UC DAVIS COLLEGE OF BIOLOGICAL SCIENCES

Name: _____

PURPOSE:

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 UC Davis 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 UC Davis Cyber-safety Policy (P&P 310-22).

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

UC Davis Cyber-Safety Policy and Procedure Manual (http://manuals.ucdavis.edu/ppm/310/310-22.pdf)

Universitywide Copyright Policies and Guidance (http://www.ucop.edu/information-technology-services/initiatives/universitywide-copyright-policies-and-guidance-.html)

ADVANTAGES:

The advantages of this policy to faculty and staff is that it will reduce the risk of - release of sensitive research data, fines for music/movies/software copyright infringement, and the likelihood of needing to deal with releases of SSNs.

SCOPE:

This policy applies to anyone who uses or has access to any of the College of Biological Sciences' networks. This will aid the College of Biological Sciences' effort to become Cyber-safety compliant.

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 the UC Davis 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 department/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 (PPM 310-23) out through the firewall (http://manuals.ucdavis.edu/ppm/310/310-22.pdf).

2. **Computer Systems:**

   2.1 All operating systems must have security related patches installed within seven days from the posted update. Operating systems and network accessible applications must be supported and vendors must supply current security updates.

   2.2 Exceptions for instrument controller computers (with older operating systems and not vendor supported) must be approved by the Dean's Office IT staff.

2.3 Antivirus software must be installed and up-to-date with the latest definitions at all times as stated in the UC Davis Cyber-safety Policy.

2.4 Personal computers may not be attached to the network without approval of the department/centers IT staff and validation of the system's compliance to Cyber-safety standards.

2.5 Non University owned computers connected to the network must be available for inspection by the IT staff to ensure compliance with the UC Davis Cyber-safety Policy.

2.6 Peer to peer networking (e.g. BitTorrent) software must be used only for business purposes and will not be supported by the IT 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 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 from the department/center IT staff.

4. Storage of Personal/Campus Information:

4.1 Storage of personal information on devices connected to the departmental network is not permitted at any time. This includes bank account information, social security numbers, driver's license numbers, and/or credit card information. 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 biannual personal identification information scanning to be compliant with the UC Davis 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 be the data custodian for all data behind such a device. All routers must have access control and have the default password(s) changed.

5.2 If a data access point is needed, we recommend the NAM be configured to host MoobileNet, as this requires each user to authenticate when connecting to the network.

6. DMCA:

6.1 Copyright infringement (sharing of movies and music) is strictly forbidden. As permitted by the Digital Millennium Copyright Act (DMCA), the University may suspend access to electronic communications resources by any user allegedly violating copyright laws (http://www.ucop.edu/information-technology-services/initiatives/universitywide-copyright-policies-and-guidance-.html). 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.pdf).

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 1.1 Created April, 2011.
Future revisions will be made in consultation with input from the chairs and MSOs.

Direct questions regarding this policy to:

Paul Hawley
Systems Administrator
College of Biological Sciences Dean’s Office
(530) 752-3076
CBS-Help@ad3.ucdavis.edu

AFFILIATION:

Please check all the CBS units you're affiliated with:

- [ ] CBS Dean's Office
- [ ] Center for Neuroscience
- [ ] Center for Population Biology
- [ ] Department of Evolution & Ecology
- [ ] Department of Microbiology & Molecular Genetics
- [ ] Department of Molecular and Cellular Biology
- [ ] Department of Neurobiology, Physiology and Behavior
- [ ] Department of Plant Biology
- [ ] UC Davis Genome Center

AGREEMENT:

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).

By clicking the “I AGREE” button below, you are electronically signing and thereby agreeing to the terms of this document.

- [ ] I Agree

Signature:_____ Date: _____