Departmental General Computing Policy
(DGCP)
Updated April 2017

The goals of the Departmental General Computing Policy (DGCP) are to:
1) Maintain the integrity and safety of the departments of Entomology and Nematology and Plant Pathology computing systems and networks
2) Maintain computing activities of the departments in accordance with University policy
3) Assure efficient use of IT staff time. Specifically, the DGCP 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 the departments of Entomology and Nematology and Plant Pathology 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.pdf)

This computing policy document will address the following 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

- All hardware and software acquisitions must be suitable and cost-effective for the intended business purpose; and must be consistent with departmental and/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 the campus IT Knowledge Base Article KB0000765 http://kb.ucdavis.edu/?id=765
- 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. eMule, uTorrent, BearShare, BitTorrent, etc), or any other software that promotes the high use of our network's bandwidth and risks the security of our computer systems and networks. 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 Entomology and Nematology or Plant Pathology 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 may be provided consultation services as resources permit, provided these systems comply with the UCD Cyber-Safety Program, University and the departmental computing policies.
- Windows, Macintosh, Ubuntu 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 them to the IT staff to have a security check and if they pass the security check, then they will be granted network connectivity in the non-restricted departmental networks.

- 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 networks. 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 departmental Microsoft Windows operating system (OS) based computer will login to the campus AD3 domain with his/her UCD Kerberos username and passphrase, unless the computer is not joined to the campus domain.
- 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 Ubuntu 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 Entomology and Nematology or Plant Pathology

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.

Operating Systems, Wireless and Network Security

All departmental computers will be setup, configured, secured and supported by IT staff as required by the UCD Cyber-Safety and Cluster's security policies.

Microsoft Windows:

- Microsoft Windows based computers will participate in the campus AD3 Windows domain; have antivirus software installed and maintained by IT staff, and be protected by its internal OS firewall.

- For departmental owned Windows computers, the campus AD3 Windows domain membership will provide global client configuration of security policies, OS hardening, port blocking through domain group policies and software patching through the campus IBM BigFix server and a departmental Windows Server Update Services (WSUS) server.

> All Microsoft Windows system that do not participate in the campus AD3 Windows domain must be set in a non-restricted departmental network subnet. PIs will be responsible for the cost of installing any needed Data NAMs or NAMs modifications to accommodate these Windows systems in the non-restricted network.

Apple Macintosh:

- Computer systems running Apple Macintosh operating system will be secured as the UC Davis Cyber-Safety Program recommends,set to security operating systems updates, set with the IBM BigFix software patching server and be protected by its internal OS firewall.

Linux/Ubuntu:

- All departmental Linux/Ubuntu 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/Ubuntu 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/Ubuntu computers will be denied network connectivity and banned from our departmental networks.
- Departmental Linux/Ubuntu based computers will be protected by its internal OS firewall, be secured (hardened) and setup in our departmental networks according to the UC

Davis Cyber-Safety guidelines and enhanced by the SANS (System Administration, Networking, and Security) Institute's Securing Linux Guide and the Linux Security Check List.

- All departmental Linux/Ubuntu system must be set in our non-restricted departmental network subnets. PIs will be responsible for the cost of installing any needed Data NAMs or any NAM modification to accommodate the Linux or Ubuntu system(s) in our non-restricted networks.
- Linux/Ubuntu Virtual Machines (VM) images are preferred and will be the first choice of setup rather than the physical standalone system. The VM images 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/Ubuntu VM has to be hosted in a departmental computer inside of our restricted networks, the security of the VM and host computer needs to be tighten.
  - 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/Ubuntu 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 be a "stand-alone" computer.

- Support to the Linux/Ubuntu systems will be done by the IT staff as much as their technical capabilities allow.

The regular maintenance of the Linux/Ubuntu 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 as needed.

