Backup	

Table 6

TOP RecoveryTeam

Contingency Plan[2]

IT 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) from a variety of sources such as natural disasters to terrorists actions. While many vulnerabilities may be minimized or eliminated through technical, management, or operational solutions as part of the organization's risk management effort, it is virtually impossible to completely eliminate all risks. In many cases, critical resources may reside outside the organization's control (such as electric power or telecommunications), and the organization may be unable to ensure their availability. Thus effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. Accordingly, in order for contingency planning to be successful agency management must ensure the following:

1. Understand the IT Contingency Planning Process and its place within the overall Continuity of Operations Plan and Business Continuity Plan process.

2. Develop or reexamine their contingency policy and planning process and apply the elements of the planning cycle, including preliminary planning, business impact analysis, alternate site selection, and recovery strategies.

3. Develop or reexamine their IT contingency planning policies and plans with emphasis on maintenance, training, and exercising the contingency plan.

This document addresses specific contingency planning recommendations for seven IT platform types and provides strategies and techniques common to all systems.

- Desktops and portable systems
- Servers
- Web sites
- Local area networks
- Wide area networks
- Distributed systems
- Mainframe systems.

Top

[2] From the Executive Summary of NIST SP800-34 page iv to v

The document also defines the following seven-step contingency process that an agency may apply to develop and maintain a viable contingency planning program for their IT systems. These seven progressive steps are designed to be integrated into each stage of the system development life cycle.

1. **Develop the contingency planning policy statement.** A formal department or agency policy provides the authority and guidance necessary to develop an effective contingency plan.

2. **Conduct the business impact analysis (BIA).** The BIA helps to identify and prioritize critical IT systems and components. A template for developing the BIA is also provided to assist the user.

3. **Identify preventive controls.** Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.

4. **Develop recovery strategies.** Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.

5. **Develop an IT contingency plan.** The contingency plan should contain detailed guidance and procedures for restoring a damaged system.

6. **Plan testing, training, and exercises.** Testing the plan identifies planning gaps, whereas training prepares recovery personnel for plan activation; both activities improve plan effectiveness and overall agency preparedness.

7. **Plan maintenance.** The plan should be a living document that is updated regularly to remain current with system enhancements.

The document presents a sample format for developing an IT contingency plan. The format defines three phases that govern the actions to be taken following a system disruption. The **Notification/Activation** Phase describes the process of notifying recovery personnel and performing a damage assessment. The **Recovery** Phase discusses a suggested course of action for recovery teams and personnel to restore IT operations at an alternate site or using contingency capabilities. The final phase, **Reconstitution**, outlines actions that can be taken to return the system to normal operating conditions.

Happy Haven Daycare, Inc. – Contingency Plan

RECOVERY TEAM - QUICK REFERENCE GUIDE[iii]

TOP (Recovery team contact information on page 19)

- Receive alert notification (p28) Normal business hours (p22) after hours (p22)
- Notify Recovery Team (p19, p28)
- Meet Recovery Team at Assembly Site (p23) (You can make notes here)
    - Location:
    - Time:
    - Contact Name:
- Use employee contact list (attach local list to the back of the plan) to notify appropriate additional personnel to:
- Proceed to Assembly Site
- If appropriate, bring resumption plan
- If appropriate, be prepared to travel (p27-40)
- Bring ID Badge(s)
- Bring pertinent resources from home or off-site (p44-46)

DO NOT TALK TO THE NEWS MEDIA

- If directed, meet the Emergency Management Team at the Command Center
    - Location:
    - Time:
    - Phone Number:
- Document information provided at the briefing
- Contact vendors and or clients if appropriate (p31 & p34)
- Report status of critical functions (p6) and potential concerns to the Emergency Management Team during the briefing
- Meet appropriate staff at Assembly Site (p23)
- Brief staff on the situation
- If Assembly Site is not the Work area instruct appropriate staff to report to the Work area (p25&36)
- Begin team recovery activities (p44 & p50)

TOP

Team Alert List

(Team Leader):

Mrs. Kim Doane	Home: 123-456-7890	Date/Time:
Cell phone: 321-654-0987	Pager:	Status:
For Emergency:		
Contact:	Relation:	Phone:

The Team Leader calls the following:

(Alternate Team Leader):

Mr. Dean Doane	Home:	Date/Time:
Cell phone: 321-654-9876	Pager:	Status:
For Emergency:		
Contact:	Relation:	Phone:

Network Engineer/Administrator:

Norm Coleman	Home:	Date/Time:
Cell phone: 810-423-1711	Pager:	Status:
For Emergency:		
Contact:	Relation:	Phone:
(Name)	Home:	Date/Time:
Cell phone:	Pager:	Status:
For Emergency:		
Contact:	Relation:	Phone
(Name)	Home:	Date/Time:
Cell phone:	Pager:	Status:
For Emergency:		
Contact:	Relation:	Phone:

Contingency Plan

(Name)	Home:	Date/Time:
Cell phone:	Pager:	Status:
For Emergency:		
Contact:	Relation:	Phone
(Name)	Home:	Date/Time:
Cell phone:	Pager:	Status:
For Emergency:		
Contact:	Relation:	Phone:

TOP

Record the date and time that each person was notified or last attempt made. Add the contact status BSY-Busy, NA-No Answer, PNA Person-not Available.

After the team notification has been completed. This checklist should be given to the Emergency Operations Center staff or Emergency Management Team.

TOP RecoveryTeam

Contingency Plan

Primary Contact: Kim Doane **Alternate: Dean Doane**

Team Responsibilities:

When notified by the Emergency Management Team that the Business Resumption Plan (BRP) has been activated, the primary responsibilities of the team will be to use their resources to support the corporate recovery effort and to activate their Recovery procedures.

Team Leader Responsibilities / Checklist

Read the entire section before performing any assignments.

