RUTGERS
School of Arts and Sciences

Division of Life Sciences

Division of Life Sciences Information Technology

Acceptable Use Policy

Acceptable Use Policy of Systems and Data for Users

The Division of Life Sciences (DLS) has developed an Acceptable Use Policy for Systems and Data for Users in order to ensure all DLS computer systems and information are maintained, secured, managed and utilized in a proper, efficient and justified manner. Please note all DLS computer policies are a supplement to and subject to overall Office Information Technology (OIT) policies and procedures. http://policies.rutgers.edu/PDF/Section70/70.1.1-current.pdf

It is necessary that this Acceptable Use Policy be followed by all employees of the DLS, visitors and anyone performing job related duties or any other tasks using IT equipment on DLS the network.

DLS Information Technology (IT) is committed to providing the highest standard of service for our students, staff, faculty and visitors in support of research, instruction, administrative, and intellectual pursuits. To that end, DLS Acceptable Use Policies provide the framework and guidance for all DLS personnel.

Establishing IT Network Connectivity

All new DLS employees need to attend IT orientation training conducted by the DLS Help Desk Coordinator to receive instructions regarding DLS acceptable use policies; use and purchase of DLS IT supported hardware and software, and guidelines establishing system and network activities.

Procedures for establishing new user account information leading to full IT support of computer and operating system are as follows:

Department requestor (either Administrative Assistant or Private Investigator-“PI”) emails Help Desk informing of new user and providing **all** of the following information:

- First and Last Name

- Position/Title
- Start Date
- Department or program: -Usually any of the following- Genetics, Helpdesk, MBB, RUCDR, NJBM, Keck Center.
- Manager's name
- Office phone number and room number
- DLS email account requirements: An alternate primary contact email address must be provided if a DLS email address is not required or not necessary for any user account created on the DLS Domain. This is done so that users can be notified when their passwords are going to expire.
- Email Distribution group requirements.
- Employment status: Full-Time, Part-Time, Temporary, etc., an account expiration date should be provided if employment status is temporary.
- Equipment requirements: Computers, Smart Phones/Mobile Devices. The requestor must inform DLS IT when equipment is already available for a new user setup. If no equipment is available, DLS IT can provide requestors with quotes for computers or mobile devices that conform to the current IT Hardware standards.
- AD Group Membership requirements: The requestor should provide DLS IT the name of each group that the new user will belong to.
- VPN access requirements: The requestor should notify DLS IT if the user needs access to connect remotely.
- Instant Messenger account requirements

Review DLS IT Action Items

- Active Directory account prepared by IT
- Email account established by IT
- Required access of IT services established for user
- IT configures existing departmental computer for new user or; IT provides quote(s) for new computer hardware by user department
- User department issues purchase order (PO)
- IT tracks PO through receipt of hardware
- IT configures new computer, places in DLS IT inventory
- IT delivers computer to new user workstation

Unacceptable practices that compromise DLS IT security must be avoided

- Peer-to-peer file sharing services such as Gnutella, Kazaa, Bittorrent, eDonkey, etc.

- Video games
- Shareware utilities
- Unacceptable workplace practices, like Dropbox

DLS IT reserves the right to revoke network or VPN access to any machine found to be using Peer-to-peer or any other software or activity that threatens the security of the DLS Network. Network or VPN removal may occur with or without warning and include, but not be limited to the following actions:

- Immediate network port or wireless disconnection
- Immediate VPN disconnection
- Immediate physical machine removal from its current location for containment and scanning purposes
- Permanent network ban for repeat offenders

Once removed, DLS IT will not allow any machine back in the network or VPN, until the machine is clean from all threats and/or the security compromising activity has been neutralized. DLS IT reserves the right to wipe or return machines to their original configuration when necessary to address machine security issues.

DLS Password Security Information:

- Old or previously used passwords cannot be re-used at any point
- DLS passwords expire every 365 days

DLS Password Requirements:

- The minimum password length is 8 characters
- Passwords must start with a letter (either upper or lower case)
- Passwords must meet the following complexity requirements:
    - Passwords cannot contain the user's account name or parts of the user's full name that include two consecutive characters
    - Passwords must contain characters from three of the following four categories:
        - English uppercase characters (A through Z)
        - English lowercase characters (a through z)
        - Base 10 digits (0 through 9)
        - Non-alphabetic characters (for example, !, $, #, %)

The DLS Account Lockout Policy will be as follows:

- Provides protection against brute force attacks

- Account Lockout Duration is 15 Minutes
- Accounts will be locked out after 5 invalid logon attempts within a 15 minute period

DLS IT services:

