UNIVERSITY OF TORONTO
FACULTY OF INFORMATION

Information Services IT Policies

Prepared by Ivan Sestak
May, 2010
updated November 27, 2011

Backup Policy

1.0 Overview

This policy defines the backup policy for computers within the Faculty which are expected to have their data backed up. These systems are typically, but not limited to servers. Servers expected to be backed up include the file server, the mail server, and the web server.

2.0 Purpose

This policy is designed to protect data in the Faculty, to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

3.0 Scope

This policy applies to all equipment and data owned and operated by the Faculty of Information.

4.0 Definitions

1. Backup - The saving of files onto disk storage, magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
2. Archive - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.
3. Restore - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

5.0 Timing

This policy provides guidelines for establishing backup procedures. Exceptions to the standard procedure are permitted when justified. All exceptions must be fully documented. The standard procedure for systems backup is as follows:

- A full systems backup will be performed weekly on Sunday. Weekly backups will be saved for 5 (five) weeks.
- The last weekly backup of the month will be saved as a monthly backup.
- Monthly backups of data will be saved for one year, at which time the media will be recycled.
- Monthly backups of servers will be saved for 6 months, at which time the media will be recycled.
- Annual Backups created in May will be saved for 3 years.
- VSS backups are performed daily. VSS backups are retained for 32 days, at which time the media will be recycled.
- All backups will be stored in a secure, off-site location. Proper environment controls, temperature, humidity and fire protection, shall be maintained at the storage location.
- All backup media that is not re-usable shall be thoroughly destroyed in an approved manner. Backup media that is used for other purposes shall be thoroughly erased.
- Periodic tests of the backups will be performed to determine if files can be restored.

6.0 Tape Storage
Archived (offline) data will be stored in the Digital Tape Library for archival purposes.

7.0 Tape Drive Cleaning
Tape drives shall be cleaned monthly and the cleaning tape shall be changed every six months.

8.0 Monthly Backups
Every month a monthly backup tape shall be made using the oldest backup tape or tape set from the tape sets.

9.0 Age of Tapes
The date each tape was put into service shall be recorded on the tape. Tapes that have been used longer than twelve (12) months for the daily/weekly shall be discarded and replaced with new tapes. Archival tapes (annual backups) will be retained until the specified time frame of discarding and destroying the tapes.

10.0 Responsibility
The IS department shall delegate a member of the IS department to perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis.

11.0 Testing
The ability to restore data from backups shall be tested at least once per month.

12.0 Data Backed Up
Data to be backed up include the following information:

1. User data stored on the File Shares.
2. System state data
3. The registry

Systems to be backed up include but are not limited to:

1. File server
2. Mail server
3. Production web server
4. Production database server
5. Domain controllers
6. Development database server
7. Development web server

Systems will be backed up according to the schedule below:
o Data stored on the SAN appliance will be regularly backed up as follows:
- VSS backup daily (Mon.-Sat. 7am, 12pm(noon) & 11pm) and data located on-site.
- Full backup weekly (Sun) and data located on-site.

o Windows Servers will be regularly backed up as follows:
- Backup daily (Mon.- Sat) and data stored on-site.
- Full backup weekly (Sun.) and data located on-site.

o The Virtual Machine Server will have its VM data drive regularly backed up as follows:

- Image backups of virtual machines will be taken daily at 7pm. These backup files will be stored on-site and retained for 14 days for the daily, 5 weeks for the weekly and 6 months for the monthly full backups.
- Weekly file and folder (data) full backup will be taken on Sunday. These backup files will be stored on-site.

A weekly job will copy the online backup files to the Digital Tape Library and the monthly backup job will be stored securely off-site.

13.0 Archives

Archives are made at the end of every year in May. User account data associated with the file and mail servers are archived one month after the User has left the organization.

14.0 Restoration

Users will be able to restore files using Volume Shadow Copy. In the event that users that need files restored outside of VSS, the request must be submitted to the Information Services Help Desk. Information must be included about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

In the event of a catastrophic system failure, off-site backed up data will be made available to users within 3 working days if the destroyed equipment has been replaced by that time.