General

The Primary responsibility of the Team Leader is to provide *leadership* of the recovery team and coordinate support for the recovery effort. Other responsibilities include:

1. Participate in Resumption meetings with the Emergency Management Team.
2. Direct the Business Continuity efforts of your team.
3. Oversee communications activities of the team.
4. Coordinate with the Emergency Operations Center regarding all administrative **issues.**

Critical Functions

Restore the following critical functions:

RTO* Critical Function

_____

_____

_____

** Recovery Time Objective (Amount of down time before outage threatens the survival of the company. RTO is determined by Senior Executives)*

TOP RecoveryTeam

Normal Business Hours Response

During an emergency that happens during normal business hours, follow the corporate emergency procedures to ensure the life and safety of all employees.

If the building is not accessible, the team personnel should assemble at:

- Primary site : 123 Main St, Flushing, MI
- Alternate site: 109 Maple St. Flushing, MI

Immediate actions to be taken by the department leader or assigned alternate:

1. Take a head count to make sure all team members are safe and available. Notify the

Emergency Management Team immediately if anyone is missing.

2. Look for a member of the Emergency Management Team to get instructions.

3. Record all the information and instructions given by the Emergency Management Team. Use the Notification Checklist located in this section as a guideline and work paper.

4. Before contacting anyone else, review the Notification Procedure located in this section.

5. Notify department personnel not already notified. Use the Notification Call List located in this section; it contains a list of who to call and what information to pass on.

6. If instructed by the Emergency Management Team, activate the Recovery procedures are located in this section.

After Normal Business Hours Response

When notified by the Emergency Management Team that the Business Resumption Plan has been activated, the team leader will:

1. Record all the information and instructions given by the Emergency Management Team. Use the Notification Checklist located in this section as a guideline and work paper.

2. Before contacting anyone else review the Notification Procedure located in this section

3. You may be instructed to only notify your alternate team leader, your entire team or as many department personnel as possible. Use the Team Alert List located in the front

of the plan or the Employee Call List located in the back of the plan. *Record the status of all notifications and give the completed call list to the team leader.*

4. If instructed by the Emergency Management Team, report to the Emergency Operations Center.

5. If instructed by the Emergency Management Team to activate your Recovery Team, procedures are located in this section.

6. When you activate your team, have them meet you at the primary or alternate meeting place listed below.

Primary Location

Facility Name: Sr. Center	
Street Address: 123 Main St	**Floor: 1st**
City/State/Zip: Flushing, MI 48433	
Contact Person: Jim Johnson **Alternate Contact: Bob Johnson**	**Phone No: 555-1212** **24 Hour No: 800-555-1212** **FAX No:** **Other No.:**
Security Considerations: Public Building, Jim Johnson will supply secure area for sensitive material.	

TOP RecoveryTeam

Contingency Plan

Alternate Location

Facility Name: Union Hall	
Street Address: 109 Maple St	**Floor: 1st rear**
City/State/Zip: Flushing, MI 48433	
Contact Person: Joe Boettger **Alternate Contact: Dean Zimmer**	**Phone No: 123-4567** **24 Hour No:** **FAX No:** **Other No.:**
Security Considerations: Will provide secure areas.	

TOP RecoveryTeam

Team Recovery

Business Resumption Plan Copies

The team leader should ensure that sufficient copies of the Business Resumption Plan are available**.**

Cellular Phone (TBD)

The team leader has a cellular phone for team use. The Emergency Management Team should be notified immediately of the cellular phone number.

Team Work area

The Emergency Management Team will provide the team with a work area for their use. Use the Business Recovery Work area Checklist in the appendix to ensure that the area is setup to match the requirements that the Recovery Team will need to support the recovery operation and resume essential business functions.

Notifications

Provide notification of the problem to vendors. The information provided should be reviewed with the Emergency Management Team before calling.

Team Recovery Steps

The following recovery actions are to be used as a guide. During a real disaster, circumstances may dictate that some or all of the steps documented may have to be altered. The team leader should use his/her judgment while managing the recovery operation.

The team leader should contact the Emergency Management Team to find out:

- When voice communications will be available at the work area.
- When servers will be operational and how current, the master files will be.

Departmental Meeting:

Key department personnel should meet to determine actions to be taken and establish the priority of restoring business functions based on the work area and resources available. The department leader should explain the goals and objectives identified by the Emergency Management Team.

TOP RecoveryTeam

Review tasks to be performed and assign personnel.

Personnel should be assigned to contact vendors and advise them about the situation and when they can expect service to be restored. Use the Vendor Notification in the appendix for contact information.

Determine if some personnel will have to travel to the business recovery site.

Distribute copies of any forms that will be needed during the recovery operation.

Distribute copies of the news media statement that has been prepared. Copies can be obtained from the Emergency Management Team. Instruct everyone not to makes statements to the news media.

Personnel should be assigned to provide recovery support needed by other teams, as needed.

Identify the category in which personnel should be alerted.

Consider:

- Personnel that might be need to give aid to other teams / departments.
- Personnel that will be needed at the work area to resume normal business functions.
- Personnel who should stay home and remain on standby (they will be needed when the initial group needs rest).

Contact personnel that will be needed to report to the assigned work area.

Designate space for personnel reporting to the work area.

Implement procedures to resume time dependent functions based on the priority established.

Instruct all department personnel to carry photo identification with them at all times and be prepared to show it to security or local authorities.

As progress continues during the recovery operation, the team should be prepared to move back to the affected facility and resume normal business operations.

Personnel Location Form

After the department personnel have been deployed, the department leader should complete the Personnel Location Control Form in the appendix. Completed forms should be sent to the Administrative Team to allow location tracking of all employees. Continue to update the information throughout each day of the recovery operation.

TOP RecoveryTeam

Status Report

The department leader should prepare written status reports frequently for the Emergency Management Team to keep them apprised of the current situation. Use the Status Report Form in the appendix as a guide.

Travel Arrangements

The department leader can get assistance for any team travel arrangements from the Administrative Support Team. This includes travel needs either inside of or out of the metro area. Use the Business Recovery Site Information section in the appendix for guidelines and to make a request.

