D'Youville

Campus Computing Policies

(Effective Date: March 1, 2005)

1. **Campus Network Infrastructure Includes:**
    a. Cable plants (i.e. copper, fiber and wireless, patch panels, patch cords and line testers for voice and data)
    b. Network Appliances (i.e. voice/data/video switches, routers, firewalls, gateways and wireless access points)
    c. Network Addressing and Resolution Services (i.e. DHCP, DNS)

2. **Campus Automated Services Include:**
    a. Hosts: servers or end-user hardware that can be assigned an IP address (i.e. workstations, PDAs, laptops, phones, printers)
    b. Software Applications: (office applications, anti-virus, backups, academic software, video streaming & VoIP)
    c. Data, databases and report generating applications
    d. Procedures, processes and host configurations to install, secure, operate and maintain hosts and their data & applications

3. **DYCnet Defined**
    a. DYCnet is comprised of all of the College's Network Infrastructure and Automated Services.
    b. There are several networks that together, comprise DYCnet including but not limited to: academic, administrative, telecommunications, departmental and test networks using part of DYC's network infrastructure and providing automated services to a user base within the college community. The sum total of these networks, their resources and the College owned standalone hosts comprise what is referred to herein as "DYCnet".

4. **DYCnet Operation & Management:**
    a. Operation and management of the network infrastructure is the primary responsibility of the Computer and Network Services (CNS) Department.
    b. CNS shall provide the greatest operational flexibility possible to the greatest number of college-affiliated users, short of compromising the operational integrity and security of the network resources.
    c. Certain academic and administrative departments may be delegated operational

responsibility for some network appliances and servers when deemed necessary to meet academic or administrative initiatives more efficiently. These delegations shall be coordinated through the DYC Network Administrator and the other department representatives as needed to maintain operational flexibility without compromising security.

5. **Rogue Network Components:**
    a. Rogue hosts, rogue services and rogue applications are unauthorized network components attached to and providing or using DYCnet resources, which are not authorized, protected or supported as an official part of DYCnet.
    b. Rogue components on DYCnet may be subject to removal from DYCnet and possible confiscation by the corresponding System or Network Administrator at any time, without the requirement for prior notice to the "owner" of the rogue component.
    c. In the case of personal property, confiscated components may be returned pending a review in accordance with the policies outlined in the student or employee handbooks,or local, state and federal laws.
    d. D'Youville shall not be held liable for any damages to rogue components removed from DYCnet and held by any agent of the College including but not limited to law enforcement.

6. **Purchasing, Acquisitions, Donations and Inventory:**
    a. CNS is responsible for the installation of all DYCnet components. Therefore, CNS must know in advance what is needed, when it will be acquired and how the component will be used in order to provide support for it.
    b. In accordance with the Purchasing Office Procedures, CNS maintains the right to review all purchases or donations of computing components prior to acquisition, particularly if those components are intended for installation on DYCnet.
    c. Acquisition of client/server software with the intent of installing it on DYCnet shall be declared to CNS early in the acquisition process to ensure compatibility, technical functionality, eliminate redundancy, reduce licensing costs and prevent security breaches.
    d. CNS cannot determine if an application meets the educational objectives of a particular curriculum. Instead, the purpose of CNS involvement in the acquisition process is to work with a vendor's technical representatives to ensure that the technical aspects of the product meet the functional needs of faculty and students, and that the application is compatible with DYCnet components.
    e. CNS reserves the right to refuse support and/or connectivity for any component (hardware or software) in the event that coordination with and approval by CNS was not obtained prior to the acquisition.
    f. Running an existing version of an application does not constitute acceptance by CNS to support a newer version of the same application. Application upgrades can be vastly different than their predecessors, creating security risks, additional resource requirements and other complications not known to the average user or purchasing authority. Such upgrades can also cause undo hardship on the CNS support staff and other DYC users.
    g. DYCnet users shall not relocate DYC owned hardware to alternate locations without coordinating with facilities and purchasing to ensure the proper network configuration and maintenance of the college inventory.

