King Arts Complex

Information Technology Assessment Report

July 09, 2012

The recommendations in this report are based on industry best practices, and should not be implemented without careful review. While most are not likely to cause operational issues, the possibility of system conflicts or other unforeseen issues does exist due to unique application and system needs.

<u>This report is not considered to be legal advice or an official statement of compliance to any Federal, State, or Local regulation but is designed for informational purposes only.</u> The information herein is obtained from sources that the authors believe to be reliable, but the authors make no guarantee as to there accuracy or completeness. The customer assumes responsibility for any actions based on recommendations contained in this report.

Table of Contents

1 Executive Summary

Security Assessment Overview

Based upon previous discussions, King Arts Complex (KAC) expressed a desire for an assessment of their overall Informantion Techology stance. Volunteers from The Community Corps 'Technology of Social Good' were assigned to assist KAC in this process, and the following represents the completion of that project.

This Final Report provides the results found during the consulting service to support KAC in their effort to strengthen their IT department in three (3) key areas – 1). Administrative, 2). Technical, and 3). Physical Safeguards. This assistance was provided by volunteers from CommunityCorp, who specifically addressed these components as it relates to their current IT processes. The objective was to provide a detailed assessment of the current environment, identify the gaps between the current state and to provide actionable recommendations. These recommendations, listed below, will position KAC to develop specific plans towards achieving a well rounded IT stance, and to meet KAC's strategic objectives as well.

Based on a five (5) year plan model – the assessment outlines the specific areas that will need to be addressed per time period. This are meant to be merely suggestions – if KAC feels one area is a higher priority than another, KAC is free to shift priorities according to their need.

For consistency, The Volunteers from CommunityCorp, will be known as 'The Volunteers' through the course of this document and King Arts Complex (KAC) will be known as 'KAC'.

Assessment Scope and Method

This assessment is documented in a table matrix format, and includes ratings and recommendations. A Microsoft Word document is being provided to consolidate the assessment information and recommendations into an easily readable format. Additionally, electronic versions of this report will be provided including Policy templates and other documentation that might be useful.

Assessment Findings Overview

The Final Report provides a detailed assessment of the current physical IT architecture, a review of internal and external network components, and policy and procedures used at KAC. The recommendations represented in this report have been drafted keeping industry best practices as the goal, while being mindful of the specific needs of a non-profit organization.

Of the specifications that are detailed in the accompanying report, The Volunteers observed five (5) specific situations during the onsite portion of the engagement that, in The Volunteers experience, required immediate attention from the appropriate KAC staff. This was an attempt to urgently remediate the potential for major computer downtime, and/or loss of productivity.

High Priority Issues:

1. The first situation involved an old server being used to store financial data.
2. The second situation involved the state of the network equipment being used in the Teleco closet. It is recommended that this equipment be updated, the cables properly labeled, and cables properly secured.

    a. Another item to mention for the Teleco closet is to turn this into the 'server' closet that houses all teleco gear, wireless routers, switches, and the server. More details on this will be provided below.

3. The wireless connections in the KAC building have poor reception or none at all. Details below will provide remediation recommendations.
4. Another concern that was mentioned is the lack of cell phone coverage in the facility. This was not deemed a high priority and is usually outside the purview of this audit team, but mention and remediation is mentioned below.
5. KAC Internet access and email resiliency was deemed poor and should be remediated ASAP

While many areas of KAC's physical and electronic security were deemed appropriate and in-line with standard best practices, this Final Report will ***only*** detail those specifications or issues that need to be remediated by KAC in order to strengthen their security and IT posture. This is to prevent this final report from being too long to manage effectively.

The tables below represent an overview of all specifications and policies that were addressed and their rating according to The Volunteers findings. If clarification is needed on the ratings structure and definition, please consult the applicable pages below for more details:

Zero to Six Month Plan
Equipment and Costs Matrix for 0-6 Month Remediation
Server Security Policy
Workstation Use Policy
Wireless Communication Policy
Router Security Policy
Data Backup Plan
Six Month to One Year Plan
Risk Analysis
Risk Management Plan
System Evaluation
Applications and Data Criticality Analysis
Protection from Malicious Software
Workstation Use Policy
Contingency Operations
ePI Integrity
Audit Controls
Automatic Logout
One Year to Two Year Plan
Disaster Recovery Plan
Information System Activity Review
Emergency Mode Operation Plan
Testing and Revision Procedures – Contingency Plan
Security Reminders & Training
Access Authorization
Passcode Management
Login Monitoring
Accountability – Device and Media Controls
Workstation Security
Emergency Access Procedure
Unique User Identification

Two Year to Three Year Plan
Termination Procedure
Assigned Workforce Responsibility
Access Controls and Validation Procedures
Device and Media Controls – Disposal
Device and Media Controls – Media Reuse
Facility Security Plan
Method to Authenticate ePI
Encryption and Decryption – Data in Transit
Encryption and Decryption – Data at Rest
Three Year to Five Year Plan
Incident Response and Reporting
Workforce Clearance Procedure
Sanction Policy
Workforce Security
Maintenance Records Procedures
Person and Entity Authentication
IT Policies and Procedures
Computer Usage Restrictions for Remote Network Users
General Acceptable Use Policy
Acknowledgement of Security Responsibilities
Information Security Policy
Acceptable Use Policy – Hardware/Software
Anti-Virus Policy
Internet Security Policy
Extranet Policy
Remote Access Policy
IT Assessment Policy
Security Configuration Guidelines (SCG)
Workforce Security Policy
Termination Procedure and Policy
Security Awareness Training Policy and Procedure
Workforce Clearance Policy and Procedure
Sanction Policy
Assigned Workforce Responsibility Policy and Procedure
Incident Response and Reporting Policy and Procedure

The Final Report provides significant detail to support an improved IT posture, increasing KAC resistance down-time, electronic outage, or novel process, while being mindful of budgetary concerns of the non-profit and attempting to provide recommendations that can be completed for little or no cost to the client.

2 Methodology and Scope

The KAC enterprise was evaluated from the perspective of a third party IT audit, both internally and externally. The Volunteers considered current Hardware and Software products being used, potential threats to the confidentiality of data, and improving overall process and procedure. Additional work was performed to ensure proper desktop computer and any servers containing financial data were identified and remediations recommended as appropriate. And finally, The Volunteers analyzed the policies and procedures that drive the day-to-day operations within KAC, for thoroughness to ensure proper legal coverage within those documents.

At the start of the assessment, interviews were conducted with the IT staff and Management, to focus the assessment on goals of importance to KAC, and to obtain the information necessary for the review. At the time of the assessment, The Volunteers were NOT provided copies of network diagrams, organizational charts, copies of all policies and procedures (including active and draft copies), and a basic inventory of all known information systems and assets. This information is either unavailable, or has not been previously considered. The Volunteers also requested an inventory of all known software used throughout the organization, an inventory of all known partnerships, a description of existing security hardware and software, and network equipment configuration detail for review to assist in the analysis – but this was unavailable at the time of the assessment as well.

A variety of methods were used to conduct an Assessment on internal systems to identify configuration weaknesses in installed software, and software with known vulnerabilities. In addition, The Volunteers studied as best as possible the network architecture to detect other potential issues. This included software currently in use, workstation security, access control to sensitive information, and emergency procedures during a potential disaster scenario. The assessment methodology follows the Assess – Recommend – Execute model for analyzing and providing actionable recommendations for KAC to remediate according to need, resources, and personnel level of expertise.

The Volunteers supplemented all of these sources of information with experience and judgment as well as currently accepted industry best practices to develop the KAC Security Assessment.

The assessment and recommendations follow a year-to-year plan that details timelines, scope, milestones, budgetary items, and most importantly priority. This plan is split up into five (5) easy to follow sections ranging from Critical Priority (zero to six months), to low priority (year three to year five).

3 Findings Matrix

The matrix tables in this report are all categorized by a predetermined rating structure. These ratings are intended to assist KAC Center in deciding which items to correct first. For example, the 'Not Started' ratings, in The Volunteers experience, should be considered first – after appropriate testing. While all four of these ratings are subjective, the following describes The Volunteers basic methodology for applying a rating to each item:

Complete: The Complete rating is the mark given to a specification that is current and exhibits standard best practice and/or exceeds. The Volunteers recommendation though, is that this specification receives continued attention to make sure that it remains within standard.

Partially Complete: The Partially Complete rating is the mark given to a specification that has been deemed incomplete according to standard best practices. The recommendation given on this rating will incorporate the necessary methods to be used in order to ensure industry best practices are being adhered to.

Not Started: The Not Started rating is the lowest rating and is the mark given to a specification that has shown 0% compliancy to industry standards. It will be The Volunteers recommendation that all specifications that receive this rating be attended to first.

N/A (Not Applicable): The N/A Not Applicable rating will be used in the instance of a specification not being applicable to KAC's organization. Due to the nature of certain Regulations, KAC's organization must have documentation stating why this specification does not apply to KAC, or documentation outlining how KAC has implemented an alternative remedy. The Volunteers will provide recommendations that will help satisfy either course of action listed above.

The additional fields within the table structure, as a point of clarification, are listed below:

Specification Sub-Section: this field lists the particular specification being discussed.

Specification Standard: this field identifies the main specification.

Explanation field: the field defines the specification per standard industry practice.

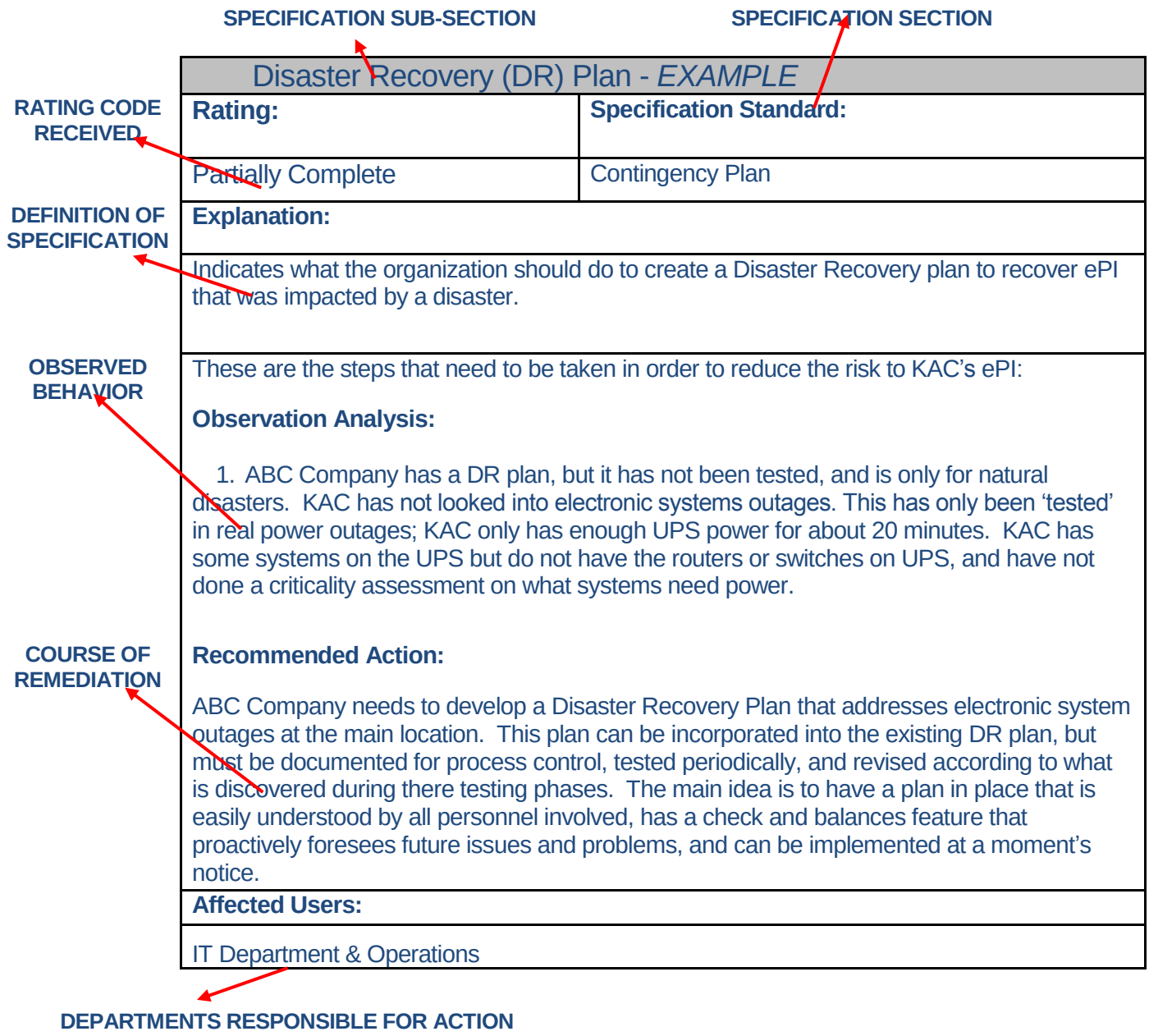
Observation Analysis: this field provides a detailed description of the behavior that was observed.

Recommended Action: this field provides detailed information to address the observation.

Affected Users: this field lists the departments that will be responsible for the remediation

The table below is a representation of the structure found in the detailed section of the Final Report. The Volunteers have provided this example to illustrate the method used in the report.

3.1 Example of Overall Matrix



Disaster Recovery (DR) Plan - *EXAMPLE*	
Rating:	**Specification Standard:**
Partially Complete	Contingency Plan
Explanation:	
Indicates what the organization should do to create a Disaster Recovery plan to recover ePI that was impacted by a disaster.	
These are the steps that need to be taken in order to reduce the risk to KAC's ePI: **Observation Analysis:** 1. ABC Company has a DR plan, but it has not been tested, and is only for natural disasters. KAC has not looked into electronic systems outages. This has only been 'tested' in real power outages; KAC only has enough UPS power for about 20 minutes. KAC has some systems on the UPS but do not have the routers or switches on UPS, and have not done a criticality assessment on what systems need power.	
Recommended Action: ABC Company needs to develop a Disaster Recovery Plan that addresses electronic system outages at the main location. This plan can be incorporated into the existing DR plan, but must be documented for process control, tested periodically, and revised according to what is discovered during there testing phases. The main idea is to have a plan in place that is easily understood by all personnel involved, has a check and balances feature that proactively foresees future issues and problems, and can be implemented at a moment's notice.	
Affected Users:	
IT Department & Operations	

This example shows the format to be used in the following analysis part of the Final Report. The intent is to help KAC understand the overall risk of any specific finding relative to the others in the Security Review.