TOP RecoveryTeam

Notification

Notification Checklist

When notified by the Emergency Management Team that the Business Resumption Plan (BRP) has been activated, the team leader or alternate should record the following information that will be passed along to department personnel:

1. Brief description of the problem: _____

   _____

2. Location of the Emergency Operations Center: _____

   _____

3. Phone number to contact the Emergency Operations Center: _____

4. Any immediate support requested by the Emergency Management Team:

   _____

   _____

5. Whether or not the facility can be entered: Yes ( ) No ( )

7. If the facility cannot be entered, the location that the team should use for a work area or meeting place:

   _____

Notification Procedure

The team leader, alternate or assigned individual upon activation of the Business Resumption Plan will contact team personnel using the following procedure:

During notifications of an alert or declared disaster, use this procedure to alert all personnel. Read the procedures thoroughly prior to making a call. By using the following instructions, you will not unnecessarily alarm family members of an employee who was working at the affected site at the time of the disaster.

TOP RecoveryTeam

Place phone call and say, “May I speak with (individual)?”

1. If available, provide the information you called to convey.

- Remind the person to make no public statements about the situation.
- Remind the person not to call co-workers (unless instructed to) and to advise their family not to call other employees.
- Record the information in the contact status column.

2. If not available, say, “Where may I reach (individual)?”

- If at any location other than the data center, get the phone number. Call the other location and providing the information you wanted to convey.
- If the individual was working at the affected site, indicate that you will reach the individual there. DO NOT discuss the disaster with the person answering the phone.
- Immediately notify the Emergency Operations Center.
- Record the information in the contact status column.

3. If contact is made with an answering machine: Make no statement regarding the situation.

- Provide the phone number to call at Emergency Operations Center; ask that the employee make contact at that number as soon as possible.
- Record the information in the contact status column.

4. If no answer:

- Record the information in the contact status column.

5. If no answer and the individual has a beeper:

- Place a call to the beeper number.
- Enter the number of the Emergency Operations Center for the individual to call.
- Record the information in the contact status column.

TOP RecoveryTeam

Notification Call List

Using the team member contact list in the front of the plan, the team leader, alternate or assigned individual should convey the following information when contacting the team personnel:

- Brief description of the problem.
- Location of the Emergency Operations Center and / or the Business Recovery Site
- Phone number of the Emergency Operations Center.
- Immediate actions to be taken.
- Whether or not the facility can be entered.
- Location and time the team should meet.
- All team members should carry photo identification with them at all times and be prepared to show it to security or local authorities.
- Instruct everyone notified not to make any statements to the media.

All callers should record status of everyone they call, noting the time the call was placed and whether the person was contacted. Make a reasonable number of attempts if the phone was busy or there was no answer. Forward the completed list to the EOC and the staff will continue to attempt to contact team members.

Corporate Headquarters Phone Numbers:

TOP RecoveryTeam

Vendor Notification

CRITICAL VENDORS*

Product/Service:	
Vendor Name:	
Street Address:	
City/State/Zip:	
Contact Person: **Alternate Contact:**	**Phone No.:** **24 Hour No.:** **FAX No.:** **Other No.:**
Comments:	

Contingency Plan

Product/Service:	
Vendor Name:	
Street Address:	
City/State/Zip:	
Contact Person: **Alternate Contact:**	**Phone No.:** **24 Hour No.:** **FAX No.:** **Other No.:**
Comments:	

TOP RecoveryTeam

Contingency Plan

Product/Service:	
Vendor Name:	
Street Address:	
City/State/Zip:	
Contact Person: **Alternate Contact:**	**Phone No.:** **24 Hour No.:** **FAX No.:** **Other No.:**
Comments:	

***List only vendors that you would be responsible for contacting.**

TOP RecoveryTeam

Customer Notification

KEY CUSTOMERS*

Product/Service:	
Customer Name:	
Street Address:	
City/State/Zip:	
Contact Person: **Alternate Contact:**	**Phone No.:** **24 Hour No.:** **FAX No.:** **Other No.:**
Comments:	

TOP RecoveryTeam

Product/Service:	
Customer/Client Name:	
Street Address:	
City/State/Zip:	
Contact Person: **Alternate Contact:**	**Phone No.:** **24 Hour No.:** **FAX No.:** **Other No.:**
Comments:	

TOP RecoveryTeam

Product/Service:	
Customer/Client Name:	
Street Address:	
City/State/Zip:	
Contact Person: **Alternate Contact:**	**Phone No.:** **24 Hour No.:** **FAX No.:** **Other No.**
Comments:	

***List only those customers you would be responsible for contacting.**

Business Recovery Work area Checklist

Work area Scenarios

The Emergency Management Team will provide the team leader with a work area for the team to use. One of the following is the most likely scenario that will take place.

Work area at the location, if the facility is accessible.

The Emergency Management Team will provide information about what area

the team can use.

TOP RecoveryTeam

Work area at a vendor Business Recovery Site, if the site is not available.

The Emergency Management Team will provide information about what area to use and the estimated time before terminals and communications to the backup site will be available.

Work area Requirements

The following lists the minimum requirements for the team at the work area recovery location. Copiers and FAX machines will be available at the work area for all teams to share.

Space in square feet: _____

Office Furniture: Desks: _____ Chairs: _____ File Cabinets: _____

Other Furniture: _____

Telephone Equipment

Phone Type: _____ Number of Phones: _____

Computer Equipment:

Indicate what terminals and PC's would require connection to the network.

Platform: _____ Terminal Type: _____ Number: _____
Network ____

PC Software: _____

Resources Required over Time

The following two forms are used to plan the arrival of recovery resources to the Work area. List only the increased amounts in each column. For example, the team needs 35 people over all. They assign 15 at the 24 hours slot, another 5 in the 48 hours slot and 15 more in the 72 hours slot.