In the event of a non-catastrophic system failure or user error, on-site backed up data will be made available to users within 1 working day.

15.0 Tape Storage Locations

Offline tapes used for weekly backup shall be stored in a secure location at our iSouth building.

Responsibilities

- Backups and Data Recovery Tony Lemmens, tony.lemmens@utoronto.ca
- Verification Ivan Sestak, ivan.sestak@utoronto.ca

We have a 5 level backup system in place.

Level 1 – Volume Shadow Copy on Domain Controller

Level 2 – Servers backed up using DPM (Data Protection Manager) to SAN according to schedule

Level 3 – All Virtual Servers are backed up using VDR (VMWare Data Recovery) to the Guest OS level as well as file level restoration

Level 4 – Most backups on the SAN (Storage Array Network) are then mirrored to a secondary SAN for longer term archival, non-critical servers' backups are not mirrored

Level 5 – Secondary SAN is then offloaded to digital tape and is transferred to iSouth

Server Documentation Policy

1.0 Overview

This policy is an internal IT policy and defines the requirements for server documentation This policy defines the level of server documentation required such as configuration information and services that are running. It defines who will have access to read server documentation and who will have access to change it. It also defines who will be notified when changes are made to the servers.

2.0 Purpose

This policy is designed to provide for network stability by ensuring that network documentation is complete and current. This policy should complement disaster management and recovery by ensuring that documentation is available in the event that systems should need to be rebuilt. This policy will help reduce troubleshooting time by ensuring that appropriate personnel are notified when changes are made to any servers.

3.0 Documentation

For every server on a secure network, there are a list of items that must be documented and reviewed on a regular basis to keep a private network secure. This list of information about every server should be created as servers are added to the network and updated regularly.

1. Server name
2. Server location
3. The function or purpose of the server.
4. Hardware components of the system including the make and model of each part of the system.
5. List of software running on the server including operating system, programs, and services running on the server.
6. Configuration information about how the server is configured including:
    1. Event logging settings
    2. A comprehensive list of services that are running.
    3. Configuration of any security lockdown tool or setting
    4. Account settings
    5. Configuration and settings of software running on the server.
7. Types of data stored on the server.
8. The owners of the data stored on the server.
9. The sensitivity of data stored on the server.
10. Data on the server that should be backed up along with its location.
11. Users or groups with access to data stored on the server.
12. Administrators on the server with a list of rights of each administrator.
13. The authentication process and protocols used for authentication for users of data on the server.
14. The authentication process and protocols used for authentication for administrators on the server.
15. Data encryption requirements.
16. Authentication encryption requirements.
17. List of users accessing data from remote locations and type of media they access data through such as internet or private network.
18. List of administrators administrating the server from remote locations and type of media they access the server through such as internet or private network.

19. Intrusion detection and prevention method used on the server.
20. Latest patch to operating system and each service running.
21. Groups or individuals with physical access to the area the server is in and the type of access, such as key or card access.
22. Emergency recovery disk and date of last update.
23. Disaster recovery plan and location of backup data.

4.0 Access

The IS server administration staff and their management shall have full read and change access to server documentation for the server or servers they are tasked with administering. The IS networking staff, enterprise security staff, application development staff, and help desk staff shall have the ability to read all server documentation.

5.0 Change Notification

The help desk staff, network administration staff, application developer staff, and IS management shall be notified when changes are made to servers. Notification shall be through email to designated groups of people.

6.0 Documentation Review

The Senior IT Administrator shall ensure that server documentation is kept current by performing a monthly review of documentation or designating a staff member to perform a review. Any current or completed projects affecting server settings should be reviewed to determine whether there were any server changes made to support the project.

7.0 Storage Locations

Server documentation shall be kept either in written form or electronic form in a minimum of two places. The documentation will be made available on our Departmental Wiki as well as in the fireproof safe located in the Director of Information Services office.