4 Zero to 6 Months IT Plan

As discussed in the on-site meetings with KAC – the below outlines a zero (0) to six (6) month plan to ensure that the organization has a goal(s) to achieve, will remediate those items that were deemed critical, and to provide a financial guideline.

Each item is related to a policy and a physical recommendation. This is to incorporate both aspects so time/effort is saved in the short term and allows for goals to be achieved in a more timely fashion. Section 4.1 outlines the high-level costs associated with remediating the critical items.

4.1 Equipment and Costs Matrix for 0-6 Month Remediation

Total costs for equipment / software recommendations as listed below = **$9,950.00**. This includes the following, with the details listed below as well:

(2) Servers with software (1 for production, 1 as backup/inventory)
(8) Ethernet Repeaters
(8) Wireless routers
(1) Cisco switch
(1) Server/switch rack and related gear
(2) Workstations (backup/inventory)

This quote does not include labor or software licensing costs.

KAC Server Replacement:

Dell PowerEdge Server – R510 Rack Server
Ave. Cost: $1,700.00 (chassis only)
Server Overview: Four (4) Harddrives, One 2.0Ghz Processor, 4M Cache, 2GB Mem – We recommend at least RAID1 for the HDs.

Microsoft Small Business Server 2011 (Standard Edition, Factory Installed): $900.00

Total Cost: $2,600.00 approx.

HP Proliant DL360 G6 Server
Ave. Cost: $1,900.00 (chassis only)
Server Overview: 1 X Xeon 2.4ghz - 6gb Ddr3 Sdram - Serial Attached Scsi Raid Controller

Microsoft Small Business Server 2011 (Standard Edition, Factory Installed): $900.00

Total Cost: $2,800.00 approx.

TOTAL AVE. COST: $2,700.00

Wireless Network Remediation:

- **Ethernet Repeater**
  - TP-LINK TL-POE200 Power over Ethernet Adapter Kit
  - **Ave. Cost:** $30.00 per repeater (KAC will need eight (8) of these devices)
- **Copper CAT5/6 cabling**
  - Costs will vary and will include materials and labor
    - Standard costing on 1000ft of CAT6 copper cabling is $135.00/per 1000 ft
    - Labor – we cannot quote pricing on labor, but this will be your biggest expense
- **Wireless routers**
  These can be mounted discretely in each area, but proper placement should be a major consideration prior to installation
  - **Cisco WAP2000 Wireless-G Access Point** – POE

  Costs: $150.00 per device (KAC will need eight (8) of these devices) = $1,200.00

- **Cell Phone Coverage Enhancement (Not required)**
  Currently, there are many different types of Cell Phone signal boosters available on the market. Some examples are mentioned below including price. As with the wireless routers, placement is a major consideration before installation:
  CAE50 Gemini Dual Band SOHO Repeater -- $400.00

  Depending on the type of coverage needed, KAC may want to consider purchasing one (1) for the Executive offices, one (1) for the theater, and one (1) for the Board room area.

TOTAL AVE. COST: $1,440.00 (does not include Cell Phone Boosters or labor/cabling)

KAC Network Switch Replacement:

- **Cisco 48-port SF 300-48** 10/100 Managed Switch with Gigabit Uplinks
  - **Ave. Cost:** $630.00

TOTAL AVE. COST: $630.00

Teleco / Server Closet:

- Server Rack: Chatsworth Rack – 7' 2-Post Relay Rack (55053-703)
  - Cost: $175.00
- Rack Shelves: Chatsworth 19" Rack or Cabinet Mount Vented Cantilever Shelf (34-105100)
  - Cost: $30.00 per shelf (KAC will need six (6)) = $180.00
- Power PDU: Rack PDU, Basic, 1U, 20A, 120V, (10)5-20; 5-20P
  - Cost: $120.00
- Concrete Floor Installation Kit
  - Cost: $30.00
- Rack Mount Cooling System
  - Pyle Pro 19" Rack Mount Cooling Fan System W/ Temperature Display LED 80MM Cool
  - Cost: $70.00 x 2 = $140.00

TOTAL AVE. COST: $650.00

Workstation / Desktop Software Replacement:

Microsoft OEM software package – all OEM software is now available for download directly from Microsoft (please see the below links). I will tell you that they do not make it easy – there are many steps to follow.

You first must sign up for the Microsoft Partner Network

MPN Sign-up site:
https://partner.microsoft.com/global/40026972

Once you have an account, you are then free to download the requested software. You may want to have SSI involved in this process.

Download Site:
http://www.microsoft.com/oem/en/installation/downloads/Pages/windows_7_sp1.aspx#fbid=XF8sUZY85ub

TOTAL AVE. COST: TBD

This is meant to be merely a suggestion, due to changes at Microsoft, this may not be the best option for your company.

If upgrading software is a priority for your company, but the OEM process via Microsoft is not viable – below are some standard pricings for software. Each item is listed **per** device:

- Office 2010 Home / Business - $159.00
- Windows 7 OS - $100.00
- Windows Small Business Server 2011 - $380.00

Workstation / Desktop Hardware Replacement:

This section is for equipment sparing / inventory purposes. You should fully consult with SSI on this as they support/maintain your equipment. If the time it takes to swap out a desktop or server is too long (more than 1 day) by SSI, you may want to modify your contract with them to ensure that they always have at least two (2) workstations, and one (1) server on-hand at all times.

Dell Workstation (includes Windows 7 OS and Office)
OptiPlex 790 Desktop
3.3Ghz processor
2GB RAM
250GB harddrive
DVD-ROM drive
Cost: $680.00

Dell PowerEdge Server – R510 Rack Server
Ave. Cost: $1,700.00 (chassis only)
Server Overview: Four (4) Harddrives, One 2.0Ghz Processor, 4M Cache, 2GB Mem – We recommend at least RAID1 for the HDs.
Microsoft Small Business Server 2011 (Standard Edition, Factory Installed): $900.00
Total Cost: $2,600.00 approx.

KAC Internet Access

Heavy empathsis should be placed on remediating this aspect of the business ASAP. Furthermore, the vendor hosting the website should be notified that no further outages will be acceptable – and that no changes to the website, domain names, or other related technical item without first consultation with KAC and then only in an after-hours situation (after 19:00 Mon-Fri or only on the weekends).

The represents so suggestions to remediate the internet access problems. While it may seem like over-kill, this solution will greatly reduce your downtime and virtually guarantee that the internet access will not go down.

Business Class DSL (2 providers – 1 primary, 1 backup)

(Primary) Verizon Small Business – 7MB Download / 768K Upload = $75.00/month

(Backup) ATT FastAccess Business DSL 6.0 – 6MB Download / 512K Upload = $30.00/month

Email Resiliency

Serious detailed discussions need to be held with SSI to ensure that any email down-time is fully minimized. While The Volunteers don't fully understand why these issues keep happening, KAC may need to resort to a 3-strike rule with SSI – i.e. SSI is given 3 opportunies to remediate, if after that they still can not maintain the Centers email account properly, have an uptime of better than 99%, or continue to make excuses – KAC should be well within their right to terminate the contract without notice and seek this type of service elsewhere.

Having two (2) internet connections should help but might not resolve all issues. Please consult an attorney prior to any contract negotiations or terminations.

4.2 Server Security Policy

Rating
Not Started

Explanation

Defines high-level standards for security configuration of all servers used in the KAC Center networks. Detailed technical standards for specific platforms are included in the Security Configuration Guidelines.

Observation Analysis:

1. NONE IN PLACE

Observation Analysis:

2. This policy should be strictly internal to the IT Department and should not be posted on the Intranet.

Observation Analysis:

3. The information that is gathered during the Data and Application Criticality Analysis can be used towards this policy. KAC needs to document, review, and test this portion of the policy as this section deals strictly with the equipment that contains and maintains ePI.

Recommended Action:

- The current server needs to be replaced with newer hardware and updated software. Please see below for standard industry rates/costs associated:

Dell PowerEdge Server – R510 Rack Server
Ave. Cost: $1,700.00 (chassis only)
Server Overview: Four (4) Harddrives, One 2.0Ghz Processor, 4M Cache, 2GB Mem – We recommend at least RAID1 for the HDs.

Microsoft Small Business Server 2011 (Standard Edition, Factory Installed): $900.00

Total Cost: $2,600.00 approx.

HP Proliant DL360 G6 Server
Ave. Cost: $1,900.00 (chassis only)
Server Overview: 1 X Xeon 2.4ghz - 6gb Ddr3 Sdram - Serial Attached Scsi Raid Controller

Microsoft Small Business Server 2011 (Standard Edition, Factory Installed): $900.00

Total Cost: $2,800.00 approx.

Please discuss specifics with SSI. This should be considered a critical priority

- All possible effort needs to be taken in fully documenting the server's current security status. Each server is only as strong as the last security patch, and KAC needs to, not only update and patch, but actively monitor each server for bandwidth utilization, storage capacity, and each port that is open to the network.

Affected Users:
IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

4.3 Workstation Use Policy

Rating
Partially Complete

Explanation

Procedures to monitor and report on login attempts, reporting and documenting any discrepancies. Procedures for creating, changing, and safeguarding passcodes.

Observation Analysis:

1. The Volunteers believe a concise, direct policy body should be created with full approval and ownership by all departments.

Recommended Action:

- **Company Computers**
  - IT can only Install authorized software
  - Use only for business purposes, limited personal
  - Do not disable any security features
  - Mandatory passcode-protected screen saver
- **Internet**
  - Acceptable use of web
  - Corporate monitoring program
  - E-mail
    - Personal use of e-mail systems
    - Directives regarding transmission of sensitive information
    - E-mail messages are company property and may be monitored

Affected Users:

All enterprise users

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

4.4 Wireless Communication Policy

Rating
Not Started

Explanation

Defines security standards for the use of wireless systems within KAC Center networks, including approval processes and specific technical configuration guidelines.

Observation Analysis:

1. NONE IN PLACE

Observation Analysis:

2. Although KAC is only currently using wireless communication on a limited basis, effort should be made to incorporate a Wireless Communication Policy to the whole organization. The following aspects should be incorporated into this policy:

Recommended Action:

- The IT Department has sole control of the implementation of wireless networking and usage within the KAC organization.
- No wireless networks can be set up by non-IT Department personnel and are strictly forbidden.
- Documentation needs to be produced regarding each wireless network security setup, including WEP protocols, SSID broadcasting areas and visibility, and the methodology used to protect the wireless equipment and type of network segmentation used.
- Only KAC staff are able to use this connection, any attempts to connect to the KAC wireless network without prior authorization, could result in loss of privileges and/or prosecution for attempted computer fraud.

To further enhance the wireless capability at KAC, the below are some recommendations on how to accomplish this goal and what areas should be addressed first.

Impacted Areas and number of wireless devices needed per area:

- Executive offices (1 or 2 devices)
- Board Room (1 device)
- Art Gallary (1 or 2 devices)
- Theater area (4 devices)

Equipment that will be needed:

- **Ethernet Repeater**
  - TP-LINK TL-POE200 Power over Ethernet Adapter Kit
  - **Ave. Cost:** $30.00 per repeater (KAC will need eight (8) of these devices)
  - **Overview:** these devices are needed so that the cabling from the teleco closet to the areas that need wireless can be extended to those areas. The maximum distance allowed on copper cabling (CAT6) is 100 meters (300 ft approx). These devices amplfy the signal so greater distances can be accomplished and will also provide Power-Over Ethernet so no power cables are needed for the wireless devices.
- **Copper CAT5/6 cabling**
  - Costs will vary and will include materials and labor
    - Standard costing on 1000ft of CAT6 copper cabling is $135.00/per 1000 ft
    - Labor – we cannot quote pricing on labor, but this will be your biggest expense
- **Wireless routers**
  These can be mounted discretely in each area, but proper placement should be a major consideration prior to installation
  - **Cisco WAP2000 Wireless-G Access Point** – POE
    - Costs: $150.00 per device (KAC will need eight (8) of these devices)

Affected Users:
All enterprise users of this service

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

4.5 Router Security Policy

Rating	
Not Started	

Explanation

Defines standards for the security configuration of routers and switches within KAC Center networks.

Observation Analysis:

1. A Router Security Policy is not currently in place at KAC. This policy is strictly intended to be internal to KAC IT Personnel and related employees and should not be posted to the Intranet for general employee consumption. This policy is a documentation on how all routers and switches within the KAC network are configured, what IOS version a specific router/switch is running, basic product information, installation location, what network traffic is being supported by the router or switch, and any technical notes that would be needed in the event of a crisis or disaster in which the Lead is not available or incapacitated.

Recommended Action:

The following are known vulnerabilities to the existing Linksys EF3124 switch and should be addressed and documented immediately:

Linksys EF3124 series switch:

This switch is no longer sold or supported by Linksys or Cisco. That does not necessarily mean that KAC should stop using this device, but as the years go by it may be harder to obtain updated information. For ease of use, the Volunteers have provided an electronic version of the support manual.

Some known vulnerabilities on Linksys EF3124 series

- Network port failures – after years of use, users report port failures with no resolution or fix
- No further network drivers will be released for this switch
- You can no longer purchase this device (except maybe on eBay or similar site)

If an upgrade to the existing device is warranted – please see below for a recommendations. If SSI is required to provide this equipment and it is supported by them, the below could used as a technical guideline:

1. **Cisco 48-port SF 300-48 10/100 Managed Switch with Gigabit Uplinks**
    a. **Ave. Cost:** $630.00
    b. **Overview:** The Cisco SF 300-48 switch is a 48-port managed 10/100 switch with four 10/100/1000 ports, two of which are combination mini-GBIC ports. It delivers the security and advanced network features needed to support business-class data, voice, security, and wireless solutions. With energy-saving technology, it optimizes power use to help protect the environment and reduce energy costs without compromising performance. Additionally, it is easy to configure and manage with intuitive browser-based tools and is offered with a limited lifetime warranty, including next business day advance replacement and one year of technical support. With all these and more, the Cisco SF 300-48 provides the ideal combination of affordability, performance, and capabilities in a switch designed specifically for small businesses.

Affected Users:
IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

4.6 Data Backup Plan

Rating	**Specification Standard:**
Partially Complete	Contingency Plan

Explanation

Discusses organizational processes to regularly back up and securely store ePI.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. Current Data backup plan is single-threaded and needs to be revised.