TOP RecoveryTeam

Resources Required Over Time

Function / Resources	24 hours	48 hours	72 hours	1 week	2 weeks	1 month
Function Name						
Staff						
Area size						
Desks						
Chairs						
Telephones						
Faxes						
PCs						
Printers						
(Other)						
Function Name						
Staff						
Area size						
Desks						
Chairs						
Telephones						
Faxes						
PCs						
Printers						
(Other)						
Function Name						
Staff						
Area size						
Desks						
Chairs						
Telephones						
Faxes						
PCs						
Printers						
(Other)						

TOP RecoveryTeam

Resources Required Over Time (Consolidated)

Function / Resources	24 hours	48 hours	72 hours	1 week	2 weeks	1 month
All team functions						
Staff						
Area size						
Desks						
Chairs						
Telephones						
Faxes						
PCs						
Printers						
(Other)						

List only the increased amounts in each column. For example, the team needs 35 people over all. They assign 15 at the 24 hours slot, another 5 in the 48 hours slot and 15 more in the 72 hours slot.

TOP RecoveryTeam

Business Recovery Site Information

Guidelines for Travel to the Business Recovery Site

Most disasters are isolated to a single building or block. During those situations, the Business Recovery site in the local area will be used for recovery. Some disasters are community wide and, as such, may eliminate the option of using the local Business Recovery site. In those instances, we may resort to using more distant recovery sites.

The team leader should divide the available personnel into two groups: those who will go to the backup site first and those who will be sent as replacements after a few days. The department leader should not over commit resources during the first few days.

The team leader should provide directions to the personnel that will be traveling to the backup site. In the event that personnel cannot drive to the backup site and will need air transportation, hotel accommodations, and advance expense money, the team leader should arrange the details through the Administrative team leader or EOC Director.

The team leader will provide the Administration team leader or EOC Director with the names of the individuals, their destination, hotel requirements, an estimate of any travel money needed, and instructions relating to specific personnel who should not travel together on the same airplane (many companies have travel policies that forbid key individuals to fly on the same airplane in case of an accident).

The EOC Staff will make the travel arrangements and will provide personnel with itineraries, tickets, and advance travel money.

TOP RecoveryTeam

Business Recovery Site Information

Primary Location

Facility Name:	
Street Address:	**Floor:**
City/State/Zip:	
Contact Person: **Alternate Contact:**	**Phone No:** **24 Hour No:** **FAX No:** **Other No.:**
Security Considerations:	

TOP RecoveryTeam

Alternate Location

Facility Name:	
Street Address:	**Floor:**
City/State/Zip:	
Contact Person: **Alternate Contact:**	**Phone No:** **24 Hour No:** **FAX No:** **Other No.:**
Security Considerations:	

Directions to the Business Recovery Site

TBD

TOP RecoveryTeam

Travel Request Form

Make additional copies as needed

This form should be completed by the team leader and given to the EOC staff.

Name	**Destination**	**Departure Date / /**	**Departure Time :**
Hotel Reservation Yes ( ) No ( ) **Rental Car** Yes ( ) No ( ) **Cash Advance $**		**Departure Date / /**	**Departure Time :**
Name	**Destination**	**Departure Date / /**	**Departure Time :**
Hotel Reservation Yes ( ) No ( ) **Rental Car** Yes ( ) No ( ) **Cash Advance $**		**Departure Date / /**	**Departure Time :**
Name	**Destination**	**Departure Date / /**	**Departure Time :**
Hotel Reservation Yes ( ) No ( ) **Rental Car** Yes ( ) No ( ) **Cash Advance $**		**Departure Date / /**	**Departure Time :**
Name	**Destination**	**Departure Date / /**	**Departure Time :**
Hotel Reservation Yes ( ) No ( ) **Rental Car** Yes ( ) No ( ) **Cash Advance $**		**Departure Date / /**	**Departure Time :**

TOP RecoveryTeam

Off Site Stored Materials

Copies of critical documents, computer/PC back up floppies and tapes, critical supplies etc. may be available from a number of sources:

- Other First Bank facilities may have similar resources or copies of critical documents.
- Clients or contractors may have copies of critical documents.
- Commercial storage facilities will usually pick up backup tapes and documents and store them in a climate controlled and secure area.

Recovery Box

Consider creating a "Recovery Box" for your business unit. This Recovery Box could contain specific items that your business unit would need if your building were not accessible. Some items that could be contained in this box include:

- Copies of forms your business unit would need right away
- Copies of Procedure Manuals
- A small supply of unique supplies your business unit would need right away

This box must, of course, be stored at an off-site location. The box and an inventory listing of its contents are both critical records and should be documented as such.

TOP RecoveryTeam

TOP RecoveryTeam

Contingency Plan

Recovery Boxes

Team:
Storage Location:
Contact Name:

Box Identification:

Contents	Comments

Box Identification:

Contents	Comments

1. Storage location refers to the name of the offsite storage facility.
2. Contact name refers to the person who coordinates retrieval of recovery boxes.
3. Box Identification refers to the identifying code on the outside of the box.
4. Contents/Comments identify the items stored in the box and special concerns such as update / maintenance or shelf life.

Critical Resources to Be Retrieved

Many incidents do not completely destroy contents of offices. Depending on the circumstances, it might be possible to clean and dry paper, microfilm or microfiche. Even if computer diskettes, tapes and hard drives have been water, smoke or soot damaged, it might be possible to extract the information from them. Do not attempt to do this yourself. Contact your technical support area or facilities staff for help when the incident occurs.

Following the incident, if authorities and your facilities staff determine your affected building is safe to enter, you might be allowed into your building for a short time. This could be for as little as 15 minutes or one half-hour. Create a list of the critical items that you would need to retrieve if you could get into your building. This assumes, of course, that the items are salvageable.

You should list these items in order of importance.

Some examples of items you might need to retrieve include: computer disks, computers, selected paper files and work in process.

Examples of items that you should not list include: family pictures, unimportant files and information that are duplicated somewhere else.