IT Asset Control & Disposal Policy Guide

May, 2010

1.0 Overview

All employees and personnel that have access to organizational computer systems must adhere to the IT asset control policy defined below in order to protect the security of the network, protect data integrity, and protect and control computer systems and organizational assets. The asset control policy will not only enable organizational assets to be tracked concerning their location and who is using them but it will also protect any data being stored on those assets. This asset policy also covers disposal of assets.

IT assets should not be confused with nor tracked with other organizational assets such as furniture. One of the main reasons to track IT assets other than for property control and tracking is for computer security reasons. A special IT asset tracking policy will enable the organization to take measures to protect data and networking resources.

This policy will define what must be done when a piece of property is moved from one building to another or one location to another. This policy will provide for an asset tracking database to be updated so the location of all computer equipment is known.

2.0 Purpose

The purpose of this procedure is to establish and define standards and restrictions for the disposal of non-leased IT equipment in a legal, cost-effective manner. Faculty of Information surplus or obsolete IT assets and resources (i.e. desktop computers, servers, databases, etc.) must be discarded according to legal requirements and environmental regulations through the appropriate external agents and the Faculty of Information upgrade guidelines. Therefore, all disposal procedures for retired IT assets must adhere to University-approved methods.

This procedure applies to the proper disposal of all non-leased Faculty of Information IT hardware, including PCs, printers, handheld devices, servers, databases, hubs, switches, bridges, routers, and so on. Faculty-owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse are covered by this procedure. Where applicable, it is desirable to achieve some residual value of the IT asset in question through reselling, auctioning, donation, or reassignment to a less-critical function.

Definitions

1. “Non-leased” refers to any and all IT assets that are the sole property of the Faculty of Information; that is, equipment that is not rented, leased, or borrowed from a third-party supplier or college partner.

2. “Disposal” refers to the reselling, reassignment, recycling, donating, or throwing out of IT equipment through responsible, ethical, and environmentally sound means.

3. “Obsolete” refers to any and all equipment which no longer meets requisite functionality.

4. “Surplus” refers to hardware that has been replaced by upgraded equipment or is superfluous to existing requirements.

5. “Beyond reasonable repair” refers to any and all equipment whose condition requires fixing or refurbishing that will likely cost equal to or more than total replacement.

Guidelines

Disposal procedures of all IT assets and equipment will be centrally managed and coordinated by the Faculty of Information IS department. The IS department is also responsible for backing up and then wiping clean of Faculty data all IT assets slated for disposal, as well as the removal of University tags and/or identifying labels. The IS department is in charge of selecting and approving external agents for recycling hardware and/or disposa.

3.0 Assets Tracked

This section defines what IT assets should be tracked and to what extent they should be tracked.

3.1 IT Asset Types

This section categorized the types of assets subject to tracking.

1. Desktop workstations
2. Laptop mobile computers
3. Printers, Copiers, FAX machines, multifunction machines
4. Handheld devices
5. Scanners
6. Servers
7. Firewalls
8. Routers
9. Switches
10. Memory devices

3.2 Assets Tracked

Assets which cost less than $100 shall not be tracked specifically including computer components such as video cards or sound cards. However, assets which store data regardless of cost shall be tracked. These assets include:

1. Hard Drives
2. Temporary storage drives
3. Tapes with data stored on them including system backup data.
4. Although not specifically tracked, other storage devices including CD ROM disks and floppy disks are covered by this policy for disposal and secure storage purposes.

3.3 Small Memory Devices

Small memory storage assets will not be tracked by location but by trustee. These assets include:

1. Floppy disks
2. Optical Drives (CD-ROM, DVD etc)
3. Memory sticks/cards

If these types of devices are permitted for some employees, the trustee of the device must sign for receipt of these devices in their possession. All employees must also agree to handle memory sticks, floppy disks, and Optical Drives in a responsible manner and follow these guidelines:

1. Never place sensitive data on them without authorization. If sensitive data is placed on them, special permission must be obtained and the memory device must be kept in a secure area and must use Faculty approved encryption software (TrueCrypt) during transport and use.
2. Never use these devices to bring executable programs from outside the network without authorization and without first scanning the program with an approved and updated anti-virus and malware scanner.