Recommended Action:

The current state of data backup at KAC is vulnerable and single-threaded, and needs to be improved. The Volunteers are providing three (3) different levels of a plan that, in The Volunteers experience, will ensure this aspect of compliance. Each level can be utilized separately, or in tandem for a consolidated approach.

LEVEL ONE DATA BACKUP:

At a basic level, if IT personnel continue to carry the data backup media home with them at the end of the day, before it leaves the KAC building, personnel must sign the media out with date/time and media ID number. Also, the back-up media CD should be password protected (at a minimum – this will be discussed in more detail later). This will at least ensure that in the event of disaster at KAC or at the IT personnel's home, the media can be recovered and used appropriately. All of this must be documented, reviewed periodically, and tested for effectiveness. One issue that THE VOLUNTEERS foresee is access to the house where the media is stored. In the event that the specific IT personnel or personnel spouse is incapacitated, KAC will need a plan on how to obtain the media from the personnel's residence.

LEVEL TWO DATA BACKUP:

Incorporating the above methodology; on level two preparedness; KAC should make two (2) backup copies each night. One would reside with the IT personnel at their house, the other will be locked in the fire-proof cabinet (or at least a locked drawer) at KAC. All copies should be neatly labeled and filed properly for ease of use, and only appropriate personnel should have knowledge of where these copies are kept. All of this must be documented, reviewed periodically, and tested for effectiveness.

LEVEL THREE DATA BACKUP:

It is The Volunteers strongest recommendation that KAC utilize a third party backup system to automate the backup process. Such a system should perform backups securely, reliably, and automatically freeing KAC resource to focus on other work.

The following vendors offer a backup system, though others are available as well:

- Symantec (http://www.symantec.com/backup-exec-small-business-edition)
- Acronis (http://www.acronis.com/backup-recovery/online/).
- Iron Mountain (http://www.ironmountain.com/Solutions/Small-Business.aspx).

Affected Users:
IT Department and Operations

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

5 Six Months to One Year Plan

The below recommendations are to be completed (or considered) between 6 months and 1 year after the IT audit results have been presented.

5.1 Risk Analysis

Rating:	**Specification Standard:**
Not Started	Security Management Process

Explanation:

Discusses what the organization should do to identify, define, and prioritize risks to the confidentiality, integrity, and availability of its Electronic Personal Information (ePI).

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:
1. KAC does not have a backup facility or current data backup plan.

Recommended Action:
This aspect will be discussed in the specification 'Data Backup Plan', 'Disaster Recovery Plan' (DR), Emergency Procedure and Testing', and 'Contingency Plan' respectfully.

Observation Analysis:
2. No discernible Information Technology Roadmap Plan.

Recommended Action:
KAC, to the best of their abilities and with consideration to annual budgeting, should incorporate an IT plan that specifically maps out hardware/software purchases, network modifications/additions, workstation modifications/additions, server modifications/additions, and any other issues that are foreseeable during a given fiscal year. This plan should be well documented with task lists, assignment goals, completion dates, and the ability to add or delete to the task list when novel situations are introduced.

Affected Users:
IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

5.2 Risk Management Plan

Rating	Specification Standard:
Not Started	Security Management Process

Explanation

Defines what the organization should do to reduce the risks to its ePI to reasonable and appropriate levels.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. KAC needs a Risk Management plan which includes several key features.

Recommended Action:

A concentrated effort must be made to consolidate all information regarding a Risk Management Plan into one clear and concise document. This would include: KAC's Disaster Recovery Plan, Contingency Plan, Data Backup Plan, Emergency Mode Operation Plan, Information System Activity Review, System Evaluation, and Testing/Revision Plan of the above procedures. The Volunteers have detailed below by specification, what should be incorporated into this document.

Observation Analysis:

2. No software or hardware audit process is currently in place. KAC should have a documented process for when new software or hardware is introduced into the system.

Recommended Action:

When new software or hardware is introduced into the enterprise system, KAC must first audit the application or hardware to ensure that it does not adversely affect the existing structure.

This process needs to be fully documented with revisions to the testing and auditing done for each new system incorporated within enterprise, and should incorporate KAC's findings within the Data and Application Criticality Analysis specification listed below. This procedure will then be a part of the Risk Management Plan document as stated above.

Affected Users:

IT Department and Operations

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

5.3 System Evaluation

Rating	Specification Standard:
Not Started	Evaluation

Explanation

Describes processes the organization implements to prevent, detect, contain, and correct security violations relative to its ePI. Describes what the organization should do to regularly conduct a technical and non-technical evaluation of its security controls and processes in order to document compliance with its own security policies and the Security Rule. Discusses what the organization should do to appropriately maintain, distribute, and review the security policies and procedures it implements to comply with the Security Rule.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:
1. KAC does not utilize end-user monitoring safeguards concerning Internet web-surfing.

Recommended Action:
KAC should work with SSI to determine if existing anti-virus software can be used to protect against unauthorized internet surfing, email borne viruses, spam, phishing, spyware, etc.

Affected Users:
IT Department & Operations

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

5.4 Applications and Data Criticality Analysis

Rating	Specification Standard:
Not Started	Contingency Plan

Explanation

Reviews what the organization should do to have a formal process for defining and identifying the criticality of its information systems.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:
1. KAC does not have a formal applications and data criticality analysis system in place, and needs to have written policy on this aspect, which includes a list of critical applications, workstations, and servers that need to be on-line

during DR, Contingency, and Emergency Mode Operations.

Recommended Action:
In The Volunteers experience, it is the recommendation that KAC take into account the Data Backup Plan first and all of the systems and applications that will be needed for that plan, and then all other plans revolving around DR, Contingency, and Emergency Mode will resolve themselves according to this hierarchical structure.

This analysis will drive all other plans, so the plan must be complete and thorough. Remember to take into account that KAC needs to analyze for the minimum amount of servers, workstations, and applications needed to perform the aspects of the business that will be needed during times of disaster or security breaches. If it is deemed that an extended power outage is acceptable, or that the below represents to high a cost, this section can be discarded.

Generator Power
Thought should be given on whether or not KAC needs a generator. If the cost is not prohibitive, or if one can be provided – the first step is to ascertain how much power is provided by the generator, and how many devices can be utilized. KAC will need to have, at the least, an internet router, switch, primary Domain Name Service (DNS) server (or as provided by a service provider), a primary file server (or if KAC choose to institute the Data Backup plan, KAC could choose another critical server or workstation), and any other server running a critical application.

Please make sure to account for having at least two workstations available as well. Once KAC has this list of hardware, determination will need to be made on how much power is being drawn from the hardware. This will determine the type and size of generator, and the amount of extra propane/gasoline to have on hand to power the generator for a sufficient amount of time.

As with all changes to the network, this analysis needs to be fully documented, tested and revised on an annual basis.

Affected Users:
IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

5.5 Protection from Malicious Software

Rating	Specification Standard:
Partially Complete	Security Awareness and Training

Explanation

Indicates what the organization should do to provide regular training and awareness to its employees about its process for guarding against, detecting, and reporting malicious software.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. All workstations are protected by anti-virus software which seems to be updated and maintained by SSI, but the process of updating these workstations has not been documented.

Recommended Action:

THE VOLUNTEERS recommend that KAC document the process and procedure utilized to update the workstations with new anti-virus patches. This documentation should then be readily available to all IT personnel in the event that the personnel responsible for performing this action are incapacitated.

Affected Users:

IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

5.6 Workstation Use Policy

Rating	Specification Standard:
Not Started	Workstation Use

Explanation

Indicates what the organization should do to appropriately protect its workstations.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. During a brief 'walk-about' in the KAC main facility, several issues were observed

Recommended Action:

In The Volunteers experience, The Volunteers recommends the following issues be addressed with all KAC users:

- All users log-off the application when leaving their work-space, even if only for a couple of minutes.
- All file cabinets in offices, cubicles, or common areas should remain locked at all times
- All sensitive information in printed form should remain in unmarked files while in use at the workstation
- All office doors should be locked when the office is unattended, even for a brief period of time
- All network ports that are currently not use should be deactivated until needed. This includes vacant offices, common areas, the lobby area, or other areas that will not have network access capability in the foreseeable future.

Affected Users:
All KAC System Users

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

5.7 Contingency Operations

Rating	**Specification Standard:**
Not Started	Facility Access Controls

Explanation

Identifies what the organization should do to be able to effectively respond to emergencies or disasters that impact its ePI. Identifies what the organization should do to have formal, documented procedures for allowing authorized employees to enter its facility to take necessary actions as defined in its disaster recovery and emergency mode operations plans.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. KAC does not have a contingency plan. There needs to be a security breach and natural disaster contingency that has built in forensics to track what was done, how it was done, and time to resolution.

Recommended Action:

The Contingency Plan can be apart of KAC's Disaster Recovery, Data Backup, and Emergency Mode Operation Plans. All of this information can be found in these sections. The important thing to remember is to consolidate this information into one clear and concise document and should include the following:

- **Risk Analysis** – determines the business impact of applicable disaster threats on specific locations and the resources placed at those locations.

- **Business Impact Analysis (BIA)** – defines critical business processes/functions and the maximum tolerable downtime for each department's critical business processes/functions in order to minimize loss exposure impact to KAC's business.

- **Disaster Recovery and Business Continuity Strategy** – involves the identification and selection of recovery strategy alternatives.

- **Strategy Implementation and Testing** – involves the development of disaster recovery plans.

- **Security Training and Awareness** – includes developing user guides and curriculum to address employee security training and awareness and safety.
- **Support from vendors** – KAC should determine what type of support they will need from the vendors that supply KAC with materials and resources. Types of vendors to include: LAN/WAN wiring vendor, network equipment supplier, Unix/Windows server provider, and water/electric/gas companies.

Affected Users:
KAC IT Department & Operations

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

5.8 ePI Integrity

Rating	**Specification Standard:**
Not Started	Transmission Security

Explanation

Defines what the organization should do to appropriately protect the integrity of its ePI. Defines what the organization should do to appropriately use encryption to protect the confidentiality, integrity, and availability of ePI it transmits over electronic communications networks.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. All remote locations are on the WAN and get their Internet access from this main location, and all data entry is in 'real-time' over the network with no post-facto transmissions are performed.

    - THE VOLUNTEERS does recommend doing a hardware upgrade & Software Upgrade. This will ensure a faster

response on the network, better security features, updated hardware, and larger storage capacity.
Affected Users: IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			
4)			
5).			
6).			

NOTES:

5.9 Audit Controls

Rating	**Specification Standard:**
Not Started	Access Control

Explanation

Discusses what the organization should do to have a formal, documented procedure enabling authorized employees to obtain audit reporting control on ePI.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. This specification has received attention within other specifications listed above.

Affected Users:
KAC IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			

2).			

NOTES:

5.10 Automatic Logout

Rating	**Specification Standard:**
Not Started	Access Controls

Explanation

Discusses what the organization should do to develop and implement procedures for terminating users' sessions after a certain period of inactivity on systems that contain or have the ability to access ePI.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. A documented policy within KAC should detail the IT Departments capacity to 'see' users that have not logged out of the system for an extended period of time.

Recommended Action:

In The Volunteers experience, KAC should develop a daily duties list for all IT personnel. This checklist should be time specific and duty specific according to job function. Several items that could be included per job function:

Network Administrator

8am Activity:

- review all network activity during the previous evening via network monitoring tools
- correct 'bottle-necks' in the network and diagnose potential problems
- check WAN connections for connectivity including wireless
- check for new updates/patches for routers
- create Daily Task List for variety of duties including – wiring and network port configurations, coordinate installations and upgrades, and trouble-shoot user problems in conjunction with the Help Desk

4pm Activity:

- prepare to run tape back-up procedure
- review network activity that occurred during the day
- review SurfControl activity (or related application)
- perform necessary maintenance and recovery as needed

System Administrator (if applicable)

8am Activity:

- perform necessary maintenance to system and related applications
- view User Log for non-compliance to log-out procedure
- promptly upgrade applications as needed
- create Daily Task List for variety of duties including – assisting the Help Desk on trouble-shooting issues, respond to system failures, and protect ePI systems from attack

4pm Activity:

- assist with tape back-up function
- perform system analysis and tuning

- monitor system performance, analyze for potential issues
- view User Log for non-compliance to log-out procedure

These job functions are not all inclusive and should be used only as a starting point. The checklist should be a dynamic document that incorporates and accepts change easily. As with other functionalities within KAC, these duties should have a checks-and-balances feature built in to ensure that all functions are being performed each day.

Affected Users:
IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

6 One Year to Two Year Plan

The below recommendations are to be completed (or considered) between 1 years and 2 years after the IT audit results have been presented.

6.1 Disaster Recovery Plan

Rating	**Specification Standard:**
Not Started	Contingency Plan

Explanation

Indicates what the organization should do to create a disaster recovery plan to recover ePI that was impacted by a disaster.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. KAC should create a Disaster Recovery (DR) plan.

Recommended Action:

KAC needs to develop a Disaster Recovery Plan that provides for electronic system outages at the main campus, in addition to natural disasters that could potentially occur. This plan must be documented for process control, tested periodically, and revised according to what is discovered during their testing phases. The main idea is to have a plan in place that is easily understood by all personnel involved, has a check and balances feature that proactively foresees future issues and problems, and can be implemented in a moment's notice. Information that needs to be incorporated into this type of document includes the following:

- An objectives and overview section:

(EXAMPLE) This disaster recovery plan has the following primary objectives:

1. Present an orderly course of action for restoring critical computing capability to KAC within 1 to 4 days of initiation of the plan.
2. Set criteria for making the decision to recover at a backup site or repair the affected site.
3. Describe an organizational structure for carrying out the plan.
4. Provide information concerning personnel who will be required to carry out the plan and the computing expertise required.
5. Identify the equipment, floor plan, procedures, and other items necessary for the recovery.
6. Establish a procedure that allows for only authorized personnel access to the critical systems.
7. Develop a phone number call sheet for everyone on the DR Team and the process, in which the plan is initiated, by whom, and the order of events that will take place during the Disaster.

KAC needs to incorporate the following in its Disaster Recovery Plan:

1. Computer Crime (as it relates to critical and non-critical systems, and can include: identity theft, accessing sensitive material without proper authorization, etc)
2. Electrical Outages not covered by the above topics
3. Terrorist Activity and Sabotage (This issue could involve KAC directly or indirectly)

The above can be included into a Threat Matrix that is designed to identify location specific disasters that could occur. For locations that are in coastal areas, for example, they may be more susceptible to hurricane than locations inland. The KAC Threat Matrix will detail specific action plans for each scenario. Many of these action plans can be reused per the scenario, e.g. A flooding threat action plan would be very similar to the action plan used during a tornado.