TOP RecoveryTeam

CRITICAL RESOURCES TO BE RETREIVED

Note: Use this form to document the materials that should be retrieved if you are able to enter your facility following the incident and the items are not badly damaged.

Business Unit: _____

Bldg./Floor:	Location on Floor: (e.g. Northwest Corner)

Items To Be Retrieved	Comments	Condition*
CRITICAL RECORDS:		
EQUIPMENT:		
OTHER:		

* Complete “Condition” at the time of the incident.

Personnel Location Control Form

Make additional copies as needed

COMPLETE DAILY

FORWARD TO THE CRISIS MANAGEMENT TEAM

Date: ____/_____/____ **Completed by:**

_____

Operations Team

Schedule Name	Recovery Location	Phone Number	Work From	To

TOP RecoveryTeam

Status Report Form

Make additional copies as needed

Use this form to log significant recovery activities.

The team leader is required to submit written recovery status reports daily. Submit completed status reports to the Emergency Management Team. This status report may be submitted handwritten as long as it is legible.

Date: ____/____/____

Time: ____:____ AM / PM

Name: _____

Department: Operations Team

Comments: _____

_____

_____

_____

_____

_____

_____

_____

Conclusions: _____

_____

_____

_____

TOP RecoveryTeam

Recovery Preparedness

Team plans are intended to be living documents. They should reflect the latest information available. Team Leaders are responsible for reviewing and updating their plans on a semiannual basis.

The Team Leader, alternate Team Leader and other individuals who have copies of the team plan will be sent updates each time the plan is changed. The accepted practice is to print and distribute only the page or pages have been changed rather than the entire plan.

Semiannual Plan Review

(Updates due January 1 and July 1)

Team Leader and Alternate Team Leader. This section identifies the persons assigned in the leadership positions. The team leader to identify changes in assigned personnel should review it.

Recovery Team Alert List. This section provides contact information for all personnel assigned to the team. This list is prone to change since team members may leave or join the team, names may change due to marriage and contact information may change. The team leader should send a copy of the Recovery Team Alert List to each team member to review and update.

Critical Functions List. This section, found in Team Leader Responsibilities, identifies the critical functions that apply to the team. The Team Leader will review the functions to determine that they are accurate.

Team Recovery Steps. This section identifies the strategies for recovery of critical functions. The team leader will review this list to determine that the strategies are meeting the current business objectives and accurately reflect the best possible solution.

Vendor and Customer Lists. This section identifies the contact information for critical vendors and customers. The team leader will review this list to determine that the list is complete and accurate.

Work area Requirements. This section identifies critical resources required to support the recovery at the work area site. The team leader will review this list to determine that the list is complete and accurate.

TOP RecoveryTeam

Off Site stored Materials. This section identifies critical records or resources stored off site. The team leader will review this list to determine that the list is complete and accurate.

Training and Exercises

Updated plans are not enough if the people assigned to recovery teams do not know what is expected of them. Team members should receive training on recovery concepts in general and their team's functions in particular. Exercises help identify needed improvements in strategies and plans. Exercises also give team members valuable experience in dealing with the challenges inherent in recovery operations.

The Business Continuity Group conducts training and exercises.

Team Member Orientation. This is a one-hour overview of the Business Continuity Program. Each team member should attend once per year. It is also available for the general employee population.

Team Exercise. The entire team participates in a two-hour tabletop exercise with a focus on their recovery strategies.

Team Leader Exercise. All the team leaders and Alternate Team Leaders participate in a two-hour tabletop exercise with a focus on facility wide recovery.

Functional Exercise. Actual hands-on test of hardware or connectivity capability at Work Area Recovery Centers. Actual use of alternate (manual) production process at the home or alternate facility.

Activity Schedule

This document allows Team Leaders to track their own plan review, training and exercise activities for the year. The Business Continuity Group will periodically request a copy of the document to review the team's preparedness status. A new document will be started each year. The Business Continuity Group will keep each year's completed activity schedule on file for audit purposes.

TOP RecoveryTeam

ACTIVITY SCHEDULE

Plan Reviews

Enter the dates when plan reviews were conducted.

Plan Holders	**Due Jan 1**	**Due Jul 1**
Team Leader (Name)		
Alt. Team Leader (Name)		
(Name)		
(Name)		
(Name)		
(Name)		

Training / Exercises

Enter the dates and number of participants for each activity. Each exercise type is expected to be conducted at least once per year.

Activity	Date Conducted	# of Participants	Comments
Orientation			
Team Exercise			
Team Leader Ex			
Functional Exercise			

Team Leaders: Attach participant sign in sheets, evaluations and comments to this sheet.

Send this page to the Business Continuity Group no later than December 1.

TOP RecoveryTeam

Task	Required Steps	Expected Results	Task Duration
1.			
2.			
3.			
4.			
5.			
6.			
7.			

Critical Function Recovery Tasks

Function name: _____

TOP RecoveryTeam

Information Security Policy[iv]

Information Security Policy Statement for Happy Haven Daycare Centers

Introduction

Information is a key resource for the Happy Haven Daycare Centers, without which virtually all of our activities would cease. Our information includes: case, control, coding and incidence data; administrative, personnel, financial and funding data; computing network and database systems, methodology; analyses; publications and references. Information may exist in many forms: it may be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

The Happy Haven Daycare Centers must endeavor to do all it can to protect its information assets in ways that are appropriate and effective. This will help enable the Happy Haven Daycare Centers to fulfill its responsibilities and to enable our staff to carry out their duties.

Objective

Our security objective is to protect the Happy Haven Daycare Centers from security problems that might have an adverse effect on our operations and our professional standing.

Security problems can include confidentiality (people obtaining or disclosing information inappropriately), integrity (information being altered or erroneously validated, whether deliberate or accidental) and availability (information not being available when it is required). A wide definition of security will be used to include all types of incident that pose a threat to the effective use of information. This includes performance, consistency, reliability, accuracy and timeliness.

