



## Section 9: Data Recovery and Protection from Power Surges and Outages

The University (NSU) recognizes the value of university data stored on various computers and requires that certain procedures and capabilities be implemented to protect university data from loss or corruption.

### Applicability

This policy applies to all computers owned and operated by the University. This policy addresses backup and restore procedures and the use of Uninterruptible Power Supplies (UPS) and surge protectors to minimize the effects of power surges and short duration power outages. This policy does not address physical security or system/network security except as necessary for physical protection of storage media.

### Backup and Restore

#### Servers

All file servers must have written backup and restore procedures that include the following:

- Individual(s) responsible for backup/restore procedures.
- Frequency of backup.
- Type of backup (full, partial, changed files only).
- Backup media (CD ROM, ZIP disk, etc.).
- Labeling procedures for backup media.
- Storage location of backup media: media should be protected from dust, heat, direct light, electromagnetic fields (magnetic media), etc. At least one set of backup media should be stored offsite.
- How access to backup media is to be physically protected and access limited to authorized individuals.
- Number of sets of backup and the rotation scheme.
- Conditions under which a restore will be implemented.
- Individual(s) authorized to request a restore procedure be performed.
- When performing a restore, how is data entered/changed since the last backup to be recovered.
- Type of restore performed (full or partial).
- Individual(s) to be notified when a restore procedure is performed.

## **Personal Computers with Critical Data**

Personal Computers (PCs) containing critical administrative data necessary for the University to continue to operate in an efficient and uninterrupted manner must be stored on a shared directory maintained by Information Systems. This ensures that all such data is backed up and available in the event the hard disk in the PC becomes damaged or unusable.

## **Personal Computers**

Backup and restore procedures for Personal Computers (PCs) that perform routine work (word processing, e-mail, etc.) are an individual responsibility. Individuals should ensure that the files needed to continue their routine work are periodically backed up to enable them to perform their work on another PC in the event of PC failure or data loss. Information Systems can assist users in establishing individual backup and restore procedures.

## **Protecting Data from Power Surges and Outages**

Power surges and unexpected power outages can potentially result in damage to hardware and the loss or corruption of data. Protection from these events may be provided through the use of surge protectors and Uninterruptible Power Supplies (UPS). Surge protectors provide protection for computers from electrical noise and damaging power surges. UPS instantly switches a computer to emergency battery backup power and allows the system to safely continue to operate through brief power outages or to gracefully shut down the system in the event of an extended outage. Information Systems can provide assistance in recommending a proper UPS or surge protector.

There is a wide variety of surge protectors. Some afford extremely limited protection and others provide an optimum level of protection.

Surge protectors should never be daisy chained as one or both surge protectors may be severely damaged.

Laser printers should not be connected to an UPS device.

## **Servers**

All University servers purchased after July 1, 2002, will be equipped with an UPS device that will enable the server to continue to operate for at least 20 minutes during a power outage. These servers will also be configured with an UPS that will enable the server to automatically shut itself down after a certain period of no main power. Although not required, it is highly encouraged that all servers purchased before the aforementioned date also be equipped with UPS devices.

### **Personal Computers with Critical Data**

All University PCs purchased after July 1, 2002, with the intent to hold critical data will be equipped with an UPS device that will enable the server to continue to operate for at least 10 minutes during a power outage. These PCs will be configured with an UPS that will enable the PC to automatically shut itself down after a certain period of no main power. Although not required, it is highly encouraged that all PCs holding critical data and purchased before the aforementioned date also be equipped with UPS devices.

### **Personal Computers**

As a minimum all University-owned PCs will be equipped with a surge suppressor.