variux

[v. var-E-ux] 1. dynamic user experience

# Internal Audit Questionnaire

***Table of Contents***

**Page**

# SECTION A: FREQUENTLY ASKED QUESTIONS (FAQ)

What is this?

This questionnaire was originally developed to survey areas of concern, identified by Internal Audit, in an IS LAN environment. We feel that by making this tool available to you, you can conduct your own internal review. This will aid you in the identification of risks in your installation and assist you in making an informed judgment as to what action to take to address these risks.

What is it intended to do?

This questionnaire surveys physical and logical security, backup and recovery, virus protection, software licensing, and trusted networks. Please note, this questionnaire is not intended to cover all issues in great detail, but we believe it covers the most important ones.

What if I'm responsible for multiple servers/systems?

If policies in your department are set differently for machines run centrally by you as compared to those run by individual labs/departments, then a separate questionnaire should be completed by each area, always taking into account the trust relationship between the installations.

Technology constantly changes, what if this survey is obsolete?

We view this questionnaire as a living document. It will continue to change as technology changes, and as we use it and gather experience with its effectiveness.

What is an Administrative workstation?

Any device (laptop, desktop, IPAD….etc) that stores or accesses proprietary or other protected data.

If you have any questions please contact Variux at 678-667-2185

# SECTION B: INSTRUCTIONS

If this document is part of a self-assessment review, please read & notate the individual(s) who completed this questionnaire:

Complete a separate questionnaire for each ***administrative*** (e.g. machines store or access proprietary or other protected information) LAN/network environment. When you use this questionnaire, remember it is not tailored to any specific hardware or software. You must take the specifics of your site into consideration at all times. It means that you must look at each issue, then at the risk it poses to your system and the data your system(s) contain. This does not mean that if an issue is not addressable by your installation, it is not important. It only means that you should address the risk the issue poses; based on your installation and the security level your department is comfortable with for the information in your system.

COMPLETED BY:

Name:
_____

Title:
_____

Date Completed: _____

Phone Number: _____ E-Mail: _____

Name:
_____

Title:
_____

Date Completed: _____

Phone Number: _____ E-Mail: _____

# SECTION C: GENERAL INFORMATION

**Note:** This section is for information purposes only and a "No" answer does not necessarily indicate a violation of business policy or generally accepted industry practices.

1. Administrator(s):

   _____

2. Administrative LAN Name:

   _____

3. Server(s):

   What network operating systems are running on your ***administrative*** server(s)?

| | # of Servers | Version, release, SP | |
|---|---|---|---|
| ☐ Windows Server 2012 | _____ | _____ | _____ |
| ☐ Windows Server 2008 | _____ | _____ | _____ |
| ☐ Windows Server 2003 | _____ | _____ | _____ |
| ☐ Novell/Netware | _____ | _____ | _____ |
| ☐ Linux | _____ | _____ | _____ |
| ☐ Solaris | _____ | _____ | _____ |
| ☐ MacOS X Server 10.11 | _____ | _____ | _____ |
| ☐ MacOS X Server 10.10 | _____ | _____ | _____ |
| ☐ MacOS X Server 10.9 | _____ | _____ | _____ |
| ☐ Other (please list below…include number and version): | | | |

4. User Workstations:

What operating systems are running on your user ***administrative*** workstations?

| | Version, release, SP | |
|---|---|---|
| ☐ Windows 10 | _____ | _____ |
| ☐ Windows 8 | _____ | _____ |
| ☐ Windows 7 | _____ | _____ |
| ☐ Windows XP | _____ | _____ |
| ☐ Linux | _____ | _____ |
| ☐ Solaris | _____ | _____ |
| ☐ Apple/Macintosh 10.11 | _____ | _____ |
| ☐ Apple/Macintosh 10.10 | _____ | _____ |
| ☐ Apple/Macintosh 10.9 | _____ | _____ |
| ☐ IPAD | _____ | _____ |
| ☐ Other (please list below…include number and version): | | |

