Astronomy Department Computer Security Policy

Astronomy Computer Committee

March 14, 2014

The UMD data security breach provides us with an opportunity to re-evaluate the computer security policies of the department. Due to the vigilance of our IT staff – Bill, Mark, and John Ohlmacher before them – we have had very few security breaches on the Astronomy Department computer network in the last 20 years. This is no reason to rest on our laurels, however, so reiterating our existing policies while updating others is in order. This will result in a system that is both more secure and easier for us to maintain.

Note the department does not maintain laptops except to register them on the DCHP server. Laptop security is up to the owner.

1 All Desktops

The following apply to **any** desktop computer attached to the Astronomy or UMD network. While non-networked machines should conform to these guidelines, they are not required to.

1. All user accounts must have strong passwords. Note difficult to guess does not necessarily mean difficult to remember – see `http://xkcd.com/936/`.
2. Passwordless accounts are not allowed.
3. For computers maintained by the department, user accounts are disabled 3 months after the user has left the department. After 6 months, the user account and files on public disks are deleted. Full details this policy, including exceptions are described on the Astronomy computing wiki.
4. **No** devices, e.g. desktop computers, laptops, printers, network interfaces, routers shall be connected to the Astronomy network without explicit consent of the IT staff.
5. Desktop computers shall not be removed from the Astronomy network nor moved to another jack without explicit consent of the IT staff.
6. Only persons specifically designated by the IT staff may have administrator/root access.

2 Laptops

Before your MAC address is registered with our DCHP server you will be asked to verify the following:

1. All user accounts should have strong passwords, especially root/administrator accounts.
2. OS and application security patches are up to date
3. Where applicable, virus/malware protection is up to date.

3 Mac

In addition to the guidelines for All Desktops, the following apply to Mac desktop computers attached to the Astronomy or UMD network. While non-networked machines should conform to these guidelines, they are not required to.

1. OS and application security patches are kept up to date.
2. Owner must monitor machines for security incidents and report any breaches immediately to the department IT staff.
3. Where applicable, virus/malware protection are kept up to date.

4 Windows

In addition to the guidelines for All Desktops, the following apply to Windows desktop computers attached to the Astronomy or UMD network. While non-networked machines should conform to these guidelines, they are not required to.

1. Department groups that use multiple Windows computers shall designate one person in that group to maintain said machines and be the IT contact. Maintain means:
   (a) Keep all operating system and anti-virus/anti-malware software up to date.
   (b) Monitor machines for security incidents and report any breaches immediately to the department IT staff.
   (c) Become an active member of the Astronomy Computer Committee.

   Mark Wolfire is the designated IT contact for the staff computers.
2. All machines will have an administrator login to which the designated IT contact has the password. Only this account may install or remove software from the OS.
3. All computers will use the anti-virus/anti-malware software recommended and provided by the UMD Division of IT. This is currently Microsoft Forefront. **Other AV software such as Norton and MacAfee shall not be installed**.
4. All computers must be on an OS currently supported by Microsoft, specifically Windows 8, Windows 7, and Vista. They **do not** include Windows XP, Windows ME, or Windows 2000. (See Microsoft Windows Lifecycle Factsheet).