4.0 Asset Tracking Requirements

1. All assets must have an ID number. Either an internal tracking number will be assigned when the asset is acquired or the use of Manufacturer ID numbers must be specified in this policy.
2. An asset tracking database shall be created to track assets. It will include all information on the Asset Transfer Checklist table and the date of the asset change.
3. When an asset is acquired, an ID will be assigned for the asset and its information shall be entered in the asset tracking database.

5.0 Transfer Procedure:

1. **Asset Transfer Checklist** - When an asset type listed on the Asset Types list is transferred to a new location or trustee, the IT Asset Transfer Checklist must be filled out by the trustee of the item and approved by an authorized representative of the organization.

   The trustee must indicate whether the asset is a new asset, moving to a new location, being transferred to a new trustee, or being disposed of. The following information must be filled in:

   1. Asset Type
   2. ID number
   3. Asset Name
   4. Current Location
   5. Designated Trustee
   6. New Location
   7. New Trustee

2. **Obsolete IT Assets:** As prescribed above, “obsolete” refers to any and all computer or computer-related equipment that no longer meets requisite functionality.Equipment lifecycles are to be determined by IS asset management best practices (i.e. total cost of ownership, required upgrades, etc.).

3. **Reassignment of Retired Assets:** Reassignment of computer hardware to a less-critical role is made at the sole discretion of the IS department. It is, however, the goal of the Faculty of Information to – whenever possible – reassign IT assets in order to achieve full return on investment (ROI) from the equipment and to minimize hardware expenditures when feasible reassignment to another business function will do instead.

4. **Trade-Ins:** Where applicable, cases in which a piece of equipment is due for replacement by a newer model, reasonable actions must be taken to ensure that a fair and market trade-in value is obtained for the old IT asset against the cost of the replacement. The Faculty of Information IS Asset manager will assume this responsibility.

5. **Cannibalization and Assets Beyond Reasonable Repair:** The Senior IT Administrator is responsible for verifying and classifying any IT assets beyond reasonable repair. Equipment identified as beyond reasonable repair should be cannibalized for any spare and/or working parts that can still be put to sufficient use within the organization. The IS department will inventory and stockpile these parts. Remaining parts and/or whole machines unfit for use or any other disposal means will be sold to an approved salvaging company. We have used both Free Geek Toronto and Greentec for disposal.

6. **Decommissioning of Assets:** All hardware slated for disposal by any means must be fully wiped clean of all Faculty data. The Faculty of Information IS department will assume responsibility for decommissioning this equipment by deleting all files, University-licensed programs, and applications using a pre-approved disk-sanitizer (Darik’s Boot and Nuke using the DoD Short – Department of Defense Short 3 pass wipe). In addition, any property tags or identifying labels must also be removed from the retired equipment. All hard drives will also be drilled through the disc plates to ensure that data cannot be recovered.

6.0 Asset Transfers

This policy applies to any asset transfers including the following:

1. Asset purchase
2. Asset relocation
3. Change of asset trustee including when an employee leaves or is replaced.
4. Asset disposal

In all these cases the asset transfer checklist must be completed.

7.0 Enforcement

Since data security and integrity along with resource protection is critical to the operation of the organization, employees that do not adhere to this policy may be subject to disciplinary action up to and including dismissal. Any employee aware of any violation of this policy is required to report it to their supervisor or other authorized representative.

Incident Response Plan

1.0 Overview

This incident response plan defines what constitutes a security incident and outlines the incident response phases. This incident response plan document discusses how information is passed to the appropriate personnel, assessment of the incident, minimizing damage and response strategy, documentation, and preservation of evidence. The incident response plan will define areas of responsibility and establish procedures for handing various security incidents.

2.0 Purpose

This policy is designed to protect the Faculty of Information resources against intrusion.

3.0 Incident Response Goals

1. Verify that an incident occurred.
2. Maintain or Restore Business Continuity.
3. Reduce the incident impact.
4. Determine how the attack was done.
5. Prevent future attacks or incidents.
6. Improve security and incident response.
7. Prosecute illegal activity.
8. Keep management informed of the situation and response.

