The goals of the Plant Pathology and Nematology Computing Policy (CP) are to: 1) maintain the integrity and safety of the department computing systems and networks; 2) maintain computing activities of the department in accordance with University policy; and 3) assure efficient use of IT staff time. Specifically, the CP sets forth standards outlining: support for purchasing, installation, and maintenance of departmental and extramurally funding computing systems, including hardware and software; computer access; operating system (OS) and network security; backup practices; and disaster recovery procedures. All computing systems that are UCD property and are owned by Plant Pathology and/or Nematology are managed by the departmental IT support staff, and must comply with the guidelines from the UC Davis Cyber-Safety Program (<http://manuals.ucdavis.edu/ppm/310/310-22.htm>).

This computing policy document will address the following hardware, software and network technical areas**:**

**Purchasing, installation, and licensing**

**Technical support and maintenance**

**Personal or non-UCD owned computer systems**

**Departmental or Lab web sites development**

**Computer Access (Physical and logical access)**

**Operating Systems, Wireless and Network security**

**Backup, archiving, and storage of data**

**Disaster Recovery**

**Purchasing, installation and licensing of Hardware and Software**

* As stated in the UCD POLICY & PROCEDURE MANUAL Section 350-26 (Acquisition of Computers, Computing and Networking Equipment, and Commercial Software), all hardware and software acquisitions must be suitable and cost-effective for the intended application; and must be consistent with departmental and/or school or college, UCD, and University wide computing policies.
* Hardware and Software supported by the department IT staff must be approved, purchased and installed by IT staff. Special hardware and software used by some faculty, staff and departmental laboratories for their research will be supported to the extent allowed by IT staff training. IT staff will provide guidance to faculty and staff to assist them in purchasing hardware and software suitable for their needs. Recommended UCD acquisitions for the latest computer configuration can be seen at <http://computerownership.ucdavis.edu>
* The department will endeavor to provide resources for IT staff to gain proficiency in support of such the above stated hardware and software for which there is sufficient demand.
* Software installed by any non-IT staff to any departmental laptop or home-office desktop, must be licensed and a copy of the license purchase order should be provided to our departmental purchasing office as proof of its legitimacy.
* Server based software will be permitted on departmental computing systems only if their users of these systems are adequately trained on the software, the software is properly licensed and it does not represent a security risk to our departmental systems and networks.
* IT staff will not install any type of peer-to-peer file sharing software (e.g. Kazaa, Mule, Limewire, Bear share, Bit Torrent, etc), or any other software that promotes the high use of our network’s bandwidth. IT staff will periodically access departmental computers for compliance and will eliminate unlicensed and illegitimate files after written discussion with the user.
* It is against the law and against University policy to install unlicensed software on departmental computers.

**Technical support and maintenance**

* Computing systems owned by the University and by the Departments of Plant Pathology or Nematology will receive full technical support on their hardware and software problems.
* All departmental computing systems will be managed by the IT staff and they will be set on our firewall protected departmental networks where they can have access and be able to use shared computer services such as file servers and printers offered by the departments.
* Departmental lab servers will be under the management of the IT staff or under the lab IT personnel who work closely with the departmental IT staff to make sure that these computing systems comply with the UCD Cyber-Safety Program, University and departmental computing policies.
* Personal home-office and laptop computers used in department – related activities by our faculty will be supported as resources permit, provided these systems comply with the UCD Cyber-Safety Program, University and the departmental computing policies.
* Windows, Macintosh, Linux and Solaris operating systems will be supported to the extent of IT familiarity with the specific issue.
* IT staff will not be expected to provide support for hardware and software that are inadequate for their intended use or for non-work related use.

**Personal or non-UCD owned computer systems**

* All personal or non-UCD owned computer systems must have an operating system vulnerability and network security check up from a member of the IT staff before they can be connected to our networks.
* All personal or non-UCD owned computer systems will be granted network connectivity only on the non-restricted departmental network, provided that they do not violate University, UC Davis Cyber-Safety Program, departmental computer policies or compromise network security. Post doctoral researchers, project scientists students, research visitors or seminar speakers, among others, that wish to have internet connectivity from our departmental networks using their own personal laptops or computing systems must bring their computer systems to the IT staff to be granted network connectivity.
* All personal or non-UCD owned computer systems that do not comply with the UC Davis Cyber-Safety Program, University and departmental computer policies and potentially compromise network security or have become compromised (by hackers, malware, spyware or viruses) will be denied access to the departmental network. Such systems will only be allowed to connect to our networks after they have been cleaned, secured and brought into compliance by their owners and deemed safe by the IT staff.
* Technical support for personal or non-UCD owned computer systems will be limited to verbal technical guidance on how to fix a specific hardware or software problem, as time and resources permit, or the owner will be directed to a vendor that can provide the needed service.

**Departmental or Lab web sites development**

* Departmental and Lab web sites should comply with the UC Davis web policy and standards.
* Lab web site developers must work closely with our departmental web manager to ensure compliance with the UC Davis web policy and standards.
* IT staff will only provide coding and web development support to primary departmental web sites and applications.
* Lab web sites are considered to be secondary web sites.
* Any special lab project or development of a software application will be the responsibility of the lab’s Principle Investigator and his/her staff, unless alternative arrangements have been made with the departmental IT manager.