Each of these topics will have an explanation of the topic as KAC defines it, preventative measures that will be taken in the

event of this occurring, and recommendations on how to deal with the event.

The testing of the Disaster Plan can be difficult at best, and potentially a logistical nightmare if not planned correctly. The recommendation for conducting this test is to choose one disaster scenario that would be most characteristic of KAC's location and environment. For example, if KAC's organization location is in the Midwest, KAC might want to run a tornado disaster scenario. Conversely, KAC would not want to run a hurricane scenario if they were in the Midwest, as this would not apply to KAC.

Typically, this type of testing is accomplished by using two different methods according to the organizations time, resources, and experience.

This first method is to run a virtual simulation of a disaster. This method is much easier to control and will still allow for useful lessons to be learned. This can occur during normal business hours, as it would not physically disrupt KAC's business continuity.

Prior to the test, there are several key elements that must be planned:

1. Determine the nature of the disaster – e.g. hurricane, flooding, thunderstorm, or tornado.
2. Determine all likely events that could occur during the disaster – e.g. loss of power, loss of potable water, flooding, sanitation issues, loss of equipment, etc.
3. Based on the Criticality Analysis, identify what systems need to be functional and what business operations need to be performed during the situation
4. Incorporate the existing disaster plan, and test the process for all likely events.

This could be utilized in a 'round-table' discussion situation, with all key personnel involved in applying their department's process to the scenario. During this discussion it is important to have a moderator who can run the simulation and keep track of the progress. Also keep in mind that resources will be limited during the event, and incorporating the Criticality Analysis of systems that will be needed to perform basic core functionality plays heavily into all situations. In other words, don't try to provide power to the entire building, when KAC only need two servers, 3 desktops, and a router and switch to fulfill KAC's business obligations and continuity.

EXAMPLE: The team has chosen a tornado situation. All possible events have been discussed and agreed upon by all participants. It is also important to discuss a time line for the scenario such as 1 to 3 days (Of course, during the simulation, time can be sped up.) Each department is given time to apply a process to each event, and then the simulation begins via the moderator. The moderator can also instigate escalating events into the scenario, or provide novel situations of their choice in order to test KAC's ability to react and work together as a team.

The second method for testing the Disaster and Contingency Planning is to perform a 'live' situation test. This could include, physically cutting all power to the building, simulating a biological, chemical, or other potential terrorist attack, or simulating a flood disaster. These types of tests take intense preparation and planning, and should only be done in an after-hours situation. Using the same criteria listed above, choose a scenario, dictate all likely events, and test the process per department on each potential situation.

With both methods, it is important to keep in mind the goal of this exercise. If the organization finds a process or procedure that is lacking in results, this is when KAC can revise the process and test it again. Proactively testing the processes in virtual situations is far better than being confronted with real-life catastrophes.

KAC should keep in mind that most disasters occur after the normal business day has ended. In that regard, KAC will need to actively plan on how to activate the DR and Contingency Response in an after-hours situation.

Another important aspect of this plan is developing a Data Criticality and System Criticality Analysis (as mentioned above) and this will be covered in the topics below, but should be considered as a part of the overall Disaster Recovery Plan.

Affected Users:

IT Department & Operations

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

6.2 Information System Activity Review

Rating	**Specification Standard:**
Not started	Security Management Process

Explanation

Describes processes for regular organizational review of activity on its information systems containing ePI.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:
1. KAC does not directly review activity on information systems. However, this function seems to be performed by SSI.

Recommended Action:
In addition to the services performed by SSI, KAC may consider implementing a process to review system activities. At a minimum this should be done annually, but The Volunteers recommend performing this function every quarter. It needs to include the following:

- An internal audit procedure must be established to spot-check records/logs of system activity. The internal audit procedure may utilize audit logs, activity reports, or other mechanisms to document and manage system activity. This information must also be maintained and stored for a period of no less than six (6) years or otherwise applicable to your type of organization.

- Audit logs, activity reports, or other mechanisms to document and manage system activity must be reviewed at intervals commensurate with the associated risk of the information system or the ePI repositories contained on said information system. The interval of the system activity review must not exceed, but may be less than, 90 days (again – using a 'spot-check' method; if issues present themselves during this review, then a more comprehensive examination can be performed).

- An Audit Control and Review Plan must be created by each department and approved by the IT Directors Office. This plan must include:
    - Systems and Applications to be logged
    - Information to be logged for each system
    - Procedures to review all audit logs and activity reports
- Security incidents such as activity exceptions and unauthorized access attempts must be detected, logged and reported immediately to the appropriate system management, security and privacy officers.
- Incorporate more functionality of software to provide auditing and reporting on network activity. Specifically, KAC should enable a function that allows KAC to filter inbound and outbound email content. This feature will enable KAC to proactively monitor and audit all email content to prevent spam, phishing emails, pornography, and other material detrimental to business. It will also provide another layer of protection for personnel that improperly send sensitive or confidential information outside the company (THE VOLUNTEERS will discuss this in more depth later in this report).

Affected Users:
IT Department & Operations

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

6.3 Emergency Mode Operation Plan

Rating	**Specification Standard:**
Not Started	Contingency Plan

Explanation

Discusses what the organization should do to establish a formal, documented emergency mode operations plan to enable the continuance of crucial business processes that protect the security of its ePI during and immediately after a crisis situation.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. If a security breach were to happen there is no procedure or plan in place to mitigate the incident.

Recommended Action:
This aspect of the regulation can be completed using details from KAC's Disaster Recovery Plan, KAC's Data Backup Plan, and KAC's Contingency Plan. Used in combination, KAC's Emergency Mode Operation will detail the aspects that deal specifically with KAC's business continuance in the event of an emergency directly before the incident and immediately after the security breach.

The below is an example of what should be included in this plan:

- Identify significant processes and controls that protect the confidentiality, integrity, and availability of EPI on KAC information systems.
- Identify and prioritize emergencies that may impact KAC information systems containing EPI.
- Define procedures for how KAC will respond to specific emergencies that impact information systems containing EPI.
- Define procedures for how KAC, during and immediately after a crisis situation, will maintain the processes and controls that ensure the availability, integrity and confidentiality of EPI on KAC information systems.
- Designate specific roles and responsibilities to initiate and maintain emergency mode operations.
- Reflect a contact/call tree that will quickly disseminate important information within KAC as necessary.
- Define a procedure that ensures that authorized employees can enter KAC facilities to enable continuation of processes and controls that protect EPI while KAC is operating in emergency mode.

Observation Analysis:
2. KAC needs to develop an Information Management Plan.

Recommended Action:
Please see below for The Volunteers recommendation based upon experience:

Physical Security during Disaster Scenario:
The Volunteers recommend, to the best of KAC's abilities, to engage with the local police or sheriff department for help in this area. They may already have a disaster response plan, and it would be worthwhile to know that KAC's facilities were included in this plan.

Additionally – due to the other tenants in the building, they need to at least be aware of your plan, and if they their own plan, that it be reviewed and if possible incorporated so that cross-collaboration can be utilized.

Back-up Personnel:
KAC should cross-train personnel on each aspect of the DR, Contingency, and Emergency Mode Operation Plan so that in the event of a disaster, if one individual is incapacitated, another individual can assume their role immediately.

Affected Users:
IT Department and Operations

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

3).			

NOTES:

6.4 Testing and Revision Procedures – Contingency Plan

Rating	**Specification Standard:**
Not Started	Contingency Plan

Explanation

Describes what the organization should do to conduct regular testing of its disaster recovery plan to ensure that it is up-to-date and effective.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. No testing has been done on their system for contingency planning.

Recommended Action:

This specification addresses all aspects of testing the various DR, Contingency, and Emergency Mode Planning. The main point of the specification is to have all testing documented and it must be done periodically. The Volunteers recommend at least once a year for all plans.

Affected Users:

IT Department and Operations

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

6.5 Security Reminders & Training

Rating	Specification Standard:
Not Started	Security Awareness and Training

Explanation

Describes elements of the organizational program for regularly providing appropriate security training and awareness to its employees. Defines what the organization should do to provide ongoing security information and awareness to its employees.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. Security training should be implemented and Security reminders should be posted.

Recommended Action:

It is in The Volunteers experience that, first and foremost, KAC needs to institute a coordinated effort to promote more than just an awareness of Security. Security Reminders need to be posted in common areas, such as the breakroom and conference rooms. Periodic reminders and training have to be performed for all KAC employees and should include the following:

- All workforce members of KAC, to include management and practitioners, shall receive training regarding security awareness.
- System Users of KAC shall receive training regarding:
  - Protection from malicious software use (including virus protection);
  - Periodic security updates;
  - Login; and
  - Passcode management.

Observation Analysis:

2. Training attendance tracking

Recommended Action:

A) Develop a tracking mechanism for employee training on security procedures. This is to document and demonstrate compliance for all employees having access to the information system(s) containing ePI. In The Volunteers experience, KAC should develop two training opportunities for its employees. The first training should include all personnel that have access to ePI. The second training should include all personnel that do not have access to ePI – e.g. maintenance personnel, secretaries, and others deemed, per job description, as not having access to sensitive information directly.

B) Develop a refresher training for security procedures that is provided to employees at a regular timeframe to be determined by KAC. This will accommodate continuing reminders, as well as, be a forum for training on any updates to the security policies.

Observation Analysis:

3. Security reminders: mechanism for ongoing reminders for security.

Recommended Action:

A) Utilize the agency's intranet to post ongoing security reminders with reference to policy and procedures available to the

user via the Intranet.

Develop a "walk-about" program to identify issues with security based on agency policy. This program could be developed by the IT team and should utilize a standard checklist (developed from prohibitions listed in policy and procedures) of items to be monitored. If an issue is discovered, e.g. a workstation is logged in to the system that is unattended, and then the notification to the user could be as simple as a note left at the workstation indicating the date, time, and description of the issue, the solution, and reference to KAC procedure. Conversely, walk-abouts could be used to indicate when policy and procedure are appropriately followed with a certificate to the user - "*Congratulations, you have received a Security award for following procedure"* This recommendation comes with the suggestion that KAC use this to positively reinforce appropriate behavior and to use this as a first level notification of improper use or behavior.

Other training reminders that can be utilized as 'rewards' for personnel compliance include: mouse pads, coasters, coffee cups, trophies, plaques, ribbons, and certificates.

C) Post security reminders, based on the prohibited items listed for training, in common areas e.g. hallway, conference rooms, break room area, lobby etc.

The Volunteers also recommend that regular email reminders be sent to all employees, and those without email addresses should receive the paper equivalent. Information should be posted in the common areas (lunch/break room, the conference rooms, the training rooms, and other areas that are frequented by a majority of KAC employees).

This should also be incorporated within KAC's Sanction and Termination Policy and Procedures to ensure full documentation is completed and that the process is tested and reviewed.

Affected Users:
Human Resources and Training Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

6.6 Access Authorization

Rating	Specification Standard:
Partially Complete	Information Access Management

Explanation

Identifies what the organization should do to ensure that all employees who can access its ePI are appropriately authorized or supervised. (Required Implementation Specification for the Workforce Security standard.) Indicates what the organization should do to ensure that only appropriate and authorized access is made to its ePI. Defines how the organization provides authorized access to its ePI.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. KAC does not have a documented process dictating File Server access control by job description.

Recommended Action:

Documentation needs to include how an employee's access and group membership within the File Server system is determined.

Affected Users:

Human Resources & IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

6.7 Passcode Management

Rating	Specification Standard:
Partially Complete	Security Awareness and Training

Explanation

Describes what the organization should do to maintain an effective process for appropriately creating, changing, and safeguarding passcodes.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. Passcode strength is not enforced and passcodes are not configured to expire automatically.

Recommended Action:

The Volunteers are in full agreement that IT creates all usernames and passcodes for all employees, and that the minimum length of characters allowed in the passcode is eight (8) with at least one character being a numeral. Windows logins should be configured to enforce password policy.

A log of all passcodes must be maintained by the IT Department. This file can be 'hidden' within the file structure of a designated Windows server, anonymously named, and its location changed bi-annually.

In addition, the IT Department should do annual spot-checks of employee workstations to ensure that no employee is writing down their passcode and displaying this information on monitors, under keyboards, or other easily accessible locations. This could be utilized during the 'walk-about' function detailed in the 'Security Awareness and Training' specification.

Affected Users:

IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

6.8 Login Monitoring

Rating	Specification Standard:
Not Started	Security Awareness and Training

Explanation

Discusses what the organization should do to inform employees about its process for monitoring login attempts and reporting discrepancies.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. This is not monitored.

Recommended Action:

The sign-on report needs to be checked on a regular basis to ensure that users are assigned to the correct group. Documentation needs to include how an employee's access and group membership within the File Server system is determined and how often the sign-on report will be checked.

Another tool that can be used includes the following:

Event Log Manager: freeware that can actively monitor workstations that are logged onto the network. http://www.netwrix.com/event_log_archiving_consolidation_freeware.html

Affected Users:

IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

6.9 Accountability – Device and Media Controls

Rating	Specification Standard:
Not Started	Device and Media Controls

Explanation

Discusses what the organization should do to appropriately protect information systems and electronic media containing ePI that are moved to various organizational locations. Defines what the organization should do to appropriately track and log all movement of information systems and electronic media containing ePI to various organizational locations.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. Appropriate safe-guards are needed for this specification.

Recommended Action:

It is in the THE VOLUNTEERS experience, that KAC develops a database that can be utilized to track all hardware and software within the organization. This would include inventory of all workstations, desktops, servers, network equipment, and software. The below is an example of the data captured:

Inventory ID Number	Type of Equipment	Location	Date Installed
2939945	**Workstation**	**Annex – Rm. 433**	**04/02/2006**
OS Type	**Applications Installed**	**IP Address**	**MAC Address**
Windows 2000	**eCET BUI**	**192.100.23.45**	**00-F3-38-23-DA-93**
Applicable License Codes	**Type of Update**	**Date of Update**	**Comments**
2398-2Z2-9483-G30Z-293	**SP2 – Windows XP**	**04/31/09**	**Case Manager**

Using the above twelve (12) fields as a basic starting point, KAC could maintain an active database that will assist in many different functional areas. It could be used as a tool for Help Desk personnel that need IP address information for remote work, and KAC could track equipment that has been removed from use with its disposal date and method of disposal.