4.0 Incident Definition

An incident is any one or more of the following:

1. Loss of information confidentiality (data theft)
2. Compromise of information integrity (damage to data or unauthorized modification).
3. Theft of physical IT asset including computers, storage devices, printers, etc.
4. Damage to physical IT assets including computers, storage devices, printers, etc.
5. Denial of service.
6. Misuse of services, information, or assets.
7. Infection of systems by unauthorized or hostile software.
8. An attempt at unauthorized access.
9. Unauthorized changes to organizational hardware, software, or configuration.
10. Reports of unusual system behavior.
11. Responses to intrusion detection alarms.

5.0 Incident Planning

In the incident response plan, do the following:

1. Define roles and responsibilities
2. Establish procedures detailing actions taken during the incident.
3. Detail actions based on type of incident such as a virus, hacker intrusion, data theft, system destruction.
4. Procedures should consider how critical the threatened system or data is.
5. Consider whether the incident is ongoing or done.

6.0 Incident Response Life cycle

1. Incident Preparation
    1. Policies and Procedures
        1. Computer Security Policies - These involve many policies including password policies, intrusion detection, computer property control, data assessment, and others.
        2. Incident Response Procedures
        3. Backup and Recovery Procedures
    2. Implement policies with security tools including firewalls, intrusion detection systems, and other required items.
    3. Post warning banners against unauthorized use at system points of access.
    4. Establish Response Guidelines by considering and discussing possible scenarios.
    5. Train users about computer security and train IT staff in handling security situations and recognizing intrusions.
    6. Establish Contacts - Incident response team member contact information should be readily available. An emergency contact procedure should be established. There should be one contact list with names listed by contact priority.
    7. Test the process.

2. Discovery - Someone discovers something not right or suspicious. May be from several sources:
    1. Helpdesk
    2. Intrusion detection system
    3. A system administrator
    4. A business partner
    5. A monitoring team
    6. A manager
    7. The security department or a security person.
    8. An outside source

3. Notification - The emergency contact procedure is used to contact the incident response team.

The following information should be included in the summary:

- How the incident was detected
- Dates
    - Inferred date of compromise
    - Date the compromise was detected
    - Date the incident was contained
    - Date the incident was finally resolved
- Names
    - People added to the Unit Incident Response Team for this incident
    - Person responsible for the IT Resource
    - Systems/Resources that are affected

4. Analysis and Assessment - Many factors will determine the proper response including:
    1. Is the incident real or perceived?
    2. Is the incident still in progress?
    3. What data or property is threatened and how critical is it?
    4. What is the impact on the business should the attack succeed? Minimal, serious, or critical?
    5. What system or systems are targeted, where are they located physically and on the network?
    6. Is the incident inside the trusted network?

Assessment includes analysis, identification, prioritization, and evidence collection and retention.

    1. Analysis. Compromised hosts must be assessed.
        1. http://sans.org/resources/winsacheatsheet.pdf
        2. http://www.sans.org/score/checklists/ID_Windows.pdf
        3. http://www.sans.org/score/checklists/ID_Linux.pdf
    2. Identification. Identify source as appropriate, including user, host or other resource.
    3. Evidence Collection and Retention.
        1. If forensic evidence is needed for law enforcement, an image of the compromised host must be retained. Email and any other relevant evidence must also be retained.
        2. If the method of compromise is unique or cannot be determined, evidence should be retained to aid in analysis of the incident.
    4. Response Strategy - Determine a response strategy.
        1. Is the response urgent?
        2. Can the incident be quickly contained?
        3. Will the response alert the attacker and do we care?
    5. Containment - Take action to prevent further intrusion or damage and remove the cause of the problem. May need to:
        1. Disconnect the affected system(s)
        2. Change passwords.
        3. Block some ports or connections from some IP addresses.
    6. Prevention of re-infection
        1. Determine how the intrusion happened - Determine the source of the intrusion whether it was email, inadequate training, attack through a port, attack through an unneeded service, attack due to unpatched system or application.
        2. Take steps to prevent an immediate re-infection which may include one or more of:
            1. Close a port on a firewall
            2. Patch the affected system
            3. Shut down the infected system until it can be re-installed
            4. Re-install the infected system and restore data from backup. Be sure the backup was made before the infection.
            5. Change email settings to prevent a file attachment type from being allow through the email system.
            6. Plan for some user training.
            7. Disable unused services on the affected system.
    7. Restore Affected Systems - Restore affected systems to their original state. Be sure to preserve evidence against the intruder by backing up logs or possibly the entire