## SECTION D: DOCUMENTATION

1. Do you have the following documentation for the administrative LAN(s)?

| | | |
|---|---|---|
| System Schematic | ☐ Yes | ☐ No |
| IP Addresses (subnets) | ☐ Yes | ☐ No |
| Data Backup and Protection | ☐ Yes | ☐ No |
| Change Control and Configuration Mgmt. | ☐ Yes | ☐ No |
| Acceptable Use | ☐ Yes | ☐ No |
| Network Security, Access Control and Device Configuration | ☐ Yes | ☐ No |
| Sanitization of Hard Drives | ☐ Yes | ☐ No |
| Reassigning workstations | ☐ Yes | ☐ No |
| Mobile Devices | ☐ Yes | ☐ No |
| Software Use | ☐ Yes | ☐ No |
| Hardware Inventory* | ☐ Yes | ☐ No |
| Software Inventory* | ☐ Yes | ☐ No |
| Other Organizational Unit/Departmental Policies | ☐ Yes | ☐ No |

**Please provide copies of above noted policies to Internal Audit.**

* Copies of Inventories are not necessary. We will view the details during the audit visit.

# SECTION E: ADMINISTRATION

**Critical updates and patches:**

1. Do you have automated procedures in place for applying critical updates to operating systems of all servers? ☐Yes ☐ No

_____

_____

   A. Do you have procedures in place to regularly review the operating system, databases, and software applications to ensure the process is working properly? If so, please explain:

_____

_____

2. Do you have automated procedures in place for applying critical updates to operating systems of all administrative workstations? ☐Yes ☐ No

_____

_____

   A. Do you have procedures in place to regularly review the operating system, databases, and software applications to ensure the process is working properly? If so, please explain:

_____

_____

3. Do you have automated procedures in place for applying critical updates to applications residing on network systems? ☐Yes ☐ No

4. When setting up new computers, how do you assure they have the most recent service packs, fixes and patches prior to connecting them to the network?

_____

_____

5. Do you utilize Network Access Control (NAC) measures to check system health prior to allowing a system to connect to your network?
   _____
   _____
   _____

**Wireless LANs:**

1. Do you have wireless LANS? ☐Yes ☐ No
2. Do you have any self-maintained guest wireless LANS? ☐Yes ☐ No
3. Do you perform regular scans looking for rogue wireless access points? ☐Yes ☐ No

**Internally Controlled or Restricted Data:**

1. What kind of client data do you store is included?
   a. Name and Home Address ☐ Yes ☐No
   b. Company Name and Work Address ☐ Yes ☐No
   c. Personal Phone Numbers ☐ Yes ☐No
   d. Social Security, Driver License, EIN, or similar ☐ Yes ☐No
   e. Medical Records ☐ Yes ☐No
   f. Legal records ☐ Yes ☐No

   A. If yes, is access to the records protected in compliance with FERPA, HIPAA, etc. regulations? ☐ Yes ☐ No

   B. If yes, how is the data protected?

   _

2. Are SSNs stored electronically? ☐ Yes ☐ No

A. **If yes, please provide a copy of the completed SSN Authorization Request and Network and System Requirements for SSN's document as required by the Privacy Office.**

3. Do any of the servers or workstations collect or process credit card transactions?
   ☐ Yes ☐ No

   A. If yes, has SOS been contacted and the PCI DSS Self-Assessment Questionnaire been completed?
      ☐ Yes ☐ No

      1. If yes, please provide a copy of the Self-Assessment Questionnaire.

4. Is any other form of Personally Identifiable Information (PII) stored on the network?
   ☐ Yes ☐ No

   A. If yes, please explain:

5. Have you implemented a two-step authentication process with a true single use password (i.e. SecurID token) to secure Internally Controlled or Restricted Data?
   ☐ Yes ☐ No

6. Have you implemented full disk encryption on all desktops and laptops which may house Internally Controlled or Restricted Data?
   ☐ Yes ☐ No

7. Have you implemented Individual File Encryption on servers or workstations to secure Internally Controlled or Restricted Data?
   ☐ Yes ☐ No

   A. If yes, please describe where Individual File Encryption has been implemented.

B. If no, have appropriate file or folder level permissions been implemented to control access to Internally Controlled or Restricted Data?

☐ Yes ☐ No

8. Have you implemented Application Level Firewalls for all Web applications hosting Internally Controlled or Restricted Data?

☐ Yes ☐ No

9. If you answered "Yes" to any of questions 1-4 above, is there a host based IDS or file integrity monitor (e.g., SNORT, Tripwire) for all servers storing non-public information (FERPA, HIPAA, PII, Credit Cards…etc)?

