Revised April 17th, 2012

Definitions

- **Data** here refers to data that is intended to be backed up. All data that is intended to be backed up shall receive equal treatment under this policy.
- For the purposes of data recovery, **Backup Media** refers to any storage medium which contains data that is not suspected or known to be corrupt.
- A device's **Reliability** is defined to be the Unrecoverable Read Error (**URE**) rate divided by the number of bits on the device.
- A **Device** is a disk or set of dependent disks which hold a single copy of all the data (note that the original data source is a device under this policy). Dependency includes any form of direct mirroring including, but not limited to, RAID or rsync mirrors.
- A **Source Device** contains the canonical representation of a set of data. It is the source from which other devices copy.
- A **Backup Device** backs up a source device. It may also be a Source Device, but not for the same data or for any subset of the data it backs up.
- **Off-Site** is defined as either:
    a. an online backup service that will distribute the backup and guarantee (within reason) its safety and security
    b. a site no less than one hundred (100) miles away from the on-site backup.
- **Backup Software** is a software or firmware based tool for transferring data from a source device to a backup device.

Backup Policy

1. All data shall be backed up to at least three devices.
2. All data shall be backed up to at least one (1) off-site device.
3. The off-site devices shall never be on-site, except in the event that:
    a. No on site backup or source device is available in on-site recovery step 6
    b. The off-site device is required for maintance or synchronization AND another off-site device is maintained throughout the maintance/update period.
4. All data shall always exist on at least two (2) devices.
    a. If at any time this number falls below two (2), the number one priority, despite anything else this document may say or any other circumstances or events (ethics and local laws excepted), is to restore this number to two.
5. Backup devices shall not be chained (every backup comes from the source device).
    a. Chaining is allowed if and only if the backup device eventually verifies its data with the source device directly. The backup is not complete until this direct verification has occurred.
6. At least two (2) backup software tools shall be used at all times. This does not affect the number or distribution of backup devices.
7. No backup device shall ever be more than twenty four (24) hours out of sync with its source device. If a device fails to meet this clause, the device shall be treated as corrupt / lost, and, if necessary, the recovery procedure shall be initiated.
    a. The clause does NOT apply in the event that a restore to this device or the creation of a new backup device (as applicable) could not be completed before the existing device can be brough back in sync.
8. If a device's reliability is less than or equal to ten (10), you must consider the device corrupt unless it is part of device which can detect AND correct a URE (such as RAID5).
    a. If the previous clause applies to a device, said device can not be considered to have the failure redundancy provided by the recovery mechanism in use to correct a URE.

9. Efforts to resolve software related problems as described in step 4b of the Recovery Procedure shall not continue for more than twenty four (24) hours, after which time the user must proceed to either step 4a or to step 5.
10. In the event that the user feels too tired or otherwise incapable of safely continuing the recovery procedure, the user MUST immediately shut down all devices. The user shall then write a brief summary of the problem(s), current theory(s), and general status of the recovery, including the current step of this procedure that the user is on. Then, sufficient rest/recovery shall be acquired before continuing with the recovery procedure.
11. A copy of these rules shall be placed in a publicly visible place near any and all on-site devices.
12. Violation of this policy is punishable in some way which is annoying to the user and proportional to the offense.

Recovery Procedure (On-Site)

1. IMMEDIATELY properly shut down and disconnect a backup device. A backup device shall remain shut down and disconnected throughout this recovery procedure.
2. Shut down the failed device. If the failed device is a set of drives (as in a RAID enclosure, even when operating in a JBOD configuration), the entire device must be taken offline. In the case of a JBOD or similar device, any drives not being used as backup media with respect to the failed device may be removed from the backup device and may continue to be used in a different device (including the failed device).
3. If:
    a. the failed device is not the source device
    b. a backup device does not exist to replace the backup device which was taken offline
    c. a device is available to replace the failed backup device

    proceed to step 6 of this procedure as it applies to the replacement device, and then continue with step 4 of this procedure.

4. Assess the symptoms of failure to determine if the problem is hardware or software related.
    a. Hardware Related: If the device is under warranty, connect the failed device to a device which is not a backup device or source device with respect to the failed device, and securely erase the data. If the device is not under warranty, physically destroy and dispose of the device.
    b. Software Related: Diagnose the system and determine a detailed recovery plan. Have this plan evaluated by someone semi-knowledgeable in computer things. Follow the plan.
5. Acquire a new hard disk(s) and / or disk enclosure(s) and properly install. If the drive must be mailed:
    a. If rule 4 of the backup policy is currently being violated, the fastest available shipping method must be selected.
    b. In all other cases, shipping must be estimated to take no longer than five (5) business days.
6. Format the new device, and proceed to restore data from a backup or source device.

Recovery Procedure (Off-Site)

1. IMMEDIATELY properly shut down and disconnect a backup device. A backup device shall remain shut down and disconnect throughout this recovery procedure.
    a. If the off-site backup is kept at a location meeting part b of the definition of off-site, the user shall contact the owner of the off-site backup to assess the situation.

i. If the problem is with the backup media, the user shall begin working with the owner of the off-site backup to initiate the recovery procedure for an on-site backup, beginning with step 2, and treating the off-site location as the on-site location and the on-site location as the off-site location for the purposes of the recovery process.
ii. If the problem is with the network connection and it is likely to persist for more than twelve (12) hours, the user must begin implementing step 2 of this procedure.

b. If the off-site backup is kept at a location meeting part a of the definition of off-site, recovery may be attempted for a maximum of twenty four (24) hours after this recovery procedure is initiated.

2. If recovery fails, the user is given a maximum of forty eight (48) hours from the declaration of failure (or the beginning of execution of this step as directed by this policy, whichever comes first) to designate and establish a new off-site backup. The user must do everything reasonably possible to expedite the backup process to the newly established off-site location.