system. Depending on the situation, restoring the system could include one or more of the following;

1. Re-install the affected system(s) from scratch and restore data from backups if necessory. Be sure to preserve evidence against the intruder by backing up logs or possibly the entire system.
2. Make users change passwords if passwords may have been sniffed.
3. Be sure the system has been hardened by turning off or uninstalling unused services.
4. Be sure the system is fully patched.
5. Be sure real time virus protection and intrusion detection is running.
6. Be sure the system is logging the correct items

5. Documentation - Document what was discovered about the incident including how it occurred, where the attack came from, the response, whether the response was effective. Forward an Incident Response Summary to involved individuals, departments, Director of IS, and the Dean if necessary.

The following information should be included in the summary:

- How the incident was detected
- Dates
  - Inferred date of compromise
  - Date the compromise was detected
  - Date the incident was contained
  - Date the incident was finally resolved
- Names
  - People added to the Unit Incident Response Team for this incident
  - Person responsible for the IT Resource
  - Person compromising the resource, if known
- Investigation and scope
  - Cause of the compromise
  - Impact of the incident
  - Incident severity
  - Nature of the resolution
  - Proposed improvements
  - Systems/Resources affected
  - Actions taken for resolution

The summary for management will probably contain sensitive information and in any case would not be targeted at the user community.

6. Evidence Preservation - Make copies of logs, email, and other documentable communication. Keep lists of witnesses.
7. Notifying proper external agencies - Notify the police if prosecution of the intruder is possible.
8. Assess damage and cost - Assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.
9. Review response and update policies - Plan and take preventative steps so the intrusion can't happen again.
   1. Consider whether an additional policy could have prevented the intrusion.

2. Consider whether a procedure or policy was not followed which allowed the intrusion, then consider what could be changed to be sure the procedure or policy is followed in the future.
3. Was the incident response appropriate? How could it be improved?
4. Was every appropriate party informed in a timely manner?
5. Were the incident response procedures detailed and cover the entire situation? How can they be improved?
6. Have changes been made to prevent a re-infection of the current infection? Are all systems patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
7. Have changes been made to prevent a new and similar infection?
8. Should any security policies be updated?

What lessons have been learned from this experience?

Workstation Refresh

Traditionally, administrative workstations have been refreshed on an as needed basis managed by individual departments. Due to competing demands within the Faculty for available funds, many office workstations exceeded their useful life and have become inefficient in performing normal functions. This has resulted in a loss of productivity for faculty and staff and an increase in labour and equipment costs to maintain the environment at an acceptable level. By centralizing office computer refresh, FI is able to take advantage of steeper discounts and provide better support by reducing the number of different computer models to be supported and eliminating older hardware.

How often will office computers be refreshed?

Office computers will be refreshed on a 4 year cycle.

How are workstations being refreshed determined?

In evaluating the current environment, it was noted that the age of the current computer inventory was fairly evenly distributed over a 5 year period with a significant number being older than 5 years. The schedule has been designed such that the individuals with the oldest computers will be refreshed in year 1 followed by the next oldest computers in year 2 and so on. An attempt is being made to refresh approximately the same number of computers each year.