☐ Yes ☐ No ☐ N/A

A. If yes, please describe the host based device and your monitoring procedures.

_____
_____
_____
_____
_

10. Have you performed a Personally Identifiable Information (PII) scan of **all**

Servers ☐ Yes ☐ No
Laptops ☐ Yes ☐ No
Workstations ☐Yes ☐ No

A. If yes:

1. Do you have plans to rescan the machines on a regular schedule?

☐ Yes ☐ No

a. If yes, what is the frequency of the rescans?

_____

B. If yes, how are you assuring there is remediation of all identified potential PII information (e.g. reviewing console activity of user's scans)?

a. If you are not assuring there is remediation, why not?

_____

_____
_____

C. If users are identified who are not remediating identified potential PII data, what steps are in place to get compliance from them?

_____
_____
_____
_____

D. If there are multiple profiles on the computers, how do you assure that PII is scanned for on every profile?

_____
_____
_____
_____

11. Is any Internally Controlled or Restricted data maintained in a cloud based storage system?
☐ Yes ☐ No

A. If yes, what type of data?

B. If yes, has anyone reviewed this storage system (i.e. Privacy Office)?

C. If yes, has anyone reviewed the contract terms (i.e. General Counsel)?

12. Do any of your applications access AIS mainframe data via the Generalized Interface?☐ Yes ☐ No

A. If yes, are you currently in compliance with the requirements of the AIS Memo of Understanding? ☐ Yes ☐ No

13. Do any of your applications access data via the Data Warehouse?
☐ Yes ☐ No

A. If yes, have you requested and been approved for a Data Warehouse ApplicationID? ☐ Yes ☐ No

14. If any of your applications access student data from the AIS mainframe via the Generalized Interface or from the Data Warehouse, do you have procedures in place to ensure all users of the application have successfully completed the FERPA tutorial quiz? ☐ Yes ☐ No ☐ N/A

A. If yes, please provide details regarding your procedures:

**Anti-virus and Spyware:**

1. Do you have automatically updated anti-virus software in place for servers and workstations?

Servers? ☐ Yes ☐ No
Workstations? ☐ Yes ☐ No

A. If yes, what programs do you use (please include versions)?

_____
_____

B. If no, please describe your process for updating software when updates become available?

_____
_____

C. If no, how often are the *virus definitions* updated and what procedures do you use
to update?

_____
_____

D. Are procedures in place to ensure the process for updating anti-virus software is functioning properly? If yes, please explain:

_____
_____

E. Is the virus protection program configured so users can't disable the software?
☐ Yes ☐ No

2. Is Anti-Virus software configured to check for attempted virus introduction from multiple vectors (e.g. web, USB…etc) in addition to boot and email viruses?
☐ Yes ☐ No

3. Do you have automatically updated Anti-Spyware software in place for servers and workstations?
Servers? ☐ Yes ☐ No
Workstations? ☐ Yes ☐ No

1. If yes, what software?_____

**Vulnerability Scanning:**

3. Have you used SOS' Security Center to conduct a scan of your network?
☐ Yes ☐ No

A. If yes, when was the last scan performed?

B. If yes, have all the vulnerabilities that were identified in the vulnerability assessment been investigated and either explained/mitigated/resolved? ☐ Yes ☐ No

C. If yes, **please provide a copy of your most recent scan results to Internal Audit.**

2. Have you or SOS ever conducted a scan of your web applications?
☐ Yes ☐ No

A. If yes, when was the last scan performed?

B. If yes, have all the vulnerabilities that were identified in the vulnerability assessment been investigated and either explained/mitigated/resolved? ☐ Yes ☐ No

C. If yes, **please provide a copy of your most recent scan results to Internal Audit.**

3. Have you had any penetration testing done on any networks housing Internally Controlled or Restricted Data?
☐ Yes ☐ No ☐ N/A

**General:**

1. When logging on to the network are users provided with a logon banner display warning stating that continued use beyond this banner signifies the users agreement to abide by corporate policies? ☐ Yes ☐ No

   **If yes, please provide a screenshot to Internal Audit.**

2. Are public and non-authenticated student systems that reside on the same physical network as administrative systems segmented from the rest of the network by a DMZ or equivalent additional segregation, e.g. VPN, VLAN or separate network or firewall interface? ☐ Yes ☐ No ☐ N/A