**Computer Access (Physical and logical access)**

* All departmental computer users will logon to their departmental computer systems with a unique non-administrative or limited username and account provided by the IT staff.
* Users using a Microsoft Windows operating system (OS) based computer will login with a Microsoft domain username and account.
* Users running a different OS than MS Windows on their office or lab computers will login to their system with a local user account as his/her regular daily working account.
* Laptops and home-office computers running the MS Windows operating system or office or lab computers running Macintosh, Linux or Solaris operating systems will have a local account with administrative privileges that will be used only when the system (i.e. laptops or home-office computers) are not in any of the Plant Pathology or Nematology buildings and no IT staff is available to the user of these systems when he/she needs to work on a hardware or software problem and cannot wait for help from the IT staff.
* Departmental computers will be physically locked down or kept in a locked room. Departmental laptop computers must be locked if kept overnight.
* All computing systems in our departments and connected to the network must be secured with a screen saver with password, as required by the UC Davis Cyber-Safety Program policies.

**Systems, Wireless and Network Security**

All Cluster computers will be setup, configured, secured and supported by IT staff as required by the UCDCS P and Cluster’s security policies.

**Microsoft Windows:**

* Microsoft Windows based computers will participate in a centralized Windows domain; have antivirus software installed and maintained by IT staff, and be protected by a network firewall.
* For Clusterly owned Windows computers, Windows domain membership will provide global client configuration of security policies, OS hardening, port blocking through domain group policies and software patching through the Windows Server Update Services (WSUS)

All Microsoft Windows system that do not participate in the Cluster Windows domains must be set in our unrestricted Cluster (DMZ) network subnets. PIs will be responsible for the cost of installing any needed Data NAMS, NAM modifications, and their monthly NAM costs to accommodate these Windows systems in the DMZ network.

**Apple Macintosh:**

* Computer systems running Apple Macintosh operating system will be secured as the UC Davis Cyber-Safety Program recommends and set to daily security operating systems updates.

**Linux/Unix:**

* All departmental Linux/Unix computer systems will be setup, configured, secured and supported by IT staff as required by the UC Davis Cyber-Safety Program and Cluster security policies.
* A request to host and setup a Linux/Unix based computer in our Cluster networks must be sent to the IT support group for approval. Upon approval it will be created and setup as needed. Unauthorized Linux/Unix computers will be denied network connectivity and banned from our departmental networks.
* Cluster Linux/Unix based computers will be secured (hardened) and setup in our Cluster networks according to the UC Davis Cyber-Safety guidelines and by any guidelines from the NSA (National Security Agency), SE-Linux (Security-Enhanced Linux) project or from the SANS (System Administration, Networking, and Security) Institute’s Linux Security Check List that may enhance the security of the systems and of our networks.
* All Cluster Linux/Unix system must be set in our unrestricted Cluster (DMZ) network subnets. PIs will be responsible for the cost of installing any needed Data NAMS, NAM modifications, and their monthly NAM costs to accommodate the Linux system(s) in the DMZ network.
* Linux/Unix Virtual Machines images (VMI) are preferred and will be the first choice of setup rather than the physical standalone system. The VMIs allows efficient manageability, easy setup/configuration, easy backup/restore with minimal downtime, and provides an isolation computing environment in case the system becomes compromised.
* If a Linux/Unix VM has to be hosted in a Cluster computer inside of our firewall, the security of the VM and host computer needs to be high.
* No administrator accounts will be given to users
* The VM network configuration will be set to use NAT and the IP of the host machine will be shared with the VM.
* Linux/Unix and VM host machine must have different root, administrator and usernames passwords or passphrases of at least, 15 characters.
* Windows based VM host machine will not be part of any Cluster Windows domain.
* Support to the Linux/Unix systems will be done by the IT staff as much as their technical capabilities allow.
* The regular maintenance of the Linux/Unix systems will be the responsibility of the user. The user most notify the IT staff when problems arise applying these updates. The IT staff will provide a security check on these systems quarterly or before as needed.
* The two Cluster network firewall protect all Cluster network subnets and restricts access to any non-authorized user or computer systems that tries to get into these subnets. As default, the ingress and egress rule sets of the firewall block the incoming and outgoing traffic to and from our subnets.
* Requests for any service to inbound and outbound ports (like FTP, SSH or file sharing services) outside the Cluster networks will be granted or denied after a network security assessment by the IT staff. Otherwise, these ports will be closed by our Cluster firewalls.
* The operating system firewall must be active in each computer to provide a second layer of protection from internal and external intrusion. Incoming traffic will be blocked by default.
* Detailed documentation for the computing configuration/setup, firewall configuration, and antivirus software will be kept restricted and up-to-date within the IT staff documentation in our file server.