KAC must also maintain all software license keys from all vendors regardless of software type. It is The Volunteers recommendation that KAC retains the physical license key, and document that key electronically in the inventory database; this information should never be destroyed.

There are many different types of uses for this database, and should be considered a priority within KAC.

Some tools that could used in developing this database include:

- **Appgini PHP Generator for MySQL:** Instantly create PHP web database applications that let users view, sort, and search and edit data of a MySQL database easily from a single web page. Can be found at www.hotscripts.com
- **ARIA Business Management:** Web-based business management software.
- **PHP Helpdesk:** A helpdesk application with a MySQL backend.

Affected Users:

KAC IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

6.10 Workstation Security

Rating	Specification Standard:
Not Started	Workstation Security

Explanation

Reviews what the organization should do to prevent unauthorized physical access to workstations that can access ePI while ensuring that authorized employees have appropriate access.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. No privacy screens on the monitors to prevent unauthorized viewing of sensitive data.

Recommended Action:

In The Volunteers experience, The Volunteers recommends that monitors in 'public' viewing areas (e.g. those not in an office or enclosed space) are provided security screen filters to prevent persons not directly sitting in front of the monitor the ability to see sensitive information on the screen. There are several manufactures of this type of screen and the average cost per monitor is between $50.00 and $100.00. The manufactures that The Volunteers recommend are: Kensington, Sony, ACCO, or Gravis.

In accordance to the above recommendation, the computers that are located in the lobby and financial areas should utilize this protection. Other computers that should incorporate this feature would include any computers that have screens facing open doorways or screens that are facing out into any open area.

Observation Analysis:

2. Other security measures that KAC might want to consider enacting at the workstation level are included in the below comments. These are only suggestions and should be tested before implementation:

Recommended Action:

Anti-Spyware/Pop-Up Blockers/Browser High-Jacking/Anti-Adware software

The above programs have been making local and national news lately and should be considered a high-priority at the workstation level. There are many free programs available on the internet that will scan the workstation hard-drive, locate spyware/adware, quarantine the offending program, and in many cases delete those programs. The Volunteers recommends running these programs at least once a month with the assistance of SSI:

- Xoftspy: freeware – deep scans registry and local drives for spyware
- Adaware: freeware – deep scans registry and local drives for adware

- F-Secure Blacklight: freeware – deep scans for browser high-jacks, cookie trackers, spyware, and root-kits

Create a Shortcut to Lock Computer

Right click a blank space on the desktop, select new, shortcut. Copy and Paste this line: "rundll32.exe user32.dll, LockWorkStation" in the program location box. Click next and create a name for the shortcut, click finish.

Disable Explorer File Menu

The file menu in Windows Explorer has some powerful items on it, such as delete, rename, and print, etc., that KAC may not want to be available in some situations. KAC can disable use of the file menu from Explorer with the following Registry change:

Hive: HKEY_CURRENT_USER
Key: Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Name: NoFileMenu
Data Type: REG_DWORD
Value: 00000001

A value of 1 means the file menu is disabled. A value of 0 enables it again. As always, use caution and frequent backups when editing the Registry.

Hide All Desktop Icons

Remove/Hide all of the icons from the desktop with the following Registry change:

Hive: HKEY_CURRENT_USER
Key: Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Name: NoDesktop
Data Type: dword
Value: 00000001

A value of 1 hides the desktop icons, and a value of 0 displays them.

Hide Last Username

A hacker (generally speaking) needs two things to gain access to resources on KAC's system: a username and a passcode. Windows NT/2000, by default, offers one of those for free. In order to prevent KAC's system from displaying the last username to login, make the following change (or create the following entry) to the registry

Hive: HKEY_LOCAL_MACHINE
Key: \Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
Name: DontDisplayLastUserName
Data Type: REG_SZ
Value: 1

Now when a user presses Ctrl-Alt-Del to logon, the username and passcode fields are both blank. As always, use caution and frequent backups when editing the registry.

Prevent Viewing Local Drives in IE

A user can open Internet Explorer, and type in the drive letter and a colon and view the drive. In order to prevent this, KAC can make the following change:

Hive: HKEY_CURRENT_USER
Key: Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Name: NoFileURL
Data Type: REG_DWORD
Value: *varies - see below*

A value of 1 means that drives can not be viewed with IE, and a value of 0 allows it.

Remove Drives from My Computer

Normally, when users open My Computer from the desktop, the employee will see an icon for each drive on the system. With the following Registry change, KAC can hide these icons, preventing users from finding them and using them.

Hive: HKEY_CURRENT_USER
Key: Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Name: NoDrives
Data Type: REG_DWORD
Value: *varies - see below*

To calculate the value to use, add up the following codes for the drives that KAC want to hide:
A=1
B=2
C=4
D=8
E=16
F=32

For instance to hide the E and F drives, the value would be 48.

Remove Explorer Options

In post SP4 systems (WIN 2000/NT), KAC can remove the "Options" menu item from the "View" menu in Windows Explorer by editing the registry and adding the following value:

Hive: HKEY_CURRENT_USER
Key: Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Name: NoOptions
Data Type: REG_DWORD
Value: 1

A value of 1 removes the Options menu item, and a value of 0 allows it. The user must log off/on for the change to take effect.

Remove Find Command from the Start Menu

Another way to lock-down the Start Menu. To remove the Find Command from the Start Menu, make the following

Registry change:

Hive: HKEY_CURRENT_USER
Key: Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Name: NoFind
Data Type: dword
Value: 00000001

A value of 1 hides the Find command, and a value of 0 displays it.

The following configurations should be used if KAC is using Internet Explorer (IE), or like web browser. These changes can be found at Tools, then Internet Options from the IE menu:

Privacy: Settings at Medium High or High, or Block all Cookies

Advanced:

- Disable auto updating for IE. Enable Install On Demand (IE 6.0 only)
- Enable checking for signatures on downloaded programs
- Enable saving encrypted pages to disk
- Disable using Private Communication Technology (PCT) 1.0
- Enable SSL 2.0, 3.0, and TLS 1.0
- Enable warning for invalid site certificates
- Enable warning if changing between secure and non-secure mode
- Enable warning if forms submittal is being redirected (very important for those personnel submitting 837 or other related data transmissions to FTP or URL's).
- Disable port 455 from sending/receiving data on all Windows servers

Enable Workstation Level Security Auditing

WIN XP has all the features enabled for setting up a small security audit application at the workstation level. Enable the 'Audit object access' in the Security Configuration and Analysis MMC, and set SACLs on the directories and files to be tracked. Just review the security logs.

Additional Recommended Actions:

Several items that KAC may consider using within the Administrative Tools Settings under Control Panel, again these are only suggestions and should be tested first before implementation:

- Account Lockout threshold – this is apart of the 'three strikes and you are out' rule
- Audit logon events – KAC can set a registry value for logging the past 10 logons, or whatever amount seems appropriate.
- Shut down system immediately if unable to log security audits – this prevents the user from disabling this feature at the registry level
- Restrict CD-ROM and USB port access – can be used based on type of workstation and user priority level
- Amount of idle time required before suspending network session

A good site from Microsoft regarding security is located at: http://www.microsoft.com/technet/security/default.mspx

Several good sites to monitor for vulnerabilities include:

www.securityfocus.com **www.sans.org** **www.virus.org**
Affected Users: KAC IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

6.11 Emergency Access Procedure

Rating	Specification Standard:
Not Started	Access Control

Explanation

Discusses what the organization should do to have a formal, documented emergency access procedure enabling authorized employees to obtain required ePI during the emergency.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1.There is no procedure for electronic data emergencies.

Recommended Action:

The Volunteers believes that this portion of the regulation will be covered under the Disaster Recovery, Data Backup, and Contingency Plans. Some items to consider within this sub-section include the following:

a. Each center shall maintain a documented procedure for access to electronic protected/confidential information during an emergency.

b. Access is only for immediate emergencies for KAC personnel with picture identification. KAC should have a list of authorized personnel that will need access to specific areas of the building, depending upon job function during a crisis event.

c. Emergency access to the server room is for implementation of the Disaster Recovery and Contingency Plans. No materials or hardware may be taken from the server room, unless granted by the highest authority within KAC. In the event that material or hardware must be removed from the server room, it must be identified before requesting emergency access, or the proper documentation is included in the procedure prior to the plans initiation.

d. This procedure should have an aspect built into the plan that allows for activation of the plan on a user-by-user basis. This will alleviate the need for staff members to seek approval before the plan can be activated saving time and resources.

Affected Users:
KAC IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

6.12 Unique User Identification

Rating	**Specification Standard:**
Partially Complete	Access Controls

Explanation

Discusses what the organization should do to assign a unique identifier for each of its employees who access its ePI for the purpose of tracking and monitoring use of information's systems.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:
1. Individuals are assigned unique usernames/passcodes by IT, but no monitoring or tracking is used.

Recommended Action:
Sufficient coverage on this topic has been outlined in the specifications above.

Affected Users:
KAC IT Department, Training, and Human Resources

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT

1).			
2).			
3).			

NOTES:

7 Two Year to Three Year Plan

The below recommendations are to be completed (or considered) between 2 years and 3 years after the IT audit results have been presented.

7.1 Termination Procedure

Rating	**Specification Standard:**
Partially Complete	Workforce Security

Explanation

Defines what the organization should do to prevent unauthorized access to its ePI by former employees.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. No clear and concise documentation on the termination policy or procedure.

Recommended Action:

Logins need to be removed once an employee leaves the organization, whether the termination is voluntary or for just cause. Current logins need to be researched and old logins need to be removed. Signon ID's should also be removed once an employee leaves the organization. In The Volunteers experience, The Volunteers approve of the policy of removing ALL users from the system that have had a termination of employment; to further this goal, The Volunteers recommends a checks-and-balances feature be built into this system to make sure that this process has occurred.

Observation Analysis:

2. There is some mention of consequences in the computer manual, but should be more specific.

Recommended Action:

KAC documents what occurrence issues are terminable. This is a particularly sensitive issue and could be documented within a policy and procedure managed by the Human Resource and IT departments and not available for general consumption. If it is determined, by KAC, to provide employees with additional information on sanctions, the confidentiality training that is conducted would be an appropriate and recommended place to do so. This information should then reside within the Sanction Policy, as listed below.

Affected Users:

Human Resources & IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

7.2 Assigned Workforce Responsibility

Rating	**Specification Standard:**
Not Applicable	Assigned Security Responsibility

Explanation

Describes the requirements for the responsibilities of the Information Security Officer. Defines what the requirements are relative to establishing organizational policies and procedures.

The Volunteers recommend that a clear, concise document be produced to outline this role. Of course this can be incorporated into an already existing role.

Affected Users:

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

7.3 Access Controls and Validation Procedures

Rating	**Specification Standard:**
Not Started	Facility Access Controls

Explanation

Discusses what the organization should do to appropriately control and validate physical access to its facilities containing information systems having ePI or software programs that can access ePI. Indicates what the organization should do to purchase and implement information systems that comply with its information access management policies. Discusses what the organization should do to record and examine significant activity on its information systems that contain or use ePI.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. KAC's server closet was not locked (even though the room had control access) .

Recommended Action:

The Volunteers minimum recommendation is that KAC installs a solid core door with lock or secured access.

Even though the room which has the server closet is secured , there are more people in the room that has physical access to the server closet & the servers.

Observation Analysis:
2. There is sufficient controlled access the front door of the building which is manned by a security .

Recommended Action:
No action required.

Observation Analysis:
3. Only few systems (desktops) were locked most of them were not logged off and there were papers found in the desks which had critical infromation.

Recommended Action:
It is The Volunteers recommendation, that should set to lock the systems after a specified amount of time.
Other methods for protecting desktops would include setting registry key values that would 'lock' the desktop after three (3) unsuccessful attempts to login. Only an administrator could 'unlock' the desktop for further use. KAC may also want to investigate software that deletes key files on the desktop that contains ePI if three (3) unsuccessful attempts to login are performed.

Frequent internal Audit has to be conducted within KAC to identify the users who has not stored papers,printouts,electronic storage devices in a secured closet/drawers.

Affected Users:
All the system users within KAC

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

7.4 Device and Media Controls - Disposal

Rating	Specification Standard:
Not Started	Device and Media Controls

Explanation

Describes what the organization should do to appropriately dispose of information systems and electronic media containing ePI when it is no longer needed.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. KAC doesn't have a standard procedure for disposal of old/decommissioned systems.

Recommended Action:

At a minimum, KAC needs to have this process documented within a central database system so that everyone who has access (strictly limited to IT Staff and Operations) to this application can easily access information on the location and disposal method used for specific pieces of hardware and media (must be listed by ID tag, type of hardware/media, location prior to disposal, and location after disposal). This recommendation is optimal.

It is The Volunteers recommendation that if KAC decides to use a disposal facility for incinerating shredded material, that it also incinerate all 'used' hardware and media as well. This will lessen the likelihood that the disposed material be stolen or lost, thereby possibly compromising sensitive information.

Another method of destroying media is to purchase a Degausser for CD-ROM/DVD media. This device is compact and makes all CD-ROM's/DVD's unreadable. Below are some specifics on this device:

- Destroys all optical media including CD-Rom, CD-R, CD-RW, DVD, and DVD-R.
- Renders Data Discs unreadable.
- Complete destruction of data.

There are several different companies that produce this type of device; The Volunteers recommends the Garner OMD-1 model.

As with other aspects of the specification, KAC will need to have a checks and balances feature built into the Track-It system for when a disposal or incineration has been made through a third party.

Affected Users:

IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

7.5 Device and Media Controls – Media Reuse

Rating	**Specification Standard:**
Not Started	Device and Media Controls

Explanation

Discusses what the organization should do to erase ePI from electronic media before re-using the media.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. KAC does not have documented method for disposing of this media.

Recommended Action:

This aspect has been covered in the above specification.

Affected Users:

IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

7.6 Facility Security Plan

Rating	Specification Standard:
Partially Complete	Facility Access Controls

Explanation

Describes what the organization should do to appropriately limit physical access to the information systems contained within its facilities, while ensuring that properly authorized employees can physically access such systems. Discusses what the organization should do to establish a facility security plan to protect its facilities and the equipment therein.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. No standard plan in place for physical data security or physical security breaches.