3. Is there an ftp server? ☐ Yes ☐ No

   A. If yes, is it anonymous? ☐ Yes ☐ No

   B. What is its purpose?

4. Are there any applications that are supported by your area that are used for administrative purposes within your business? ☐ Yes ☐ No

   A. If yes, and the application is a custom application, was a Security Review conducted at regular intervals during Development?
   ☐ Yes ☐ No

   B. If yes, and the application is a custom application, do you have a documented Configuration and Change Control Process in place for the application?
   ☐ Yes ☐ No

5. Do you allow users to connect their own devices to the administrative network?
☐ Yes ☐ No

A. If yes, what types of devices are allowed?

I. ☐ Laptops/Tablets
II. ☐ Smartphones
III. ☐ External Hard Drives/Flash Drives

B. If yes, do you have any of the below noted policies/procedures/requirements in place to aid in controlling the use of external devices and their access to critical or sensitive data?

I. ☐ Acceptable Use Policy
II. ☐ Defined Security Software requirements
III. ☐ Specifically Approved Device listing
IV. ☐ Use of Secure Virtual Environments
V. ☐ Centralized IT management requirement
VI. ☐ Restriction of mobile data access to specific apps
VII. ☐ Monitoring of applications installed on devices

C. If no, how do you control the use of external devices?

_____

6. Is institutional data stored on the portable or mobile devices (laptop, phone, IPAD…etc) protected in accordance with business policy, Non-office Telecommunications Services, which states "All institutional data must be protected from unauthorized disclosure and must be protected with the same granularity of security control provided by the originating host system. This includes institutional data on mobile devices, including personal devices which may be used for business purposes."

☐ Yes ☐ No ☐ N/A

A. If yes, how is this accomplished?

8. Do you maintain your telecommunication wiring devices? ☐ Yes ☐ No

A. If no, who does?

____ _____

9. Have you implemented SharePoint or some other collaboration system?

☐Yes ☐ No

A. If yes, what is it being used for?

B. If yes, how do you secure any Internally Controlled or Restricted Data?

10. Do you have procedures in place for reviewing user data on file servers and shared workspaces upon their departure (i.e. for archival, retention, deletion)? ☐Yes ☐ No

A. If yes, please describe

11. Do you have a method to sanitize all hard disks and removable media prior to their disposal or reuse?
☐ Yes ☐ No

A. If yes, what method are you using?

# SECTION F: LOGICAL SECURITY

**Administrator accounts and access:**

1. Who has administrator rights/privileges/accounts on the servers/LANs?

| Name | Title | Reason |
|---|---|---|
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |

*If additional individuals have administrative accounts, please provide a detailed listing to Internal Audit

** Please provide a screen shot of the LAN administrators

2. Do all administrators also have a non-administrator account on the LAN for day-to-day activities?
   ☐ Yes ☐ No

3. Are local administrator computer account passwords changed every time there is a change in personnel who know them? (If common passwords are in use.)
   ☐ Yes ☐ No

**User accounts and access:**

1. How are users authorized to use the LAN/network environment?
   - ☐ Written authorization form must be completed (**please provide a copy of a blank form to Internal Audit**)
   - ☐ Notified by E-Mail
   - ☐ Verbal Authorization from user's supervisor
   - ☐ Other (please describe below)(**please provide copies of any forms or procedures to Internal Audit**):

2. Do you follow the Least Privilege Method when assigning user rights?

☐ Yes ☐ No

A. If no, please justify why not:

B. If yes, do you permit users to elevate privileges (e.g. second account)?
☐ Yes ☐ No

3. Are all users forced to authenticate to a LAN to obtain internet access?
☐ Yes ☐ No

A. If yes, how is this accomplished? If no, please explain how they gain access.

B. Are ports locked down to MAC addresses and IP addresses?
☐ Yes ☐ No

4. Do you periodically verify your authorized user lists? ☐ Yes ☐ No

A. If yes, how often do you verify users?

B. If yes, please describe your verification procedure:

5. Are there procedures in place to ensure accounts assigned to users who have been terminated or assigned to other duties are promptly removed from the LAN?
☐ Yes ☐ No

A. If yes, what are the procedures used (please describe or **provide a copy of the written procedures to Internal Audit**)?