The proposed timeline for the computer refresh each fiscal year is;

<u>December – February</u>

Validate departments and personnel to be refreshed in current fiscal year

Build proposed equipment list for each department/individual based on current inventory

Discuss with department heads and adjust configuration list if necessary

Obtain department budget account number for additional equipment outside of standard configurations

Receive department head signoff

Final departmental lists completed by 2/15 for budget submission

<u>June - August</u>

Order and receive new computers

Contact faculty and staff to develop upgrade schedule

Refresh office computers

The current model of workstation being deployed is the University of Toronto desktop standard which can be found at UofT's UShop site.

The current standard desktop as of November 28, 2011 – (Subject to change each year)

Minimum 3.1GHz i5 2400 Processor
Minimum 4GB RAM (Memory)
Minimum 500GB Hard Drive
Minimum 16X DVD+/-RW
Standard Keyboard and Mouse
Minimum 19” LCD Monitor with Speaker bar (22in Wide Monitor, VGA/ DVI – recommended. For users with visual strain issues an UltraSharp LCD Monitor is recommended)
4 Year Pro Support with 4 Year NBD (Next Business Day) Service

IS has worked with Dell and other vendors to determine a computer configuration that is more than sufficient to handle the day to day functions of most faculty and staff on campus and can aid in determining differing configurations to service unique and/or particular work functions such as intense processing for tasks (3D rendering), video editing or Computer Aided Design.

Battery Backup (UPS) Maintenance & Configuration

Maintenance of the UPS consists of preventive and corrective maintenance. Preventive maintenance consists of a scheduled list of activities. Performing these activities keeps the UPS in good working order and helps to prevent failures. Corrective maintenance is performed as a result of a failure. Corrective maintenance addresses the failure and gets the unit working again.

A general guide for the maintenance requirements of the UPS systems modules, static switches, and controls is provided. Although electronic components are not subject to wear in the same degree as electromagnetic (EM) components, they do require systematic maintenance. A standard maintenance procedure cannot be developed for all types and sizes of UPS units. The manufacturer's user's manual should always be consulted as to specific maintenance requirements and troubleshooting diagnostics guidelines.

Safety

Do not rely on memory. Follow the user's manual guidelines. Such guidelines should provide safety precautions. If your user's manual limits the maintenance that can be provided by the user, follow the manual's instructions unless general instructions are supplemented with additional guidance. Physical maintenance or troubleshooting should only be performed by personnel trained on the system. Operating personnel not instructed in UPS maintenance must limit their efforts to identifying the symptoms of a fault. Always be aware of the DANGER, as voltages within the UPS modules and associated switchgear are lethal.

Lethal voltages are present even when the output circuit breaker in the UPS is open. It is necessary to open the circuit breaker in the distribution panel feeding the UPS and the UPS bypass circuit breaker, plus opening the direct current (dc) link connection to the battery, before all dangerous voltages within the UPS are eliminated. Capacitors may need to be discharged of their stored energy. Use CAUTION when operating UPS equipment to prevent serious injury or death.

Preventive maintenance

Periodic maintenance is required to maintain the integrity and lifetime of the battery. Power electronic equipment also requires scheduled maintenance even though solid-state devices are used. Preventive maintenance may require that the UPS system be shut down. A transfer of the critical load which may not provide the power enhancement capabilities of an UPS system is something that the user must tolerate in order to obtain maximum reliability and minimize downtime and repair costs.

1. Records

Preventive maintenance is systematic maintenance. The objective is to minimize equipment operating problems and prevent failures by making minor or necessary repairs before major operating difficulties occur. The general condition of the equipment needs to be evaluated periodically, and records need to be maintained for comparison at subsequent inspections. Recorded information is more reliable than a maintenance technician's memory.

Records should be concise but completely describe equipment conditions. Inspection records should provide complete information on the following topics, preferably on separate record sheets.

(a) Equipment record

This record should list the basic information on the equipment itself, e.g., manufacturer's identification, style, serial, size, location, etc., and incorporate inventory-control data for spare parts. Warranty requirements covering uninterruptible operating conditions should be abstracted from the user's manual.

(b) Repair cost record

This record should provide a history of repair and associated costs of maintenance for the UPS system. It is an essential diagnostic record for avoiding future difficulties, especially for systems determined to be of poor quality, misapplied, or marginal for the application.