1. Computer security
    a. Use of DLS computers is only for DLS and university business related activities
    b. Understand the difference between internal Rutgers sites and External internet sites
    c. Never disable or tamper with the DLS NAI Antivirus scanner
    d. Do not leave your password taped to your screen or under your keyboard. Your password should not be written down or made visible
    e. Your password should not be shared with anyone
    f. DLS IT will never request you to email us your password or provide it to us through any other means. Do not send your password to anyone via email.
    g. All DLS computers on the LAN must run an Anti Virus scanner (provided by DLS IT)
    h. All Non DLS or non RU machines on the DLS network must run an Antivirus and the helpdesk will require it during the registration of the machine. All non-DLS or non-RU machines connected to the DLS network should abide by the rules of this and all DLS, SAS, and other Rutgers University policies. Violation of any of these policies will result in machine removal from the DLS network.
    i. Email is not a secure method for transferring confidential or sensitive information. Any information that's sent via email may potentially be seen by others. Do not send any sensitive information via email to anyone inside or outside of the DLS. **Please contact the DLS Helpdesk for assistance if you are in need of transferring sensitive electronic information**
    j. Special care should be observed while opening email attachments or links from unknown or unexpected senders. Please contact the DLS Helpdesk if you have any doubts about the legitimacy of an email message
    k. Under no circumstance should any individual engage in any activity that is illegal under local, state, federal or international laws while utilizing DLS owned hardware or software or while connected to the DLS network through non-DLS owned hardware
    l. Any DLS user or email account that has not logged on for a period of five (5) months or longer will be considered inactive and will be automatically disabled
    m. New DLS user or email accounts will have a 30 day grace period in which to log on for the first time. Any new DLS user or email account that has not logged on 30 days after being created will be automatically disabled

n. All user or email accounts that become automatically disabled will be deleted four (4) months after being disabled, unless the DLS Helpdesk is contacted to re-activate the account. DLS IT will automatically backup any data associated with accounts being deleted, where applicable, before they are eliminated from the system

o. Any DLS computer that has not been logged to the DLS network for a period of five (5) months or longer will be considered inactive and will have its DLS computer account automatically disabled.

p. All DLS computer accounts that become automatically disabled will be automatically deleted 4 months after being automatically disabled, unless the DLS Helpdesk is contacted to re-activate the account

q. The corresponding PI or Administrative Assistant must notify DLS IT via email once a user or email account needs to be terminated. Once notified, DLS IT will disable the user account and remove the user from the Global Address List within a 24 hour period. User files will be made available to the corresponding manager upon request. Email can be forwarded for a maximum period of 1 month if requested

r. This section is only applicable to RUCDR employees. Due to the sensitivity of the data accessed by RUCDR employees, particularly, that data associated with government contracts, there are additional restrictions and monitoring tools in effect, as follows:

i. Unauthorized or improper use of DLS Systems for RUCRD use, which include but are not limited to the following: DLS computers, the DLS Network and all computers connected to it, all devices and storage media attached to the DLS network or to a computer on the DLS Network may result in disciplinary action, as well as civil and criminal penalties

ii. RUCDR employees have no reasonable expectation of privacy regarding any communication or data transiting or stored on DLS systems. At any time, and for any lawful DLS purpose, the university or DLS may monitor, intercept, and search and seize any communication or data transiting or stored on DLS systems

iii. Any communication or data transiting or stored on DLS systems may be disclosed or used for any lawful DLS purpose

iv. RUCDR employees will be presented with a logon banner outlining the conditions above. Access to DLS systems will not be granted to such users until they have agreed to these conditions by pressing the “OK” option on the logon banner

2. Computer backup services

  a. All DLS users get a five (5) GB allotment of redundant, backed up personal network storage, identified as the M: drive
  b. All the contents of the Windows "My documents" folders are automatically re-directed to a network server for file management backup services
  c. Video and music files should not be stored on DLS servers, unless they are strictly required for DLS or University related work activities
  d. All documents should be saved on network shared drives regardless of whether they are saved on local drive(s). DLS IT does not guarantee the capability of restoring any lost files or folders that were not saved to a network drive

3. Wired Networking
  a. Access to wired networking is restricted by Media Access Control (MAC) address and physical inventory, all machines need to be registered with DLS IT prior to connectivity
  b. No switches, mini-switches, mini-hubs or routers are allowed for any reason on the DLS network. These violate DLS policy and will be removed without warning
4. Wireless networking
  a. DLS broadcasts three separate wireless networks:
    i. DLSWireless
    ii. DLSWireless-Secure
    iii. RUWireless-DLS (for student Access)
  b. When using the wireless network please adhere to the Acceptable Use Policy
  c. No Wireless Access Point (WAP) or Wireless router may be added to DLS network
  d. No Service Set Identifier (SSID) or wireless public names may be broadcast on the DLS network
  e. DLS IT reserves the right to prevent devices from attaching to DLS wireless network if they do not meet our minimum security requirements. These are Windows 7 or MAC 10.x fully patched with DLS Anti-virus
5. Firewall
  a. The DLS firewall filters all traffic in and out of DLS IT network for protection against hackers, internet attacks, Malware, Spyware, SPAM and Virus
  b. Any publicly accessible server must meet DLS IT minimum requirements and reside in the DLS datacenter, Room B229, Nelson Biological Laboratories
6. DLS Email
  a. DLS IT hosts, backs up, protects and completely supports all DLS email accounts created on the DLS email server only. DLS IT has no capabilities to manage, support, backup/restore or troubleshoot any issues related to any non-DLS email accounts

b. DLS email accounts are intended to be the primary email accounts for all DLS constituents. As such, email forwarding to non-DLS accounts cannot be made permanent. Any circumstance that requires permanent email forwarding to any non-DLS email account would deem the existence of a DLS email account unnecessary. Thus, such situations will call for the complete deletion of any existing DLS mailboxes and the addition of an address book entry pointing to the non-DLS email address required instead