**Access Accounts**

1. Do users or administrators use Access Accounts to login to workstations? ☐ Yes ☐ No

2. If yes, how is this implemented?

☐ Kerberos client
☐ AD domain membership (OU or child domain)

☐ membership in another Active Directory domain with Kerberos trust to
prefix.domain.com (please name the domain here):
_____
☐ other (please describe below):

_____

Note: If you answered yes, when you complete the next section "User Accounts Passwords and logon ID's", please complete it for local AD user and admin accounts only.

**User Account Passwords and logon ID's:**

1. Does the operating system have a way to force users to use complex passwords, has this feature been enabled? ☐ Yes ☐ No

   A. If yes, how is this accomplished/enforced?

   B. If no, explain why not?

   C. If no, has any password cracking software (method referenced in ADG02) been run to determine if adequate passwords are being used? ☐ Yes ☐ No

2. Is the operating system configured to keep a password history & minimum password age to prevent a user from cycling back to their favorite password?
   ☐ Yes ☐ No

   A. If yes, how is this accomplished/enforced?

   B. If no, explain why not:

3. What is the required minimum length of passwords?

    A. How is this accomplished/enforced?

4. Are the following passwords periodically changed?

    Users: Administrators:
    ☐ Yes ☐ No ☐ Yes ☐ No

    A. If yes, how is this enforced?

    B. If yes, how often are they required to be changed?

    Users:

    Administrators:

    C. Have any passwords been set to never expire? ☐ Yes ☐ No

        1. If yes, please explain why.
        _____
        ___
        _____
        ___

5. Are users prohibited from sharing passwords? ☐ Yes ☐ No

6. Do all accounts have passwords? ☐ Yes ☐ No

7. Are there controls in place to provide against repeated attempts (failures) to access the system? ☐ Yes ☐ No

    A. If yes, how many logon attempts are permitted before the user is locked out and what is your procedure for resetting accounts?

    _____

B. If no, explain why not?

***Please provide a screen shot of Group Policy Object settings for information identified above.**

8. If you have group logon ID's complete this question.

   A. Please state the reason for use of group logon ID's:

   B. If yes, is there written approval (ADG02 standards)?
   ☐ Yes ☐ No

      1. If yes, **please provide a copy of the authorization to Internal Audit**.

   C. Do you change the group logon ID password when an employee has been terminated or assigned to other duties? ☐ Yes ☐ No

**Remote Access:**

1. Is remote access permitted to servers from outside the network? ☐ Yes ☐ No

   A. What software and version is used to control access?
   _____

   B. How is this accomplished/controlled (e.g. password protected, VPN, etc.)?

   C. Who is authorized to use remote access?

| Name | Title | Reason |
|---|---|---|
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |

***If additional individuals are authorized to use remote access, please provide a detailed listing to Internal Audit.**

D. Are all data, passwords and user ids encrypted? ☐ Yes ☐ No

2. Is remote access permitted to workstations from outside the network?

   A. What software and version is used to control access?

   _____

   B. How is this accomplished/controlled (e.g. password protected, VPN, etc.)?

   C. Who is authorized to use remote access?

| Name | Title | Reason |
|---|---|---|
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |

***If additional individuals are authorized to use remote access, please provide a detailed listing to Internal Audit.**

   D. Are all data, passwords and user ids encrypted? ☐ Yes ☐ No

3. Is remote support access permitted to workstations from inside the network?
   ☐ Yes ☐ No

   A. If yes, what software and version is used to control access?

   _____

   B. How is this accomplished/controlled (e.g. password…etc)?

   _____

   C. Who is authorized to use remote support access?

| Name | Title | Reason |
|---|---|---|

| | | |
|---|---|---|
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |

***If additional individuals are authorized to use the software please provide a detailed listing to Internal Audit.**

D. Are all data, passwords and user ids encrypted? ☐ Yes ☐ No

**General:**

1. Have permissions been properly set for shares to control access to resources, directories, files, etc., following the concept of "least privilege"? ☐ Yes ☐ No