Recommended Action:

In The Volunteers experience, a Facility Security Plan must be designed, tested and implemented that specifically addresses physical security breaches. This must be scalable in order to take into account the various locations under KAC's purview. This incidents could include the following:

- Non-KAC personnel gain access to computers containing ePI – e.g. vendors or other business associates under contract to perform work for KAC Center
- Non-KAC personnel gain access to waste material that contains ePI
- Non-KAC personnel steal hardware or software that contains ePI.
- KAC personnel gains access to ePI that is not at the appropriate access level controls.
- KAC personnel steals hardware or software that contains ePI
- KAC personnel sends sensitive information via email or other transmission mode to unauthorized accounts or locations not within the control of KAC
- KAC personnel gains access to waste material that contains ePI

An example of what this plan might include or contain is listed below:
In the same way that any society needs laws and guidelines to ensure safety, organization and parity, so any organization requires a Site Computer Security Policy (CSP) to ensure the safe, organized and fair use of computational resources.

The use of computer systems pervades many aspects of modern life, including academic, engineering, and financial applications. When one considers these roles, such a policy assumes a large degree of importance.

A CSP is a document that sets out rules and principles which affect the way an organization approaches these specific problems.

Furthermore, a CSP is a document that leads to the specification of the agreed conditions of use of an organization's resources for users and other clients. It also sets out the rights that the employee can expect with that use.

Ultimately a CSP is a document that exists to prevent the loss of an asset or its value. A security breach can easily lead to such a loss, regardless of whether the security breach occurred as a result of an Act of God, hardware or software error, or malicious action internal or external to the organization.

The above description should be included in KAC's Facility Security Plan as a sub-part. A CSP can be viewed as a document of three distinct parts, all of which are necessary, but within themselves not sufficient.

The first part outlines the parameters within which the policy will operate, and may consist of many sections.

The second part of the policy is essentially a risk analysis, which discusses assets that need to be protected, the

threats that may cause damage to the assets, and the mechanisms that may be used to realize these threats. The material in this part forms the logic behind the rules and guidelines that form the actual security policies that are formally defined in the third part.

In order to be effective, the CSP must be the product of a directive from an influential and authoritative person within the organization.

It is important to define the driving force behind the development and implementation of the policy. Furthermore, this section must outline the person who has ultimate authority in the interpretation and application of it to a particular situation, particularly in lieu of any issue that may be addressed in subsequent sections.

Another consideration when writing this section is that of allowing for flexibility. That is, decision makers may need a clause in the policy that allows for a policy statement to be temporarily waived from time to time by a person of authority under certain conditions or guidelines. Such a clause allows those in authority to act with initiative (and still within policy boundaries) should unusual situations arise.

A CSP that is prepared in a final form and never reviewed for the appropriateness of its contents during its lifetime may quickly become a document that is either cumbersome or useless. A review section should formally set out the periodic and necessity for reviews of the CSP.

Rights and Responsibilities of KAC

There is a myriad of information that could be placed in this section. The content of this section assumes a large degree of importance when one considers recent statistics regarding the proportion of crimes involving computers that are committed by people internal (or recently internal) to the organization.

Some (but by no means all) issues that could be addressed here include:

- Personnel backups;
- Contact information;
- host configuration guidelines, including:
    - allocation of responsibility;
    - network connection guidelines;
    - authentication guidelines;
    - authority to hold and grant account guidelines;
    - auditing and monitoring guidelines;
    - passcode format, enforcement and lifetime guidelines; and
    - login banners;
- network construction, configuration and use guidelines, including:
    - allocation of responsibility;
    - supported protocols;
    - network design principles;
    - address allocation and authority guidelines; and
    - use of network management and other equipment;
- physical security guidelines; and
- Privacy guidelines.

There are no doubt many other issues and principles that could be discussed in this section. The content of this section is really a product of the basic philosophy of the organization providing the resource.

There could be a subsection devoted entirely to security incident handling principles. This subsection would be used directly in the construction of a set of procedures to be followed in the event of an actual security breach in progress. It could broach such issues such as:

- parties who should be notified, and the method and urgency of such notification;
- policy on the necessity, timing and requirements of any backups taken and logging that must be carried out;
- computer system and network isolation authority and guidelines;
- statement of entrapment policy (if this is not already expressed in the CSP philosophy); and
- Statement of policies and requirements should an alleged offender be traceable and possibly confronted (particularly where actions may be affected by external requirements such as a Statute dictating that Security Officers must identify themselves).

It may be desirable to also offer guidelines for liability of personnel with regard to security breaches. Such policies may tend to encourage people who are the victims of ignorance but honest intent to offer information that can be used constructively to prevent future incidents, rather than attempt to hide details of a breach that the employee may have (somewhat innocently) been involved in.

The absence of a Site Computer Security Policy leaves a large void in any organization's ability to operate effectively and maintain business continuity, and allows for ad-hoc decisions to be made by unauthorized personnel. Conversely, a well written and easily understandable Site Computer Security Policy provides an effective basis for decision making and planning. It gives the providers and users of a resource a clear understanding of what is expected, and what may be expected in return. Adherence to such a policy lends some evidence to an organization’s integrity and trustworthiness.

Observation Analysis:

1. No extended electrical power supplied to the server room.

Recommended Action:

THE VOLUNTEERS recommends that a power backup is provided for the server and related equipment.

Affected Users:
KAC IT department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

7.7 Method to authenticate ePI	
Rating	**Specification Standard:**
Complete	Integrity
Explanation	
Discusses what the organization should do to implement appropriate electronic mechanisms to confirm that its ePI has not been altered or destroyed in any unauthorized manner.	
These are the steps that need to be taken in order to reduce the risk to KAC's ePI: **Observation Analysis:** 1. All networks are on the LAN, and data is entered in 'real-time'.	
Affected Users: KAC IT Department	

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

7.8 Encryption and Decryption – Data in Transit	
Rating	**Specification Standard:**
Not Started	Access Control
Explanation	
Discusses what the organization should do to appropriately use encryption to protect the confidentiality, integrity, and availability of its ePI. Describes what the organization should do to appropriately protect the confidentiality, integrity, and availability of the ePI it transmits over electronic communications networks.	
These are the steps that need to be taken in order to reduce the risk to KAC's ePI: **Observation Analysis:**	

1. Some ePI information is being sent via email daily.

Recommended Action:
The Volunteers supports the use of some sort of encryption tool (like cryptomite) to encrypt the emails containing sensitive data.

Only Managers or Supervisors should have the ability to send ePI via email. A documented record should be kept on all emails that have been sent with ePI, this should include the following:

- Senders Name
- Senders Title
- Date Sent
- Recipient Full Name
- Recipient Organization Name
- Brief Description of what was sent

Affected Users:
IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

7.9 Encryption and Decryption – Data at Rest

Rating	**Specification Standard:**
Not Started	Access Control

Explanation

Discusses what the organization should do to appropriately use encryption to protect the confidentiality, integrity, and availability of its ePI. Describes what the organization should do to appropriately protect the confidentiality, integrity, and availability of the ePI that resides on the server.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:
1. This specification is not implemented in KAC.

Affected Users:
IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

8 Three Year to Five Year Plan

The below recommendations are to be completed (or considered) between 3 years and 5 years after the IT audit results have been presented.

8.1 Incident Response and Reporting

Rating	**Specification Standard:**
Partially Complete	Security Incident Procedure

Explanation

Discusses what the organization should do to maintain a system for addressing security incidents that may impact the confidentiality, integrity, or availability of its ePI. Defines what the organization should do to be able to respond effectively to security incidents involving its ePI.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. KAC does not have a documented approach to security breaches, whether physical to the specific location, or from an external source. Some incidence response capability is provided by SSI, but KAC should ensure that their needs are fully met.

Recommended Action:

The scope of this specification covers the response to and reporting of security incidents, including the identification of and response to suspected or known security incidents, the mitigation of the harmful effects of known security incidents, to the extent possible, and the documentation of security incidents and their outcomes. Below is a sample of what should be included in this procedure:

EXAMPLE:

All incidents, threats, or violations that affect or may affect the confidentiality, integrity, or availability of ePI must be reported and responded to in accordance with the following procedures:

a) Users must notify their local IT Support for issues involving viruses, local attacks, denial of service (DOS) attacks, etc. If an incident directly affects ePI, the user must immediately notify the Security Liaison for the user's Business Unit. If the assigned Security Liaison is unavailable, the user should report the incident directly to the IT Director Office.

b) Local IT Support must notify the main location if the incident affects or may affect other systems and networks. Local IT Support must notify there IT Security Liaison if the incident is a threat to ePI. If the Security Liaison is unavailable, the IT Director Office should be notified.

c) IT Support should investigate and propagate recommended updates or fixes to threatened or actual security incidents. IT Support also should notify the IT Director Office if a threat to ePI exists.

d) Each Security Liaison should aggregate and assess the severity of security incidents within their Business Unit involving ePI and report those incidents, when appropriate, to the IT Director Office. Incidents that should be reported include, but are not limited to:

- Virus, worm, or other malicious code attacks
- Network or system intrusions
- Persistent intrusion attempts from a particular entity
- Unauthorized access to ePI, an ePI based system, or an ePI based network
- ePI data loss due to disaster, failure, or error

e) The Security and Privacy Offices must notify each other of security or privacy issues if KAC determines that an

incident or issue could affect the other office. The IT Director Office must notify The Board of Directors if a security incident involves an outside entity or traverses the WAN network.

f) All correspondence with outside authorities such as local police, FBI, media, etc. must go through the COO Office or equivalent personnel.

Documentation of Security Incidents

All security related incidents and their outcomes must be logged and documented by each Business Unit. The IT Director Office also will document and log incidents and outcomes related to Security. Each Business Unit must develop and implement disaster recovery reporting procedures so that all instances of failures, outages, or data loss that involve critical ePI are logged internally within the Business Unit and all instances of failures, outages, or data loss that involve critical ePI are reported to the IT Director Office. The above processes and procedures must be documented and tested for effectiveness.

Mitigation of Harmful Effects of Known Security Incidents

The harmful effects of known security incidents will be mitigated by following the reporting procedures outlined above for notifying others within KAC of a known incident so that appropriate action may be taken. IT Security Liaisons will be notified of viruses and other malicious software and KAC-wide threats to ePI. Such notifications may be made by way of the IT Support distribution list or the IT Director Office. The IT Security Liaison is responsible for propagating these notifications within its Business Unit and ensuring that appropriate measures are implemented to mitigate the harmful effects of such security threats based on such notifications.

It is important to note that all KAC employees must be given the ability to report security incidents, no matter what the situation or infraction.

Regarding a physical security breach, this potentially could be more difficult to address and contain. The Volunteers was encouraged by the swipe card access utilized at KAC, and this can be seen as a major deterrent for malicious intent.

If, at any time, KAC chooses to employ a 'security guard' at any facility, there are several issues that need to be addressed with this personnel include the following:

- Signed Confidentiality agreement between KAC and each individual law enforcement personnel stationed in the lobby.
- Privacy training conducted on an annual basis with law enforcement personnel.
- Security Awareness training that includes potential scenarios that could occur at KAC – e.g. suspicious desktop usage, computer equipment being removed from the premise, or unauthorized persons in sensitive areas.

Again, KAC will need to account for those incidents that could happen during an after-hours situation as well.

The above is just an example of what could be included within this procedure. As with these types of processes, it must be tested and reviewed periodically to ensure completeness and functionality.

Affected Users:
IT Department & Operations

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			

2).			
3).			

NOTES:

8.2 Workforce Clearance Procedure

Rating	**Specification Standard:**
Not Started	Workforce Security

Explanation

Reviews what the organization should do to ensure that employee access to its ePI is appropriate.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. KAC needs to clearly document clearance procedures.

Recommended Action:

Group security and register-level security is currently not in place. Documentation needs to include how an employee's access and group membership within the File Server System is determined.

Affected Users:

Human Resources

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

8.3 Sanction Policy

Rating	Specification Standard:
Not Started	Security Management Process

Explanation

Indicates actions that are to be taken against employees who do not comply with organizational security policies and procedures.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. Sanction Policy should be specified in the employee computer use manual including what behavior is prohibited.

Recommended Action:

A) The employee manual needs to be reviewed for prohibited actions, and it needs to be documented that the specific action is sanctionable due to Security regulations.

B) Human Resources needs to have a documented procedure for what the sanctions are for each of these items, but this list can not be all inclusive due to the possible number of incidents that could occur on a daily/monthly basis. These sanctions need to include a general accounting of terminable and non-terminable actions and should be managed by the Human Resources department. Language should be inclusive enough to ensure that all KAC personnel are well aware of acceptable and unacceptable behavior.

THE VOLUNTEERS support the process of deleting user access on the day of termination. The Volunteers recommend, that KAC specifically detail this process within the policy. Documentation of this procedure will cover KAC legally.

C) If it is determined by KAC to provide employees with additional information on sanctions, the confidentiality training that is conducted would be an appropriate and recommended place to do so.

D) Enhance the occurrence reporting mechanism to incorporate the process for reporting sanctionable offenses through the investigation and follow-up process. This reporting mechanism should include employee incident reports through the appropriate channels. This feature should be documented within the policy and a checks-and-balances feature built into the system.

Affected Users:

Human Resources, Operations, and IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

8.4 Workforce Security

Rating	Specification Standard:
Partially Complete	Workforce Security

Explanation

Describes what the organization should do to ensure ePI access occurs only by employees who have been appropriately authorized.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. Clause within KAC job description outlining justifiable access to ePI.

Recommended Action:

KAC should approach this issue per each job description within the agency (e.g. from maintenance level personnel to CEO level) that includes a general outline on what access, per job description, the specific job will need to perform their daily functions. The intent of this recommendation is to encourage KAC to document. The key point is that this must be documented, reside within the individual personnel file, and reviewed for completeness.

Affected Users:

IT Director Officer & Human Resources

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

8.5 Maintenance Records Procedure

Rating	**Specification Standard:**
Not Started	Facility Access Controls

Explanation

Defines what the organization should do to document repairs and modifications to the physical components of its facilities related to the protection of its ePI.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. KAC does not address proactive maintenance on workstations, network equipment, or servers.

Recommended Action:

In The Volunteers experience, The Volunteers recommends that KAC initiate a maintenance plan for all workstations, network equipment, and servers on an annual basis. This would include the following and should be documented and tracked within the Track-It application:

- Equipment should be wiped down externally, especially around the air-intake grills for the processor fans.
- Equipment should be vacuumed out internally to clear dust and particle deposits on the motherboard, chassis, and cooling fans.

Please remember to take all necessary precautions when performing this task: Wear an anti-static band that is grounded to the case (not the motherboard), use dry wipes, unplug the equipment completely from any power-source, and if possible remove all monitor, mouse, and other connectors during the cleaning.