**Wireless:**

* The campus Moobilnetx or Moobilnet wireless networks will be preferred by all Cluster offices and labs for their wireless connectivity needs when they are available.
* **Moobilenetx** is the on-campus wireless network available to all UC Davis computing account holders. It employs an encrypted authentication protocol called 802.1x and all wireless traffic between your laptop and the wireless access point is encrypted. Once you configure your laptop and authenticate onto moobilenetx, your wireless connection will auto-associate with all moobilenetx access points. Please see instructions below on how to authenticate to moobilenetx.
* **Moobilenet** is the legacy wireless network that is available to all UC Davis computing account holders and sponsored guests. moobilenet employs a browser-based captive-portal authentication and this means that there are limitations on "roaming" from one wireless access point to another (you may have to re-authenticate if you change buildings while using moobilenet) and the wireless traffic between your laptop and the wireless access point is not encrypted.
* If the campus Moobilnetx or Moobilnet wireless networks are not available and an office or lab needs a wireless networks then All Cluster wireless routers must be configured and installed by the IT staff.
* All Cluster wireless routers must be setup on the non-restricted Cluster network.
* All wireless routers must be configured and secured properly by using strong passphrases and using the most current generation of security protocols..
* Wireless router passphrases are kept by the IT staff and are given to the PIs and lab managers and should not be distributed among the lab members. When a passphrase is compromised the passphrase on the device will be changed and kept by the IT staff and PI only.
* Computer users that request access to our lab wireless networks need to have a computer security check from the IT staff before they try to join to the lab wireless network. If no member of the IT staff is available at the time when a computer user needs access to the lab wireless network and the PI or lab manager determines that they cannot wait for the IT staff, then the PI or lab manager can grant wireless access to the user. After being granted wireless connectivity, the PI or lab manager must ask the user to bring his/her computer system to the IT staff for a security check.
* All wireless routers passphrases in all our conference rooms and classrooms will be changed at the end of every academic quarter.
* Computer users that request wireless access in our classrooms and conference rooms will be granted access at the discretion of our Faculty, CAO or IT Staff.
* Detailed written information on the configuration, setup and management of our departmental wireless routers and networks is kept by the IT staff.
* Periodically network and security vulnerability scans will be conducted as precautionary measurement to detect weak and vulnerable systems in our Cluster networks.

**Backup, archiving, and storage of data**

* The Cluster IT staff will not backup personal or non-work related data stored on the local hard drive of individual workstations. It will be incumbent upon each user to backup their own data to alternate media on a regular basis to protect their own personal data.
* The Cluster IT staff will not backup data stored on the local hard drive of individual workstations. It will be incumbent upon each user to backup their own data to the Cluster NAS or to an alternate media, if one of the Cluster NAS servers was not chosen as their primary data source.
* NAS servers are available to all our cluster desktops that can be used as their primary source of their data or as their secondary depository of their local data. However, the first option is recommended as backups from the local machine to the NAS since may fail unnoticeably.
* All work related data from the Phoenix cluster will be backed up and archived to the cluster NAS servers.
* NAS data will have differential /incremental backups performed daily and full backups will be performed every month.
* Monthly backups will be performed the first week of each month and they will be archived for at least six months and will be stored on the Phoenix cluster NAS servers.
* To test the veracity of backed up data , partial data restores will be performed on all backup NAS folders, mainly on the monthly folders.
* In addition, all the data from one NAS server will be backed up to the other NAS server. This backup from one NAS to the other will make the our backups system a “fault tolerant backup system”. What it means, is that in the event that one NAS becomes inaccessible for any reason then the other NAS should be able to serve the users of the other NAS.
* Mission critical and work related data should be stored in the Phoenix NAS servers.
* Data files which contain sensitive or personal information (e.g. social security numbers, credit card numbers, etc.) are not allowed to be stored in the cluster NAS servers or in any computing systems, as required by the University of California and UC Davis Cyber-Safety Program policies.
* Periodical scans to find sensitive or personal identifiable information (PII) in the cluster NAS servers will be conducted to avoid the storage of such files on the systems. Users are responsible in reading and removing sensitive or PII data from their computer/NAS folder per UC Davis Policy and Procedure Manual Acceptable Use Policy Section 310-23

**Disaster recovery**

* In the event of a catastrophic hardware or software or failures the IT staff will work only on cluster computing systems to rebuild them and/or to restore their lost information from them.
* To prepare for this event on the servers, an up-to-date copy of the Cluster Disaster Recovery Procedures document will be kept available to the IT staff at all the times. This document will aide in the restoration of infrastructure, data, and services. Lost infrastructure may include the local area network (LAN), servers, client computers, and peripheral devices.
* To restore the LAN, IT staff will need to contact the campus Network Operations Center (NOC). The campus NOC will work in conjunction with IT staff to restore the physical and logical LAN.
* To restore lost computer systems, IT staff will need to approve the purchasing of client and server computers as well as the purchasing of any lost peripheral devices such as printers or network switches that were lost. With network and server infrastructure in place, IT staff will use the information from the Cluster NAS servers to restore data and services to the department.
* A detailed disaster recovery plan will be documented within the Clusters’s Disaster Recovery Plan Procedures document.

#### References:

#### UCD POLICY & PROCEDURE MANUAL

#### Section 350-26 - Acquisition of Computers, Computing and

####  Networking Equipment, and Commercial Software