Principles

Approach

We will:

Use all reasonable, appropriate, practical and effective security measures to protect our important processes and assets in order to achieve our security objective.

TOP RecoveryTeam

Utilize ISO17999: Code of Practice for Information Security Management as a framework for guiding our approach to managing security.

Continually review our use of security measures so that we can improve the way in which we protect our business.

Protect and manage our information assets to enable us to meet our contractual, legislative, privacy and ethical responsibilities. We are aware of the need to provide value for money and be aware of public opinion.

Responsibilities

All staff, past and present, permanent, honorary and temporary, of the Happy Haven Daycare Centers have an obligation to protect our information assets, systems and infrastructure. They will, at all times, act in a responsible, professional and security-aware way, maintaining an awareness of and conformance to this Policy.

Everyone will respect the information assets of third parties whether or not such protection is required contractually, legally or ethically.

All members of the Happy Haven Daycare Centers are responsible for identifying security shortfalls in our existing security practices and/or improvements that could be made. These should be reported to the Security Steering Group.

All members who have supervisory responsibility are required to actively promote best practice amongst their supervised staff.

The Director of the Happy Haven Daycare Centers has ultimate responsibility for ensuring that information within the Happy Haven Daycare Centers is adequately protected. The Director will delegate responsibility for approving and reviewing access rights to information to named, responsible individuals.

The Director of the Happy Haven Daycare Centers is responsible for ensuring that our security objective is achieved. Network Solutions is authorized by the Director to pursue appropriate activities and actions that contribute to achieving our security objective and that are consistent with this Information Security Policy.

The Director of the Happy Haven Daycare Centers is responsible for allocating sufficient resources so that the Happy Haven Daycare Centers can realistically achieve its security objective. This includes people, time, equipment, software, education and access to external sources of information and knowledge.

TOP RecoveryTeam

Practices

We will identify our security risks and their relative priorities, responding to them promptly and implementing safeguards that are appropriate, effective, culturally acceptable and practical.

All members of Happy Haven Daycare Centers will be responsible for their actions with regard to information security.

All information (including third party information) will be protected by security controls and handling procedures appropriate to its sensitivity and criticality.

The Happy Haven Daycare Centers will ensure that its activities can continue with minimal disruption, or other adverse effect, should it suffer any form of disruption or security incident.

Actual or suspected security incidents will be reported promptly to Network Solutions, who will manage the incident, and arrange for an analysis of the incident and consequent lessons to be learnt.

Documented procedures and standards, along with education and training, will support these Principles and the Practices to which they give rise.

Compliance with the Policy will be monitored on a regular basis by Network Solutions, which will meet on a regular basis.

The Director of the Happy Haven Daycare Centers owns this Information Security Policy and is committed to the implementation of it. He or she will facilitate an annual review of it by Network Solutions. It will be reviewed for completeness, effectiveness and usability. Effectiveness will be measured by the Happy Haven Daycare Centers ability to avoid security incidents and minimize resulting impacts.

The Director of the Happy Haven Daycare Centers will sign off all new versions of the Information Security Policy. All members of the Happy Haven Daycare Centers are responsible for identifying ways in which the Information Security Policy might be improved. Suggestions for improvement should be sent to Network Solutions. If immediate changes are required a special meeting of the security team will be called, otherwise suggestions will be discussed at the meeting to conduct the annual review of the Policy.

Policy Awareness

A copy of this Policy will be made available to all staff currently employed, or when they join the Happy Haven Daycare Centers. Individual sections of the Policy will be updated as required and will be available on the Happy Haven Daycare Center's Intranet site. All members of the Happy Haven Daycare Centers are expected to be familiar with, and to comply with, the Information Security Policy at all times. The members of Network Solutions will, in the first instance, be responsible for interpretation and clarification of the Information Security Policy.

Staff requiring further information on any aspects of this Policy should discuss their needs with a member of Network Solutions.

Applicability and Enforcement

This Policy applies to all members of the Happy Haven Daycare Centers and those who use its facilities and information. Compliance with the Policy will form part of the contract of employment.

Failure to comply with the Information Security Policy could harm the ability of the Happy Haven Daycare Centers to achieve its aims and security objectives and could damage the professional reputation of the organization. Failure to comply will, in the ultimate sanction, be treated as a disciplinary matter. The Director of the Happy Haven Daycare Centers will be responsible for all decisions regarding the enforcement of this policy, utilizing the disciplinary procedures at his or her disposal as appropriate.

The Happy Haven Daycare Centers will encourage the adoption and use of this Information Security Policy by third parties cooperating in joint ventures.

TOP RecoveryTeam

Information Security Poster – Educate our kids[v].

Data Classification

Data Classification Scheme

Data classification is a decision making process where you assign a level of sensitivity to the data. The data is classified as it is being created and re-classified anytime it is amended, enhanced, stored, or transmitted. It determines the extent of which the data needs to be controlled, secured and/or protected. It is indicative of the value in terms of a business asset.

Classification of data is essential to the differentiating value between documents of little value and that, which is highly sensitive.

Classification	Examples	Description
Confidential	Plans or designs, Pending mergers or acquisitions, investment strategies, annual reports, accounting information, business plans, sensitive information of customers, banks, solicitors, accountants, medical records, etc.	Highly sensitive internal documents which if lost or made public or even shared, could seriously damage the organization's reputation or financial status or impeded the operations. This information should not be copied or removed without specific authority. Documents at this level should be kept at highest security level.
Sensitive	Work procedures, project plans, designs and specifications defining the way the organization operates.	This information is considered proprietary and for authorized personnel only. The security level for these documents is considered High.
Public	Brochures, press statements, public domain documents.	Information which has been approved for public use and which would normally cause the organization no undue hardship. Security level is minimal.

See examples below of how to mark each type of document.

Confidential and Sensitive documents should state their classification in the header and footer two-font sizes larger than the text of the body and in the same font as the document itself. The classification should also be printed on the cover in a large font but in the form of a watermark

Public needs no watermark or header/footer classification stated.