This annual maintenance plan will extend the life of the equipment, and lessen the time spent troubleshooting hardware failures. At a minimum, The Volunteers recommends this plan for KAC's mission critical servers and network equipment.

Affected Users:

KAC IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

8.6 Person and Entity Authentication

Rating	Specification Standard:
Not Started	Person and Entity Authentication

Explanation

Defines what the organization should do to ensure that all persons or entities seeking access to its ePI are appropriately authenticated before access is granted.

These are the steps that need to be taken in order to reduce the risk to KAC's ePI:

Observation Analysis:

1. KAC should build a checks-and-balances feature into this aspect of compliance. This could reside within the IT Departments and would provide a mutually assured method of making sure that all employees are appropriate at each level of access granted.

Affected Users:
KAC IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

9 IT Policies and Procedures

Background:

The Volunteers were not provided copies of the existing KAC policies. Instead, questionnaires were utilized to assess the current situation and to provide recommendations.

General Policy and Procedure Recommendations:

Below are the policies and procedures that The Volunteers feel needed to be created, or the policy might exist and needs more detailed content added to bring it into compliance. The items within this section are not deemed critical and can be resolved within the first 2 years after this assessment.

Other observations of the policies and procedures within KAC are as follows:

1. The Volunteers encourages KAC to create a 'Security Folder' that would contain all information related to Privacy, Security, Policy/Procedure, and relevant Plans as detailed in the above specifications section. This file would contain all policies and procedures, including all Disaster Recovery and Contingency Plans, as well as the processes in place that address each specification. This folder then can be used as a quick reference guide as the need arises.

2. Frequent revisions / review is highly encouraged on each policy form. The Volunteers encourages KAC to add a field on the policy header that reads 'Current Review Date' as this makes the policy 'seem' more time-relevant.

    a. The Volunteers agree that reviewing policies each year is a strong administrative stance; but this process tends to be time consuming. The Volunteers encourages KAC to review all policies and procedures at least every three (3) years. In addition, KAC will need to develop a Policy Revision Team that will own all modification to the policies.

3. KAC, in The Volunteers experience, should have all outside vendors, who are granted physical access to any area of the facility, sign a Confidentiality Agreement prior to any work being performed on the premise. Also included in this category should be all vendors that might have electronic access to ePI whether directly or indirectly. These agreements should be stored in a central location, or be apart of their company file on record with Operations and Maintenance. This type of agreement will only need to be signed once and then stored within that vendors file.

    - Diskettes, DVDs and CD-ROM's

        a. This aspect should only be performed when and if ePI was stored on this type of media. All other media can be discarded immediately after use if the media did not contain ePI.

    This policy will need to be reviewed requently, especially when new vendors are brought in to perform work.

4. Maintenance & Emergency Management Plan: These policies should be incorporated within the KAC Center Disaster Recovery Policy and Procedure, so as to present on clear and concise document. Such information can be obtained in the above section labeled Disaster Recovery Plan.

    - If a computer breach affects ePI directly or indirectly, each party agrees to notify the other within X number of days. The affected party will then remediate the incident, to the best of their abilities. If the affected party can not do so within the specified timeframe, this contract will be null and void.

5. Creation of a Center wide Policy Revision/Deletion Log: this log details when a specific policy within KAC has been reviewed and/or deleted. The Volunteers is in full agreement on maintaining this type of log. Special care should be taken when deleting or discontinuing the use of a policy. Also, as past experience has shown, all discontinued policies should be maintained indefinitely in a file so it can be easily referenced if the need arises.

6. The Volunteers also recommends that if KAC has a vendor onsite that is using a desktop or related device, and needs network access to perform a function or duty – that vendor should, as a normal course of operation, by instructed to have all anti-virus software updated prior to arrival. This will prevent the possibility of a virus outbreak on the KAC network.

9.1 Computer Usage Restrictions for Remote Network Users

Rating	
Not Started	

Explanation

Defines the method of connection to the main database by remote users and dictates what operations can be performed by remote users.

Observation Analysis:

1. This should only be in regards to outside vendors (SSI) who have access to critical / sensitive information

Recommended Action:

- Institute as apart of the vendor file and signed document of this type outlining allowable and disallowable actions on the part of the vendor while they are accessing the server.

Observation Analysis:

2. The Volunteers believe a concise, direct policy body should be created with full approval and ownership by all departments.

Affected Users:

All remote users under KAC engagement

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

9.2 General Acceptable Use Policy

Rating
Partially Complete

Explanation

This policy is targeted at the end-user, and should be seen as the authority's guideline to all personnel on what behavior is expected of them while an employee of KAC. This document should be no more than one-two pages, bulleted, and very easy to read and understand.

Observation Analysis:

1. The Volunteers believe a concise, direct policy body should be created with full approval and ownership by all departments. Although technical security controls can be implemented without guiding policies, the expectation of reasonable security cannot be achieved without the assistance of the end user. The end user is capable of circumventing even the most rigorous controls, as that employee holds a position of trust within the network. Reasonable policies and policy awareness initiatives are primarily intended to mold the behavior of the end users. Then, given that technical controls and user awareness are never perfect, an automated system of monitoring and enforcement are added to help complete the picture. Since the depth of these different elements is dependent on the organization's needs, this model holds true for all departments and remote locations within KAC.

Observation Analysis:

2. While this policy is targeted at the end-user, language of the document can make it very difficult to determine what is required and what is not. While most organizations find it necessary to have a policy that's more legal in nature, The Volunteers highly recommend the creation of a brief policy synopsis document whose only purpose is to foster a true understanding of the security issues facing the Organization and the end-user's responsibilities related to information security matters. This document should be no more than one-two pages, bulleted, and very easy to read and understand.

Recommended Action:

Listed below are some sections that KAC should have incorporated into this policy:

- **Passcodes**
  - Reasonible passcodes for each workstation should be produced by the IT Dept and changed frequently
- **Information Controls**
  - Access and use of KAC Center and ePI information
  - Legal statement on the authorized use of KAC Center and ePI information
- **Personally owned computers and software**
  - State KAC Center policy on the use of personal computers to access KAC Center systems and networks.
- **Data Classification**
  - Clearly summarize what data and information that should be handled as sensitive
- **Software installation**
  - State the KAC procedure on installing new software on workstations – this should be forebidden except when critical to the end users job, and only then approved by the IT Dept.
- **Unauthorized copying of licensed software**
  - Clearly detail the policy and procedure for this type of infraction
- **Personal Computers and Workstations**
  - Detail the behavior that is acceptable and unacceptable on company resources and equipment

- **External Network Connectivity**
  - Outline how KAC employees external to the network are to interact and gain access back to company resources and databases

- **Wireless Technology**
  - Summarize acceptable use of wireless technology within the KAC enterprise at all locations. This should include 'smart' devices like Palm-Pilots, Blackberry's, Treo's, tablet PC's, or other devices that can store information and access networks wirelessly.

- **Encryption**
  - Detail expected behavior on using the encryption email technology and who is authorized to use within the KAC organization. On the whole – no one should be able to use this type of software except the IT Dept.

- **Desktop Computers**
  - Summarize the expected recipients of desktop computers, what the desktop should be used for, how to access the network securely, how to physically protect the desktop from theft or damage, and data security

- **Telephone, Fax, Electronic Mail**
  - This section deals solely with the use or misuse of these company resources, what information is shared with whom, how to report abuse or attempts at soliciting sensitive information, and the proper method of transmission via fax or email.

Affected Users:
All enterprise users

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

9.3 Acknowledgement of Security Responsibilities

Rating	
Not Started	

Explanation

This basic policy is intended for all employees and should be a one-two page overview of KAC Center security guidance, acknowledged by all users with their signature. New employees should be required to read and acknowledge these responsibilities during orientation.

Observation Analysis:

1. The Volunteers believe a concise, direct policy should be created with full approval and ownership by all departments.

Observation Analysis:
2. This can be an appendix on the General Acceptable Use Policy.

Affected Users:
All enterprise users

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

9.4 Information Security Policy

Rating	
Not Started	

Explanation

Establishes Information Security Policies for KAC Center and provides a basis for Security Configuration Guidelines (SCG) and related procedures. The Information Security Policy defines specific accountability for information protection and each user's responsibility for the protection of information. Numerous individual policies not identified in this outline are internal to this document, depending on decisions made by KAC Center on policy separation.

Observation Analysis:
1. The Volunteers believe a concise, direct policy body should be created with full approval and ownership by all departments.

Observation Analysis:
2. Paper and Electronic Records retention and protection section

Recommended Action:

- Emergency access to critical passcodes
  - This sub-section outlines the procedure within the Emergency Mode Operation Plan. This should only be shared internally with the employees that is responsible for the plan and not posted to the Intranet.
- Destruction of magnetic media
  - This sub-section outlines the procedure within the Accountability of Device and Media and the Device and Media Controls – Disposal specifications. This should only be shared internally with the employees that is responsible for

the plan and not posted to the Intranet.

- Destruction of sensitive papers
  - This sub-section outlines the procedure within the Accountability of Device and Media and the Device and Media Controls – Disposal specifications with regard to paper copy. This should only be shared internally with the employees that is responsible for the plan and not posted to the Intranet.

Affected Users:
All enterprise users

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

9.5 Acceptable Use Policy – Hardware/Software

Rating	
Not Started	

Explanation

This policy outlines the acceptable use of computer equipment at KAC Center. These rules are designed to protect the user and KAC Center from inappropriate use issues, such as virus attacks, compromise of network systems, and legal exposures.

Observation Analysis:

1. The Volunteers believe a concise, direct policy body should be created with full approval and ownership by all departments.

Recommended Action:

- **Policy Maintenance**
  - Policy Acceptance
    - Users must acknowledge acceptance of KAC Center security policies (in writing) prior to being granted system access. This can be apart of the KAC orientation or apart of the initial Training on KAC systems.

- **End-user responsibility**
  - Protection of sensitive information – This needs to be apart of the sign-off sheet and reinforced during the training section involving the KAC computer system.
  - Protection of on-screen information – This sub-section revolves around the provision listed in the Workstation Security (e.g. the protective screen to prevent unauthorized viewing of the monitor)
  - Passcode management – This sub-section strictly involves the Passcode Management specification and the procedure that KAC uses to maintain this portion of the policy.
  - Security violations – This sub-section strictly involves the Sanction Policy and the procedures that KAC uses to

maintain this portion of the policy.
- Security violations – This sub-section strictly involves the Sanction Policy and the procedures that KAC uses to maintain this portion of the policy.

Affected Users:
All enterprise users

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

9.6 Anti-Virus Policy

Rating
Not Started

Explanation

Defines the corporate guidelines for reducing the risk of computer viruses on the KAC Center network. Includes mandatory controls such as anti-virus KAC's, specific protocol scanning activities, anti-virus software standards, and distribution of updates. Procedures for notifying the workforce of new and potential threats from malicious code such as viruses, worms, denial of service attacks, or any other computer program or code designed to interfere with the normal operation of a system or its contents and procedures for protecting systems from the aforementioned malicious software.

Observation Analysis:

1. The Volunteers believe a concise, direct policy body should be created with full approval and ownership by all departments.

Recommended Action:

- **Anti-virus**
  - Corporate Standard – what anti-virus software is being used, where it is being used, how it is updated
  - User Responsibilities
  - All CDs/DVDs, e-mail, and downloaded files must be scanned. As with the above sections, this policy is strictly internal to the IT Department and those designated on the Executive Level.
  - Do not leave CDs/DVDs in computer when it shuts down – this sub-section may be a non-issue depending upon

what procedures or limitations KAC chooses to incorporate at the workstation level. These limitations are listed in the Workstation Security section.

Affected Users:
All enterprise users

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

9.7 Internet Security Policy

Rating
Not Started

Explanation

Defines standards for the secure configuration of all Internet-facing hardware and software, including specific protocol support. Defines standards for security testing and configuration control for all hardware and software.

Observation Analysis:
1. NONE IN PLACE

Recommended Action:

- **Internet Connectivity**
  - All users must use only approved KAC Center Internet access points
    - All Internet use will be monitored – this sub-section will refer to the Sanction Policy as it dictates punishable offenses and the consequences of unauthorized behavior. This sub-section should also be listed within the Acceptable Use Policy and documented within the Workstation Security specification.
    - Detail inappropriate behavior – this should be specific to ePI and detail unauthorized behavior as referenced in the Sanction Policy.

Affected Users:
IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

9.8 Extranet Policy

Rating
Not Started

Explanation

Defines specific connection requirements for third party organizations requiring access to KAC Center networks, including appropriate security filtering, and encryption standards if required. Defines the standard Extranet security infrastructure.

Observation Analysis:

1. The Volunteers believe a concise, direct policy body should be created with full approval and ownership by all departments.

Observation Analysis:

2. This policy should be incorporated into the Business Associate Contract agreements. KAC should reevaluate this policy, as well as the Business Associate Contract annually to make sure that all Business Associates adhere to the KAC policy. The Volunteers also recommend that KAC obtain information from all Business Associates as to their status regarding Security and their assessment ratings.

Affected Users:

All Business Associates and IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

9.9 Remote Access Policy

Rating
Not Started

Explanation

Defines standards for remote access to the KAC Center network from any host or network external to the organization, including authentication standards, appropriate dial-in and VPN access and its use by authorized personnel.

Observation Analysis:

1. The Volunteers believe a concise, direct policy body should be created with full approval and ownership by all departments.

Observation Analysis:

2. This policy is strictly internal to the IT Department and the remote users involved and should not be placed onto the Intranet for general KAC employee consumption.

Observation Analysis:

3. KAC will need to have a separate signed agreement form for this policy as it will only be used by those accessing the KAC network from outside the standard protocol.

Observation Analysis:

4. Consideration must be made for third party vendors and those under the Business Associate Contracts as an inclusion into those separate policies.

Affected Users:

All remote users under KAC employment

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

9.10 IT Assessment Policy

Rating
Not Started

Explanation

Provides the authority for Management to conduct IT assessments and remediate identified risk within the organization.

Observation Analysis:

1. NONE IN PLACE

Observation Analysis:

2. As stated above, KAC needs to incorporate an internal document that outlines the hierarchical authority to conduct planned and unplanned risk assessments within the organization.

Recommended Action:

- The planned assessments need to be added to the annual budget, documented as being apart of the IT Security initiative to maintain continued proper IT guidelines and procedures.