(c) Inspection check list

This list should provide necessary and pertinent information on points to be checked and establish the recommended recurring dates when these checks should be made. Since shutdown may require a sliding window period, the amount of time for which this request must precede the shutdown window should also be stated.

(d) Periodic maintenance schedule

This schedule provides a complete listing of the day-to-day, weekly, monthly, and annual duties which should be reviewed on the same periodic time basis so that potential trouble situations can be investigated and corrected as soon as possible.

(e) Maintenance inspection and repair records

These necessary and vital documents should be completed in detail by the inspector or an assigned individual and will be maintained in the IT share network drive.

2. Use of records

These records provide for a workable preventive maintenance program. The information obtained from the necessary periodic inspections can be quickly lost.

This is particularly true when test results are required. Unless records and data on the test and performance of equipment are retained, the maintenance program will be defeated. Unless records are updated at each succeeding test period, valuable information is lost. Comparative test data materially assists an UPS specialist in defining problems, especially when test results differ from manufacturers' recommended settings or actual factory test data. Significant changes in comparative test data can, in general, be related to the equipment's condition.

3. Scheduling

Scheduling of UPS and battery maintenance is normally based on the manufacturers' recommendations. Since an UPS system is vital to the operation of critical loads, it may be considered advisable to provide more inspections than those the manufacturer recommends. Certain items on the UPS should be inspected daily or weekly.

4. Periodic system status checks

The continued monitoring of the operating status of any electronic equipment greatly enhances the probability that failure of that equipment will be prevented. All of our UPS systems are network enabled and are constantly monitored for variances in performance. Automatic diagnostics are scheduled to run bi-weekly and reports are output to it.ischool@utoronto.ca. Runtime diagnostics are scheduled to run on a monthly basis and reports are output to it.ischool@utoronto.ca.

5. Major system inspections

These should be performed at least annually. By performing this type of maintenance on a scheduled basis, it is possible to find and remedy potential problems before the system's operation is affected. Table 1 provides general guidance for the major system inspection, however, the manufacturer's recommendations should be strictly followed.

6. Minor system inspections

Minor system inspections should be provided either after 5 months from an annual major inspection or after 3 months from a semiannual major inspection unless a more frequent requirement is recommended by the manufacturer. Minor system inspections should include at least the first four items listed under major inspections. Off-line load testing is required if major component replacements are required.

Table 1 – Major System Inspections Checklist

- Perform visual checks and operational tests of all UPS equipment and associated cables.
- Review maintenance logs and log all alarm operations and output.
- Complete a functional checkout and test of the UPS diagnostic systems.
- Check environment, temperature, dust, moisture, room vents, etc.
- Check cabling for abrasions and burn spots, visually check components for signs of overheating, swelling, leaking etc.
- Replace air filters at regular intervals. Site conditions will determine how often the filters should be replaced, but generally, they will need to be replaced at least every 6 months in clean environments. If more frequent replacement is required, the cleanliness of the environment should be upgraded.
- Perform system and component functional tests on all UPS equipment to insure proper functioning within specified parameters.
- Run all UPS system diagnostics, and correct all diagnosed problems.
- Resolve any previous outstanding problems, review operation with user personnel, and report any power enhancement or equipment operation recommended changes.

- Replace control batteries at least every 3 years. If the control batteries have been used without inverter or bypass AC power, they may need replacement sooner.
- Off-line load test the UPS system to ensure that the system is completely functional.
- Return the UPS to service following the manufacturer's recommended start-up procedures. Make sure that no damage to the UPS equipment or shutdown will occur because of inrush currents.

Server Shutdown Sequence

In the event of a power failure the UPS infrastructure is sufficient to power our critical servers (Web Server, Domain Controller, SAN) for 20 minutes.

As soon as a power outage occurs, the UPS will begin a shutdown sequence of servers beginning with non-critical servers.

A detailed summary of the shutdown sequence (including scripts) can be obtained from the IS team by contacting support.ischool@utoronto.ca.