Classified Page - Example

Document Title
Author
Company Name
Address
etc.

TOP RecoveryTeam

Classification Cover Sheet – Example

SENSITIVE

FOR OFFICIAL USE ONLY

SENSITIVE

Information Security Officer

JOB DESCRIPTION

Job Summary: Under general direction, is responsible for protecting Company information generated, stored, and transmitted electronically; designs and implements a Company information security program; assesses security risks and threats to Company information systems; provides security training, education, and advice for the Company community; coordinates the implementation and management of information security tools, systems, policies, and procedures; participates in security-related policy development, communications, enforcement, and management of the Company's response to security threats and incidents.

Essential Duties and Responsibilities:

Include the following. Other duties may be assigned.

- Monitors and assesses the security risks to the Company's information assets; identifies information systems security requirements; coordinates the development, implementation and/or administration of the Company's security and information systems disaster recovery plans, policies, and procedures; coordinates the implementation and management of information security tools, systems, policies, and procedures.
- Develops, administers, and coordinates programs and procedures to ensure compliance to government, Company, and other regulatory policies and laws related to information security and privacy; develops and enforces physical and electronic security standards for Company information systems; responsible for assessment and acquisition of Information security hardware and software.
- Establishes and administers an information security education program; provides security training, education, and advice for the Company community; serves as a resource person regarding information security matters and related emerging technologies; maintains an information security web section.
- Assists with assessing network threats, managing intrusion detections and virus protection systems, protecting against cracker attacks, monitoring security logs, and responding to security problems and intrusions; establishes and administers an information security emergency response program including an emergency response team.
- Assesses the security impact of new technology implementations; organizes, convenes, and moderates information security program committees and working groups.
- Engages in a planned program of professional development, coordinates with ITS goals and responsibilities, to maintain continual growth in professional skills and knowledge essential to the position; performs special projects and other duties as assigned.

KNOWLEDGE, SKILLS, ABILITIES AND PERSONAL CHARACTERISTICS

- Knowledge of issues and problems related to information security
- Knowledge of contemporary hardware, software, and network architectures
- Strong technical background in systems and networking
- High level of integrity and sound judgment concerning security, privacy issues and complex situations
- Written and verbal communication skills
- Strong service commitment
- Planning skills
- Ability to work as a productive, responsible, self-motivated member and/or leader of a team

- Ability to work independently and manage time effectively
- Ability to understand and implement cultural change related to technology

MINIMUM QUALIFICATIONS

Qualifications: To perform this job successfully, an individual must be able to perform each essential duty satisfactorily. The requirements listed below are representative of the knowledge, skill, and ability required. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

Education and Experience:

Bachelor's degree from four-year college or university within area of assigned responsibility; and seven to ten years related experience and training; or equivalent combination of education and experience.

Communication Skills:

Ability to read, analyze, and interpret general business periodicals, professional journals, technical procedures, or governmental regulations. Ability to write reports, business correspondence, and procedure manuals. Ability to effectively present information and respond to questions from groups of managers, clients, customers, and the general public.

Mathematical Skills

Ability to add, subtract, multiply, and divide in all units of measure, using whole numbers, common fractions, and decimals.

Ability to define problems, collect data, establish facts, and draw valid conclusions. Ability to interpret an extensive variety of technical instructions in mathematical or diagram form and deal with several abstract and concrete variables.

Computer Skills:

Knowledge of Information Technology within area of assigned responsibility preferred.

Certificates, Licenses, Registrations:

Bachelor’s degree; supplemented with three (3) years of experience relevant to information security and IT policy development and implementation, preferably in a complex, multi-platform higher education IT environment. Certification as a Certified Information Systems Security Professional (CISSP) and/or Systems Security Certified Practitioner (SSCP) is desirable.

TOP RecoveryTeam

Sample Computer and Technology Acceptable Use Policy[vi]

Computer and Technology Resource Usage Policy HAPPY HAVEN DAYCARE CENTERS provides a variety of electronic communications systems for use in carrying out its business. All communication and information transmitted by, received from or stored in these systems are the property of HAPPY HAVEN DAYCARE CENTERS and, as such, are intended to be used for job-related purposes only.

Employees are required to sign an acknowledgment form before receiving access to the various systems in use at HAPPY HAVEN DAYCARE CENTERS. The following summary guidelines regarding access to and disclosure of data on any HAPPY HAVEN DAYCARE CENTERS electronic communication system will help you better determine how to use these systems in light of your own, the company's privacy, and security concerns. The following are only summary guidelines; employees should contact the Information Technology (IT) department for more detailed information.

The IT department maintains the Computer and Technology Resource Usage Policy on behalf of HAPPY HAVEN DAYCARE CENTERS. However, other departments may develop supplemental policies and controls to accommodate specific requirement so long as these policies do not compromise corporate policies and controls.

Monitoring: HAPPY HAVEN DAYCARE CENTERS provides the network, personal computers, electronic mail and other communications devices for your use on company business. HAPPY HAVEN DAYCARE CENTERS may access and disclose all data or messages stored on its systems or sent over its electronic mail system. HAPPY HAVEN DAYCARE CENTERS reserves the right to monitor communication and data at any time, with or without notice, to ensure that company property is being used only for business purposes. The company also reserves the right to disclose the contents of messages for any purpose at its sole discretion. No monitoring or disclosure will occur without the direction of either the human resources department, or executive leadership, unless otherwise noted.

Retrieval: Notwithstanding the company's right to retrieve and read any e-mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any e-mail messages that are not sent to them and cannot use a password, access a file, or retrieve any stored information unless authorized to do so.

