CBS Network Security Policy  
College of Biological Sciences – Deans Office

PURPOSE:

Supporting a large number of computers with varying types of software and user modifications can be a daunting task for IT staff within each of our units. To ensure the integrity of each of our departmental networks, prevent data breaches and allow specific research needs on the network, it is necessary to enact this Network Security Policy to compliment what is set by the UCD campus cyber-safety policy.

SUPPORTING POLICIES:

This policy provides conformance to the UC Davis Cyber-Safety Program. It is your responsibility to be aware of your rights and obligations under the University of California, Davis, Cyber-Safety Policies (P&P 310-22).

UC Davis Cyber-Safety Program (http://security.ucdavis.edu/cybersafety.cfm)


Advantages:

The advantage of this policy to faculty and staff will reduce risk of release of sensitive research data, reduce risk of fines (thousands of dollars) for music/movies, and reduce likelihood of needing to deal with releases of SSNs.

SCOPE:

This policy applies to anyone who uses or has access to the College of Biological Sciences department/center Networks. This will help to bring all CBS in compliance with Cyber-Safety Policy.

POLICY:

The PI is ultimately responsible for all computing and network activity within their labs.

1. Department Firewall:
   1.1. By default the firewall will block all inbound traffic to reduce vulnerabilities according to campus Cyber-Safety policy. Any hosted services (i.e., websites) on the Network must have faculty/PI approval before they are allowed access. All access should be documented. All exceptions must be approved by the faculty PI, and Dept/Center IT Staff, with notification to Chairs/Directors/MSOs.
   1.2. All outbound traffic will be filtered to only allow business related traffic and/or communications defined as incidental personal use in campus policy 310-23 out through the firewall (http://manuals.ucdavis.edu/ppm/310/310-23.htm).

2. Computer Systems:
   2.1. All Operating Systems must install security related patches within seven days from the posted update as stated in the Campus Cyber-Safety Security Policy. Operating systems must be supported and vendors must supply current security updates.
   2.2. Exception for instrument controller computers (with older operating systems and not vendor supported) must be approved by the Dean’s Office IT staff.
   2.3. Anti-Virus software must be installed and up-to-date with the latest definitions at all times as stated in the Campus Cyber-Safety Security Policy.
2.4. Personal computers may not be attached to the Network without approval of the Dept/Centers IT Unit and validation of systems compliance to Cyber-Safety standards.

2.5. Non University owned computers connected to the network must be available for inspection by the IT Unit to ensure compliance with the campus cyber-safety policy.

2.6. Peer to Peer networking (e.g. Bit torrent) software must be used only for business purposes will not be supported by the IT Unit staff.

3. Printing:

3.1. All network devices, including printers must comply with 2.4 see above.

3.2. Use of Administrative printers is for official University business only.

3.3. Network based shared printers are provided for the majority of printing needs. Individuals may request help in setting these printers up using the Dept/Center IT Staff.

4. Storage of Personal/Campus Information:

4.1. On devices connected to the department network, storage of personal information such as bank account information, social security numbers, driver's license numbers, and/or credit card information is not permitted at any time. Exceptions to this policy for legitimate business needs may only be granted if proper encryption and other security measures are in place and approval is obtained from the Department Chairs/Directors and CBS Dean’s Office IT staff.

4.2. All network connected devices or systems must be made available for bi-annual scanning for personal identification information in order to be compliant with Campus Cyber-Safety Policy.

5. Routers:

5.1. All routers will be the sole responsibility of the PI of the lab who installed the device. They also agree to being the data custodian for all data behind such device. All routers must have access control and have the default password(s) changed.

5.2. If a data access point is needed, we would recommend the NAM be configured to host MoobilNet as this will force each user to identify themselves when connecting to the network.

6. DMCA:

6.1. Copyright infringement (movies and music) is strictly forbidden. As permitted by the Digital Millennium Copyright Act (DMCA), the University may suspend access to Electronic Communication systems by any user allegedly violating copyright law upon receipt of a DMCA notification. http://innovationAccess.ucdavis.edu/dmca. As appropriate, information relating to a particular notification will be referred to campus authorities for review relating to campus policies. Campus authorities include Student Judicial Affairs, Student Housing Judicial Affairs, Human Resources, Vice Provost--Academic Personnel, and, if the individual subject to a notification is a University employee, his or her department head http://manuals.ucdavis.edu/ppm/250/250-05.htm.

EXCEPTIONS:

Changes to this policy need to be approved at the Dean’s Office, Dean’s level.

APPROVAL:

This policy has been approved by the College of Biological Sciences Department Chairs/Directors and CBS Dean’s Office.
REVISION:

Version 1.0 Created Sept, 2010
Future revisions will be made in consultation with input from the Chairs and MSOs.

Direct questions regarding this policy to:

**Dean Bunn**
**CBS Network Administrator, Information Technology**

As a user of the University and my department's electronic communication resources, I have read, understand and will abide by the provisions of the CBS, UC, and the UCD Electronic Communication Policies (P&P 310-23 and 310-24).

__________________________________________
Signature

__________________________________________    __________
Printed Name                           Date

MAC Address(s): ____________________________