



Data Security Policy

Version 2.1 - August 29, 2010 - mdille3@club, lroop@club

Guiding Principles

This policy is in place to prevent potentially sensitive CMU Computing Services or CMU Computer Club data from leaking to untrusted parties. Careful adherence will allow the club to remain in the good graces of Computing Services, preclude an unpleasant public relations incident, and avoid a scramble to identify leaked data and secure potentially compromised services.

Used Hard Disks

Used disks are obtained primarily as donations from Computing Services or (occasionally) SCS facilities. Such disks may be in varying levels of working order and should have been wiped before we received them (and, in an effort to maximize our flow of used hard disks, the club presents a standing offer to wipe disks under Computing Services supervision to spare them labor). However, as a precaution, the disks should be treated as though they may contain sensitive Computing Services data, and reasonable steps should be taken to securely segregate them until the receiving procedure has been completed.

The receiving procedure shall consist of running a destructive read-write test using the linux *badblocks* utility, both testing the disk and writing random data to all sectors, destroying any data which was previously on the disk. This allows us to both ensure that the disk is in good working order, and ensure that data previously stored on the disk is not recovered and misused. The used disk shall then be clearly labeled with "Badblocks OK" and the date when the test was ran. This prevents the disk from being confused with untested disks.

New Hard Disks

New hard disks should not contain any sensitive data, and should be in good working order, so they can be placed directly into service. The disks will be formatted as necessary for the purpose they are intended to be used for, and this should eliminate any chance of a virus that was written onto the disk at some point in the supply chain infecting our machines.

Also, new hard disks should be labeled with the date of purchase, and a copy of the purchase receipt should be stored in a safe location for warranty claims.

Handling of Defective Hard Disks

When a disk fails, it should be removed from service and replaced with a disk of equal or greater capacity as soon as possible to allow the RAID array (if applicable) to rebuild before further disk failures occur.

If the failed disk is still under warranty, it shall be returned to the seller or manufacturer as applicable for replacement. If at all possible, the disk should have a destructive *badblocks* pass run on it to remove any Computer Club data. At very least, a sincere attempt to write random bytes to the first few sectors of the disk should be made to obscure the format of the filesystems.

If the failed disk is not under warranty, it shall be marked with a large "X" symbol in black ink on the top of the disk to ensure that it is not returned to service. The failed disk shall then be placed in the "Defective Hard Disks" box. Periodically, the box of defective hard disks shall be delivered to Computing Services to be erased and disposed of by procedures of their choice (eg, degaussing and recycling). As a polite gesture, whoever delivers this box should offer to run the disks through the degaussing machine to spare Computing Services labor.