Passwords: Initial passwords are assigned by the IT department and should not be given to other staff or persons outside the organization. Employees should change the provided passwords as soon as possible using the instructions provided by the IT staff. HAPPY HAVEN DAYCARE CENTERS reserves the right to override any employee-selected passwords and/or codes. Employees are required to provide the company with any such codes or passwords to facilitate access as needed. Periodically, staff may be required to change their passwords. At no time should an HAPPY HAVEN DAYCARE CENTERS employee allow a temporary, contractor or another employee use of their login. In the case where an employee does provide another person access to their account, they will be responsible for the actions of

the individual using their account. Passwords should not be stored in computer data files, on the network, or be displayed openly at any workstation.

Message Content: The e-mail system is not to be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations. The system is not to be used to create any offensive or disruptive messages. Among those that are considered offensive are any messages, which contain sexual implications, racial slurs, gender-specific comments or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability. The organization's overall employee manual or code of conduct shall be considered the prevailing authority in the event of possible misconduct.

Employees should note that any data and information on the system will not be deemed personal or private. In addition, the e-mail system may not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.

Legal Proceedings: Information sent by employees via the electronic mail system may be used in legal proceedings. Electronic mail messages are considered written communications and are potentially the subject of subpoena in litigation. HAPPY HAVEN DAYCARE CENTERS may inspect the contents of electronic mail messages in the course of an investigation, will respond to the legal process and will fulfill any legal obligations to third parties.

Physical Security: Access to computer rooms will be limited to staff who require access for the normal performance of their jobs. Computers with sensitive information installed on the local disk drive should be secured in a locked room or office during non-business hours. Equipment, which is to be removed from HAPPY HAVEN DAYCARE CENTERS property, must be approved in advance with the IT department and an inventory of this equipment maintained by IT. All equipment removal from the premises by an individual must be documented, including the makes, manufacturers and serial numbers on an IT supplied form, and a copy of this form shall be filed in the employees' HR folder. If the employee leaves the organization, he or she must return the equipment to HAPPY HAVEN DAYCARE CENTERS prior to the last day of employment.

Network Security: IT will monitor network security on a regular basis. Adequate information concerning network traffic and activity will be logged to ensure that breaches in network security can be detected. IT will also implement and maintain procedures to provide adequate protection from intrusion into HAPPY HAVEN DAYCARE CENTERS's computer systems from external sources. No computer that is connected to the network can have stored, on its disk(s) or in its memory, information that would permit access to other parts of the network. Staff should not store personal, business, member or other credit card/account information, or passwords within word processing or other data documents.

Personal Computer Security: Only legally licensed software will be installed on HAPPY HAVEN DAYCARE CENTERS computers. Users are expected to read, understand and conform to the license requirements of any software product(s) they use or install. Software cannot be copied or installed without the permission or involvement of the IT department. IT will

configure all workstations with virus protection software, which should not be removed or disabled. Each employee is responsible for protecting their computer against virus attack by following IT guidelines for scanning all incoming communications and media, and by not disabling the anti-virus application installed on their workstation. All data disks and files entering or leaving HAPPY HAVEN DAYCARE CENTERS should be scanned for viruses. All staff will log out of the network and turn their computers off before leaving the office at night. Staff should log off the network when they will be away from their desk for an extended period.

Backup Procedures: All network resources are backed up nightly, and tapes are rotated on a 6-week schedule and stored off-site. Nightly backups are stored for one week, and a weekly tape will be stored for no more than five weeks. Data stored on the local PC drives is not routinely backed up, and as a result, important data and applications should not be stored on the C: drives of these machines. Staff working on especially crucial information is encouraged to backup these projects to disks, which can be supplied by the IT department. Computer users will be responsible for ensuring that the data stored on their local machines is backed up as required by the owner.

Access to HAPPY HAVEN DAYCARE CENTERS Computers: HAPPY HAVEN DAYCARE CENTERS will provide computer accounts to all HAPPY HAVEN DAYCARE CENTERS staff. External people who are determined to be strategically important to HAPPY HAVEN DAYCARE CENTERS, such as temporary staff, volunteers, or contractors, will also be provided accounts as appropriate, on a case-by-case basis. The employee managing the temporary or contract staff assumes responsibility for the identification of access requirements and use of the account. Accounts will be revoked on request of the user or manager or when the employee terminates employment at HAPPY HAVEN DAYCARE CENTERS.

Internet Use: The Internet is to be used for business purposes only. Employees with Internet access are expressly prohibited from accessing, viewing, downloading, or printing pornographic or other sexually explicit materials. In addition, employees should be mindful that there is no assurance that e-mail texts and attachments sent within the company and on the Internet will not be seen, accessed or intercepted by unauthorized parties.

Failure to comply with all components of the Computer and Technology Resource Usage Policy may result in disciplinary action up to and including termination of employment. If you do not understand any part of the policy, it is your responsibility to obtain clarification from your manager or the IT department.

Software Usage: Employees are expected to use the standard software provided by IT, or identify applications they need in the course of their work. Staff members are not permitted to download applications, demos or upgrades without the involvement of IT. Employees will use the standard e-mail system provided by HAPPY HAVEN DAYCARE CENTERS for official e-mail communications, and should not install their own e-mail systems. Additionally, use of instant messaging programs, such as ICQ, AOL Instant Messenger, Microsoft Messenger, etc., is prohibited unless otherwise approved by management or the IT department.

Failure to comply with all components of the Computer and Technology Resource Usage Policy may result in disciplinary action up to and including termination of employment. Any employee who does not understand any part of the policy is responsible for obtaining clarification from his or her manager or the IT department.

TOP RecoveryTeam

Endnotes:

[i] Information Security Governance: A Call to Action. 2nd Edition, IT Governance Institute, Rolling Meadows, IL. 2006
[ii] Management of Information Security: 3rd Edition, Course Technology, Boston, MA 02210
[iii] Ed Pearce's Business Resumption Plan Templates on Disaster Recovery Journals website.
[iv] Adapted from Mike Murphy – The Research Group – Oxford University (as example)
[v] Design by Mass.gov public campaign to educate our kids about internet safety and security.
[vi] Adapted and used with permission. Source: Techno Prophet site Credit: George Breeden