Network Security

- The Entomology and Nematology and Plant Pathology network firewalls protect all the network subnets of the departments and restrict access to any non-authorized users or computer systems that tries to get into these networks. As default, the ingress rule sets of the firewalls block all the incoming traffic to our network subnets.
- Requests to open inbound network ports for any service (like SSH or file sharing services) outside the departmental networks will be granted or denied after a network security assessment by the IT staff.
- The operating system firewall must be active in each computer to provide a second layer of protection from internal and external intrusion. All incoming traffic will be blocked by default.
- Detailed documentation for the computing configuration/setup and firewall configuration will be kept restricted and up-to-date within the IT staff documentation in our file server.

Wireless:

- The campus Moobilenetx, Eduroam or UCD Guest wireless networks will be preferred by all departmental 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 connections will auto-associate with all Moobilenetx access points.
- **Eduroam** is the wireless network available to all eduroam-enabled accounts. It employs an encrypted authentication protocol called 802.1x and all wireless traffic between your laptop and the wireless access point is encrypted. For more information on eduroam, visit www.eduroam.us/. To use an eduroam account from another educational institution, please follow the instructions linked under "How to get started" on how to connect to eduroam with your operating system.
- **UCD Guest** is the wireless network that is available to all guests of the campus. UCD Guest 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 UCD Guest) and the wireless traffic between your laptop and the wireless access point is not encrypted.
- If the campus Moobilnetx, Eduroam or UCD Guest wireless networks are not available and an office or lab needs a wireless network then a departmental wireless router must be configured and installed by the IT staff.
- All departmental wireless routers must be setup on a non-restricted departmental network.
- All wireless routers must be configured and secured properly and set to use MAC filtering, strong passphrases and one of the following security options: WPA2-PSK [AES], WPA-PSK [TKIP] + WPA2-PSK [AES] or WPA/WPA2 Enterprise.
- 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.
- Computer users that need wireless access in our classrooms and conference rooms can use the Moobilenetx, Eduroam or UCD Guest wireless networks.
- 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 departmental networks.

Backup, archiving, and storage of data

- The 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 back up their own data to alternate media on a regular basis to protect their own personal data.
- The IT staff will not backup data stored on the local hard drive of individual workstations. It will be incumbent upon each user to back up their own data to the departmental file server, to an alternate media or to CrashPlan, a cloud backup solution that is available to all UCD departments.
- The cloud storage solution Box is available to all UCD departments and our departmental desktops from our offices and labs can use it as their primary source of their data, if preferred.
- If an office or lab has the need to use an in-house file server, then the IT staff will try to find the best solution for the need and it will be presented to the office or lab for consideration.
- All work related data from the departments must be stored and archived using the cloud storage solution Box or in-house file server solution and backed up using CrashPlan.
- The data from the Entomology and Nematology and Plant Pathology is on the cloud storage solution Box which has guaranteed the availability, integrity and security of it at all of the times, same as for the data for other campus departments. The Box file versioning and its 90-day file recovery features can be considered as short-term backup solution. If a Windows based in-house file server is used, then its data will be backed up using CrashPlan with the backup frequency of “one day” and additional versions to keep of “every week”, “every month”, “every six months” and “every year” keeping deleted files for ever.
- To test the veracity of the backed up data, partial data restores of some of the backed up files and folders will be performed from CrashPlan.
- Mission critical and work related data should be stored in Box or in-house file 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 Box, or in any of the in-house departmental file servers or in any desktop or computing systems attached to our networks, 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 in-house departmental file 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 computers or in-house file servers, per UC Davis Policy and Procedure Manual Acceptable Use Policy Section 310-23 and the UC Davis Security Standards Exhibit A (https://manuals.ucdavis.edu/PPM/310/310-22a.pdf).

Disaster recovery

- In the event of a catastrophic hardware or software or failures the IT staff will work only on departmental computing systems to rebuild them and/or to restore their lost data on them.
- To prepare for this event an update copy of a 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), firewalls, 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 servers infrastructure in place, IT staff will use the information from Box, Crashplan or form the in-house file servers to restore the needed data.
- A detailed disaster recovery plan will be documented within the Disaster Recovery Plan Procedures document

References:

UCD POLICY & PROCEDURE MANUAL

Chapter 310 Section 22.a - UC Davis Cyber-Safety Program
Chapter 310 Section 23 - Electronic Communications—Allowable Use