Affected Users:
IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

9.11 Security Configuration Guidelines (SCG)

Rating
Not Started

Explanation

Defines technical standards for the secure configuration of all major operating platforms within KAC Center. Intended to be used as a resource for technical personnel responsible for the configuration of servers and network devices. Defines the basis for host-level security audits and compliance monitoring on specific platforms.

Observation Analysis:

1. NONE IN PLACE

Recommended Action:

- **Policy Overview**
  - **Objective**
    Establish Information Security Policies for KAC Center and provide a basis for Security Configuration Guidelines (SCG) and related procedures. The KAC Center security program is focused on providing the foundation for assuring the confidentiality, integrity, and availability of all KAC Center resources, whether processed and stored on computer systems, transmitted over networks, or maintained in any form. The Information Security Policy defines specific accountability for information protection and each employee's responsibility for the protection of information.

  - **Scope**
    The KAC Center Information Security Policy is mandatory for all KAC Center departments, employees, contractors, vendors, students, and others having access to KAC Center information resources.

- **Security Configuration Guidelines (SCG)**
  - Describe their purpose and intent of this policy and the incorporation of all sub-sections within this document
  - List the available guidelines
  - Detail enforceability and waiver processes – as dictated in the Sanction Procedure and Termination Policy guidelines.
  - Incorporate a testing and revision process within this document to include any operational changes to the environment that contains ePI. This would include adding network hardware/software, new network ports, new access points to the internet, configuration changes to routers/switches, or similar additions or modifications.

Affected Users:
IT Department

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

9.12 Workforce Security Policy

Rating
Partially Complete

Explanation

The scope of this policy covers the procedures each Business Unit must implement to ensure that Workforce members who work with EPI or in locations where EPI is available are appropriately supervised, that Workforce members are granted appropriate access to EPI, and that Workforce members' EPI access is terminated when employment ends or when a determination is made that such access should be terminated or otherwise modified.

Observation Analysis:

1. The Volunteers believe a concise, direct policy body should be created with full approval and ownership by all departments.

Observation Analysis:

2. The Volunteers believe that this policy is sufficiently covered under the other policies listed above.

Affected Users:

All enterprise users

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

9.13 Termination Procedure and Policy

Rating
Not Started

Explanation

Each Business Unit must develop and implement procedures for terminating access to EPI when the Workforce member's employment ends or when the access granted is determined to be no longer appropriate.

Observation Analysis:

1. The Volunteers believe a concise, direct policy body should be created with full approval and ownership by all departments.

Observation Analysis:

2. Currently, no employee that voluntarily or involuntarily terminates their employment with KAC is made to sign a confidentiality agreement.

Recommended Action:

In The Volunteers experience, The Volunteers recommends that all personnel that are terminated for cause or voluntarily resigns should sign a confidentiality agreement with KAC. This could be the same agreement that is used for all new hires. This will coincide with the employee closing meeting prior to vacating the premise.

Observation Analysis:

3. Additionally, KAC should incorporate a clause within the Termination Procedure that deals with a person's level of access.

Recommended Action:

If it is deemed that the person, who either voluntarily or for cause, leaves KAC's employment and they had Administrative rights (admin, superuser, etc.) to systems containing ePI, that all Admin and Superuser passcodes be changed immediately no matter the reason for termination.

Observation Analysis:

4. KAC currently does not have a separate process for voluntary or involuntary terminations. Special care should be taken to separate these two termination distinctions. Terminations for just cause should be seen as a greater security risk than voluntary resignations and needs to have other specific procedures that are used during this event, these would include:

Recommended Action:

- Depending upon the offense, if it was security related, a picture of the ex-employee should be kept at the front desk for a period of several months.
- The uniformed law enforcement official in the lobby should be notified and made aware of the situation
- If the ex-employee worked at another facility, all staff members at that facility should be notified of the situation
- Deletion of all user accounts should be done prior to the person leaving the KAC premise.
- Depending on the severity of the incident, discussion should be done on changing physical passcode access, or changing locks at the appropriate location

Likewise, a detailed process checklist should be devised to be used during the termination of an employee. This would be a step-by-step list documenting the procedure that occurs with all terminations.

Affected Users:

All enterprise users

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

9.14 Security Awareness Training Policy and Procedure

Rating	
Not Started	

Explanation

To ensure that the organization workforce is properly trained and made aware of security policies, procedures, potentials threats, and incidents.

Observation Analysis:

1. The Volunteers believe a concise, direct policy body should be created with full approval and ownership by all departments.

Observation Analysis:

2. KAC Center is currently in the process of developing a program to achieve and maintain security awareness. Since the security policies themselves are being completed, The Volunteers recommends focusing on the completion of the policies identified in this document first – allowing KAC Center to build their awareness program around an easily understood policy body.

Observation Analysis:

3. An effective Security Awareness program is the best defense against many different exposures, including social engineering, passcode issues, inappropriate use issues, and other critical elements specified in policy. An KAC security awareness program will ensure that all users are constantly aware of the importance of security in their daily duties. Annual briefings, newsletters, Intranet messages e-mails, posters are all methods used to enhance awareness. Minimally, the awareness program should ensure that all users have read and acknowledged (by signature) their understanding of a brief policy synopsis. All new employees should receive this document during in processing, and existing users should be asked to read and sign it as well.

Observation Analysis:

4. KAC should also focus on developing an ongoing security awareness program that outlines continual reminders to KAC personnel on such security topics as: Incident Reporting on Suspicious Activity, Unauthorized requests for sensitive information, peer security reviews, security awareness postings in the common areas, and cubicle and office reminders on locking desktops and file cabinets.

Recommended Action:

- **Security Awareness**
  - Describe the Security Awareness Program, prescribing the frequency of awareness training and placing the responsibility.
  - KAC, in The Volunteers experience, should incorporate a 'walk-about' process that, at random, selects various work-areas to be inspected for Security compliance. This program could be used on a quarterly basis, and by the end of the year ensure that all work spaces and environments had been visited. Take special care not to single out any one group, department, or individual, and all KAC personnel will be included (from the CEO office down to the maintenance closet).

Observation Analysis:

5. As KAC adds and modifies certain policies, in The Volunteers experience, not all KAC staff should have access to sensitive internal information and processes. It is The Volunteers recommendation that if the decision is made to post all policies and procedures to the company intranet, there should be a password protected area within the intranet

that contains information for Executive Level staff only. This could include the Router and Server Security Policy, the 'Walk-About' process documentation, or the Workforce Clearance Policy et al.

While the physical security at KAC is deemed sufficient – the above recommendations will enhance KAC's overall stance on security and will provide all employees the necessary tools and reminders.

Affected Users:
All enterprise users

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

9.15 Workforce Clearance Policy and Procedure

Rating	
Partially Complete	

Explanation

The background of all workforce members must be adequately reviewed during the hiring process. When defining an organizational position, the HR Department and the hiring manager must identify and define both the security responsibilities of and level of supervision required for this position. All employees who have access to ePI must sign a confidentiality agreement and a 'conditions of employment' document that states their commitment to and understanding of their responsibility for the protection of confidentiality, integrity, and availability of KAC's ePI.

Observation Analysis:
1. The Volunteers believe a concise, direct policy body should be created with full approval and ownership by all departments.

Observation Analysis:
2. KAC must document and review all workforce clearance policy and procedure, and make sure that there is a checks and balances feature built into section.

Observation Analysis:
3. The Volunteers recommend that, at a minimum, all due diligence be performed for all new hires regardless of position.

Recommended Action:
For those employee positions that deal strictly with ePI, special care needs to taken in validating those individuals and checking the proper databases for past indiscretions - drug/alcohol convictions, identity theft convictions, mail fraud or similar background, and gambling convictions.

Observation Analysis:
4. It is at the Manager discretion on hiring new personnel with past infractions.

Recommended Action:
There should be a checks-and-balances procedure built into this process. In The Volunteers experience, the Manager should recommend to the HR Department that new personnel be hired by KAC, but the ultimately authority in hiring a person with past infractions should lie with the HR Department. This will alleviate discrepancies and provide a better documental process should an issue occur.

Affected Users:
Human Resources

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			
3).			

NOTES:

9.16 Sanction Policy

Rating	
Partially Complete	

Explanation

Defines the different levels of possible incidents within the organization and gives clear understanding to the penalties that could occur.

Observation Analysis:
1. The Volunteers believe a concise, direct policy body should be created with full approval and ownership by all departments.

Recommended Action:

- **Disciplinary Measures**
  - Detail the importance of adhering to KAC Center policy
  - Must include process for prevention, detection, containment, and correction procedures
  - Provide warning on which actions may be taken for policy violations – must be as specific as possible
  - Provide detailed list of unacceptable behavior and the specific punishment per line item

Affected Users:
All enterprise users

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

9.17 Assigned Workforce Responsibility Policy and Procedure

Rating	
Partially Complete	

Explanation

Each Business Unit must develop and implement procedures to ensure that the EPI access of its Workforce members is appropriate when granted and continues to be appropriate on an on-going basis. Each Business Unit must maintain documentation detailing each Workforce member's current role and responsibilities and the EPI access required for such role and responsibilities.

Observation Analysis:

1. The Volunteers believe a concise, direct policy body should be created with full approval and ownership by all departments.

Recommended Action:

- Policy Maintenance
  - Detail who is responsible for maintaining and reviewing policy
  - Detail frequency of policy updates – KAC should review and update their policy and procedure structure annually.
  - Detail process for getting policy changes approved
  - Policy Exceptions
  - Detail process for requesting exceptions through the Board

- **Key Roles and Responsibilities**
  - **IT Director**
    - Approval and oversight of Information Security Policy
    - Providing resources necessary to carry out the Information Security Program

  - **IT Director Officer**
    - Providing guidance, direction, and authority for the KAC Center Information Security Program
    - Serving in lead role to evaluate changes submitted to the Configuration Control Board
    - Providing direction and technical expertise to ensure that KAC Center information is properly protected
    - Coordinating and directing specific actions to ensure the security of computer systems and networks
    - Performing information security vulnerability assessments
    - Investigating information security incidents to include investigations across business units
    - Developing, maintaining, and distributing Information Security Policy, Security Configuration Guidelines, and related procedures
    - Providing security specifications for vendor products
    - Providing security guidance for in-house application development
    - Providing advice and assistance on the implementation of new security architectures and security controls
    - Review and reconcile requests for policy exceptions
    - Managing the KAC Center Security Awareness Program

Group security and register-level security is currently in place and appropriate. Documentation needs to include how an employee's access and group membership within the File Server system is determined.

Observation Analysis:
2. Currently, KAC has a dictated policy on annual reviews of ALL policies and procedures by the Board of Directors.

Recommended Action:
In The Volunteers experience, The Volunteers recommends that this process be delegated to the management staff of KAC. This will save time and resources for KAC, and increase efficiency. Within the scope of this arrangement, KAC should centralize the review and revision of all policies and procedures to one (1) department. In The Volunteers experience, this aspect should be delegated to the Human Resources Department exclusively. This will provide a greater level of adaptation within the organization and alleviate the need for committee process. In accordance with this new procedure, the KAC HR staff should consider reviewing all policies annually – e.g. the review should incorporate a process that visually 'scans' the policy for completeness and signed off per the applicable calendar date. A revision process should, as applicable, be performed every two to three years. If a department policy is changed, this should be reported to HR, and depending upon the revision timeframe, approved and updated appropriately.

Affected Users:
Human Resources

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

9.18 Incident Response and Reporting Policy and Procedure

Rating	
Partially Complete	

Explanation

Defines the method and procedure for addressing all security incidents within the organization.

Observation Analysis:

1. The Volunteers believe a concise, direct policy body should be created with full approval and ownership by all departments.

Recommended Action:

- **Telephone & Voice-mail**
  - Verify need to know – all personnel should be trained in responding to requests of information, especially when associated with ePI
  - Never provide passcodes or system details
  - Proper use of voicemail system – need to document proper use as it relates to what information is left on a person's voice-mail, especially in regards to ePI

- **Duty to report**
  - Any attempt to gain passcode information – whether via email, possible phishing web-site, or telephone conversation
  - Any suspicious behavior on systems
  - Suspected or known breaches of IT systems
  - Suspected virus activity

  - **Audit**
    - Reviewing and assessing KAC Center adherence to security policy
    - Reporting audit findings to executive management – this procedure must be documented, reviewed and tested

- **Incident Response**
  - Emergency access to critical passcodes – as it relates to the Passcode Management recommendations and Emergency Mode Operations
  - Compromised hosts
  - Assessing system damage – as it relates to the Risk Management section and computer forensic capability
  - Passcode changes prior to resumption of service – detail the procedure on resetting passcodes, especially on mission critical servers, after a security breach
  - Reporting to authorities – documents who has direct responsibility on reporting incidents to the local or state police, and where applicable the FBI.
  - KAC should have a clearly documented policy on self-disclosure to the media regarding Sentinel Events. This should include who will provide the information, and how it will be provided.
  - For Business Associates, KAC should have a clearly defined method of disclosing information to their Business Associates regarding Sentinel Events. This should include who will provide the information, and how it will be provided.

Affected Users:
All enterprise users

TASK	ASSIGNED TO	COMPLETED DATE	COMMENT
1).			
2).			

NOTES:

8 Appendix References

Vendor Security Sites

Microsoft Security website
http://www.microsoft.com/security

Cisco Network Security
http://www.cisco.com/go/security

Cisco PSIRT Advisories
http://www.cisco.com/warp/public/707/advisory.html

Security Procedures Guidance

National Security Agency Security guidelines
http://nsa1.www.conxion.com/win2k/index.html

CMU's Handbook for CSIRT's
http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf

CERT Responding to Intrusions Security Improvement Module
http://www.cert.org/security-improvement/modules/m06.html

General Security Sites

Security Focus
http://www.securityfocus.org/

CERT
http://www.cert.org/

NIPC
http://www.nipc.gov/

Sans
http://www.sans.org/

ICAT
http://icat.nist.gov/icat.cfm

CONTACT INFORMATION

Project Lead

Jonathan Grimes
Volunteer – CommunityCorp
Technology for Social Good
Office: 614-217-9651
jonathan.x.grimes@jpmchase.com

Technical Lead

Murugan Subramaniyan
Volunteer – CommunityCorp
Technology for Social Good
Office: 614-213-5491
muruganandam.subramaniyan@jpmchase.com

Technical Lead

Pelayo Montoto
Volunteer – CommunityCorp
Technology for Social Good
Cell: 614-900-5407
pelayo.montoto@chase.com