7. Foreign Language Support
   a. DLS IT does not support any machines with non-western based character languages installed
   b. A best effort will be made to support all machines with western based character languages installed. However, DLS IT reserves the right to limit support to non-English based computers

8. Personal Use of DLS owned computers
   a. Connectivity: DLS IT is only responsible for ensuring proper connectivity to DLS wired and/or wireless networks. DLS IT is not responsible for troubleshooting connectivity problems involving any personally owned wireless and/or wired networks
   b. Software: DLS IT is not responsible for installing or otherwise supporting any software that is not used for the purpose of conducting DLS or other university business related activities. DLS IT reserves the right to uninstall any personally installed, non-supported software if it is interfering with proper operations or if it compromises security. DLS IT is not responsible for the loss of any data that may result from uninstalling this type of software. Further action may be taken if unauthorized software is installed on DLS owned equipment, particularly if it interferes with proper operation or violates DLS, SAS or University policies
   c. Hardware: DLS IT is only responsible for supporting DLS owned equipment. DLS IT may only provide limited assistance to install the necessary drivers for non-DLS equipment connectivity, where applicable, as long as the equipment is being used solely for DLS or other university business related purposes. However, if and when issues arise, it is the responsibility of the user to work with the relevant company’s technical support for resolution
   d. Personal User Data: Users are responsible for backing up any personal data that is present on their systems through their own means. The personal network storage offered to each individual user, identified as the M: drive, as well as any other network storage offered by DLS IT is not to be used for the storage of non-

university related data. This includes, but it is not limited to, personal music libraries, photos, videos or any other personal data. DLS IT will not be liable for the loss of such content at any time

e. A certain amount of incidental personal usage is expected on University devices that are mobile or stationed offsite. For example, it is not uncommon for a University system to be used for personal e-mail and authoring documents. However, systems that are used disproportionately for non-University business will not be supported. Examples of disproportionate use include, but are not limited to, the installation of unauthorized software, the creation of accounts for users who are not affiliated with the University, evidence that the system is primarily used by someone who is not employed by Rutgers University or any other practices that compromise security or violate DLS, SAS or University policies. DLS IT reserves the right to restore any systems that are disproportionately used for non-University business to their original supported state, and to discontinue support altogether for repeat offenders.

Please adhere to Rutgers University Acquisition and Disposal of DLS IT computing hardware and software: (see RU page 5 13.2.3)

All DLS/Rutgers University issued hardware/software assets are property of Rutgers University, including all data generated by or residing on DLS issued/approved/registered equipment.

1. DLS IT will provide support for hardware/software on the following equipment:
   a. DLS IT recommends HP Business machines for laptops and desktops. Please contact the DLS helpdesk for an updated quote
   b. DLS IT also supports Dell Business Machines , please contact the DLS helpdesk for an updated quote
   c. DLS IT recommended Apple MAC Pro Product line devices, as well as MAC Mini and IMAC devices. Please contact the DLS helpdesk for an updated quote
   d. DLS IT Supports Lenovo Business Line Laptops, please contact the DLS Helpdesk for an updated quote
2. Any non HP business, Dell Business or Apple machine will not be supported by the DLS Help Desk. DLS IT will add the machine to the DLS network upon request and install the DLS antivirus if needed. No other re-imaging or updating will be done and the user will be 100% responsible for the unit.

   Personal computers: DLS IT will not support <u>personal</u> computers for DLS or off-site.

Please inform the DLS IT Help Desk before disposal of any/all DLS computing hardware/software. Rutgers University Equipment Transfer/Disposal Form must be completed before removal from premises of any assigned hardware/software equipment

DLS Internet Filtering Services

a. All DLS internet requests are compared against a Real Time Black List (RTBL) in real time for protection against SPAM, Malware, Spyware and Virus
b. A particular site may be blocked due to malware, SPAM or Malicious content; a block page will inform the user of the block.
c. A multimedia site may also be blocked when DLS total bandwidth exceeds 30%, a block page will inform the user of the block.
d. All DLS internet activity maintains an electronic fingerprint that can be retrieved and scanned for authorized use.

Smartphone's and Mobile Devices

a. DLS IT only supports Windows Phone 7, Android, and IPhone smartphones on the ATT network. The network provides global coverage. Please contact the helpdesk for coverage.
b. DLS IT will make a best effort to connect any unsupported device or any supported device not on the ATT network to the DLS email system or DLS wireless network if time permits.