   A. If yes, what method are you using to assure permissions are correct?

2. Are workstations configured to use a locking feature and/or screen saver passwords?
   ☐ Yes ☐ No

   A. If yes, after how long are they activated? _____

   B. If yes, are the features configured so that users cannot disable them?
   ☐ Yes ☐ No

3. Is the LAN protected by a firewall? ☐ Yes ☐ No

   A. If yes, please complete the firewall questionnaire.

4. Are any workstations protected by a personal firewall (e.g. Windows, Zone Alarm…)?

   A. If yes, please describe:
   _____
   ___
   _____
   ___
   _____
   ___

5. Is the LAN protected by a real-time intrusion detection system (IDS) or intrusion prevention system (IPS)?
   ☐ Yes ☐ No

   A. If yes, is SOS monitoring the activity? ☐ Yes ☐ No

   B. If SOS is not monitoring the activity, please describe the device you are using, who is monitoring the activity and your monitoring process.
   _____
   _____
   _____
   _____
   ___

6. Are public facing servers (e.g. web server) isolated in their own DMZ?
   ☐ Yes ☐ No

## SECTION G: PHYSICAL & ENVIRONMENTAL SECURITY

1. Are the servers protected from environmental damage (fire, climate, flood, etc.)?

A. Fire ☐ Yes ☐ No

1. If yes, how?
   - ☐ Chemical Extinguishers
   - ☐ $CO^2$ Extinguishers
   - ☐ Sprinkler System
   - ☐ Other (please describe):

B. Climate Changes ☐ Yes ☐ No

1. If yes, how?

C. Flood Damage ☐ Yes ☐ No

1. If yes, how?

2. Is access to servers, switches and routers, and wiring areas adequately controlled?

A. Servers: ☐ Yes ☐ No

1. If yes, how?

2. If yes, who has access to the server(s)?

| Name | Title | Reason |
|---|---|---|
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |

***If additional individuals have access to the location of the servers, please provide a detailed listing to Internal Audit.**

B. Wiring Closets, Switches and Routers: ☐ Yes ☐ No

1. If yes, how?

2. If yes, who has access to the above areas?

| Name | Title | Reason |
|---|---|---|
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |

***If additional individuals have access to the wiring closet(s), please provide a detailed listing to Internal Audit.**

3. Are the wiring closets free of janitorial supplies, instructional equipment, computer peripherals, etc.? ☐ Yes ☐ No

   a. If no, identify additional materials in closets:

   _____

3. Have you deployed surveillance cameras to record access to all facilities housing Internally Controlled or Restricted Data?
   ☐ Yes ☐ No

   A. If yes, is the security footage regularly reviewed by authorized personnel?
   ☐ Yes ☐ No

4. Have you implemented procedures to ensure Employee Identity Proofing?
   ☐ Yes ☐ No

A. If yes, what procedures have you implemented?

5. Are there controls to prevent access to the server console (e.g., locked using Ctrl, Alt & Delete, and screen saver with password protection)? ☐ Yes ☐ No

6. If some workstations are used to display sensitive information, are there sufficient controls to prevent unauthorized viewing of the information?
   ☐ Yes ☐ No

   A. If yes, how is this accomplished?

7. Are there uninterruptible power supply (UPS) devices for all servers?
   ☐ Yes ☐ No

   A. If yes, how long can the UPS sustain power?

_____

   B. If yes, at what capacity is the UPS current running?

_____

8. Do you have backup generators available in the event of an extended power outage? ☐ Yes ☐ No

   A. If no, why not?

9. Are video conferencing and satellite equipment kept in a secure area?
   ☐ Yes ☐ No

10. Have the default settings for the video conferencing equipment been changed to prevent unauthorized monitoring? ☐ Yes ☐ No

    A. If yes, what settings have you reconfigured?

# SECTION H: BUSINESS CONTINUITY AND BACKUP

1. Do you have a written business continuity plan (BCP) that consists of service recovery and disaster recovery plans? ☐ Yes ☐ No

   A. If yes, **please provide a copy to Internal Audit** and complete the remainder of this question.

   B. Which of the following does the BCP include?

   ☐ A listing of persons to be contacted in the event of a disruption, including where they can be reached.
   ☐ Procedures and guidelines that describe each person's responsibilities and job function until normal operations are able to continue.
   ☐ Service recovery plans that prevent interruption of mission-critical functions, allowing the Business to continue to provide support and service to customers.
   ☐ When some functions are to be performed on a temporary basis on resources that reside at another location, the plan provides for a list of these functions and assigns each function to a responsible person or group.
   ☐ A plan for backup hardware at an alternate location, in the event of loss of key equipment.

   C. Is the plan maintained up-to-date? ☐ Yes ☐ No

      1) If yes, by whom? __

   D. Is the plan tested periodically? ☐ Yes ☐ No

      1) If yes, how and by whom?

2. Are you aware of your organization/department/units building evacuation plans?
   ☐ Yes ☐ No

3. Are backups of data performed? ☐ Yes ☐ No

   A. If yes, what servers and workstation components are backed up?

   _____

_____
_____
____

B. If yes, what is the frequency of the backups?

_____
_

_____
_

_____
_

C. If yes, how and by whom?

_____
_____
_____
_____
_____

4. Do you have daily procedures to ensure backups ran successfully?
   Yes ☐ No ☐

   A. If yes, please explain?

   _____

5. Has the use of backup files been tested by restoring backup files?
   ☐ Yes ☐ No

   A. If yes, when was testing last performed?

   B. If no, explain why not:

   _____
   _____
   _____
   _____

6. Is backup media maintained offsite? ☐ Yes ☐ No

   A. If yes, where is it maintained?

   _____
   _____
   _____

7. Are backup copies, which are maintained offsite and at the office, protected against unauthorized access?

   Onsite: ☐ Yes ☐ No
   Offsite: ☐ Yes ☐ No

   A. If yes, please explain how:

   _____
   ___
   _____
   ___
   _____
   _____
   _____

8. Do you have redundancy for:
   a. Your web server? ☐ Yes ☐ No
   b. Your file server? ☐ Yes ☐ No
   c. Your mail server? ☐ Yes ☐ No
   d. Your firewall? ☐ Yes ☐ No
   e. Your domain controller? ☐ Yes ☐ No

   A. If you answered NO to any of the above, please explain what plans you have for implementing redundancy:

   _____

## SECTION I: LOGGING AND MONITORING

1. Are System level audit logs showing both general and privileged access captured and retained in accordance with AD35 and the General Retention Schedule?
   ☐Yes ☐ No

2. Are Application level audit logs showing both general and privileged access captured and retained in accordance with AD35 and the General Retention Schedule?
   ☐Yes ☐ No

3. Are Network level audit logs showing both general and privileged access captured and retained in accordance with AD35 and the General Retention Schedule?
   ☐Yes ☐ No

4. Are transaction records for electronic email captured and retained in accordance with AD35? ☐Yes ☐ No

5. Are procedures in place to proactively review audit logs? ☐Yes ☐ No

   If yes, how often and by whom?

# SECTION J: STAFF BACKGROUND AND TRAINING

1. Describe the experience of your system administrator(s) and IT staff?

Name:_____

Job Title:_____

_____

_____

_____

Name:_____

Job Title:_____

_____

_____

_____

Name:_____

Job Title:_____

_____

_____

_____

Name:_____

Job Title:_____

_____

_____

_____

2. What training have system administrators received in support of their job (e.g. skills, classes, seminars, certifications, etc.)?

Name:_____

Job Title:_____

_____

_____

_____

Name:_____

Job Title:_____

_____

_____

_____

Name:_____

Job Title:_____

_____

_____

_____

Name:_____

Job Title:_____

_____

_____

_____

# SECTION K: SUMMARY OF REQUESTED DOCUMENTATION

**Please provide copies of all documentation electronically, if possible.**

**Policies and Procedures:**

System Schematic
IP Addresses (Subnets)
Organizational Unit/Departmental Policies
Backup Procedures
Sanitization of Hard Drives
Reassigning Workstations
Mobile Devices
Software Use
Business Continuity Plan

**Network Information:**

Screen Shot of GPO settings
Screen Shot of LAN administrators
Screen Shot of Logon Screen warning
Copy of User Access Request Form

**Vulnerability Assessments:**

Results of Network Scans
Results of Application Scans
Results of Internal Vulnerability Scans

**Additional Questionnaires/Forms:**

Individual Server Purpose List
Firewall
SSN Authorization Request and Network and System Requirements forms (if applicable)
PCI DSS Self Assessment (if applicable)