7. **Network and Server Planned Maintenance Scheduling:**
    a. DYCnet planned maintenance and installation scheduling shall be coordinated with academic and administrative departments and be communicated as efficiently as possible using combinations of email, phone, memo or web postings as appropriate.
    b. Every effort shall be made by DYC network and server administrators in CNS and other departments to limit network downtime such that interruptions have a minimal effect on DYCnet users.
    c. As a general rule, planned network upgrades and maintenance shall be performed during low utilization periods such as early morning, evenings, weekends, and breaks in the academic calendar. These times are chosen to minimize the affects of the downtime for the greatest number of users. It must be noted that the availability of vendors and the nature of the maintenance or upgrade is also taken into account when planning downtime.

8. **Unplanned DYCnet Downtime & Troubleshooting:**
    a. Occasionally it becomes necessary to perform network configurations and repairs outside of a predetermined maintenance schedule. In these cases, network interruptions may occur during prime network hours. A reasonable effort shall be made by systems and network administrators to minimize interruptions and communicate estimated downtime and its effects to users.
    b. Emergency maintenance and troubleshooting does not make all forms of notification practical in every instance. Users should not expect network downtime notifications to come in the same form every time a notification is "sent". Typical forms of notification may not be reasonable given the nature of the problem (i.e. email or web server down). The following types of notifications may be used: email, web posting, instant messages, phone tree calling, hardcopy notices, and voicemail messaging.
    c. CNS cannot be held responsible for end users not receiving notifications sent out through reasonable means to communicate the DYCnet downtime. Notifications may only reach those who are logged in, or diligent about checking the various communication avenues.
    d. All Server and Network Administrators are required to keep CNS informed of any circumstances that may affect the operational capability of DYCnet or any portion thereof. For example notification must be made if a new host or appliance is to be installed, virus or intrusion found or suspected, or network interruption planned or realized on their assigned servers or networks.

9. **Third Party Network Access:**
    a. DYCnet server and network administrators shall not provide others unauthorized access to DYCnet networks, services or components for their personal favors, financial gain, activism, or illegal activity. Authorized access to internal DYCnet services shall be limited to students, collaborating educators, employees and approved third parties such as contractors and consultants.
    b. CNS is responsible for facilitating all third party network access to DYCnet. This may be done directly by CNS staff or delegated by CNS to DYC representatives such as faculty, staff or consultants.
    c. Third party access includes any person, group, business or entity such as a vendor, contractor, consultant or non-DYC user who gains client level access to an internal server and/or network, whereby the client obtains DYCnet's client IP addressing.

d. Third party access to private DYCnet servers and DYC administrative networks must be agreed to in writing and signed by the vendor as well as a responsible agent of the college due to the legal liabilities in the event of criminal activity. This document shall hold the third party legally responsible for their actions while connecting through DYCnet.

10. **Web Assets, DYC Logos, and Official Web Sites:**
    a. The College's web assets include www.dyc.edu and various other domains and sub-domains, each of which are governed by their respective system administrators and maintained by its owner. The main college website and source of official information is www.dyc.edu, which is maintained by Web Services. While academic and personal sites on College domains are not censored, the college may require those pages to carry a disclaimer that notifies the viewer that the content may not reflect official College viewpoints.
    b. All changes, upgrades, system updates and configurations on servers running the DYC web sites shall be coordinated through the administrator(s)/owner(s) of the respective server(s)/site(s) in advance of the change.
    c. Requests for updates and additions to the official web site are submitted to Web Services via the Help Desk. Material changes to the official website are approved by the Vice President of Enrollment Management.
    d. The digital and identity assets that represent D'Youville College including the college "name," domain names (such as dyc.edu, dyouville.edu, dycchc.com, kavinokytheatre.com and associated sub-domains), logos, trademarks, seals or copyrighted photos and drawings, may not be used without the prior approval of the Office of Public Relations. Unauthorized use of College owned names, domain names, trademarks and logos by third parties implies endorsement by the college for products, services and statements, which the college may not choose to endorse. Therefore, unauthorized use of D'Youville College digital assets in third party web sites, advertising, and commercial or fundraising activities will be treated by the College as a serious matter which may fall under federal copyright laws.
    e. Contracting with third parties for web-related services including (but not limited to) imagery, design, copywriting, development, programming, affiliate advertising, linking and search optimization/ranking shall be reviewed and approved by Web Services. Purchase orders for such services should be forwarded to Web Services for approval.

11. **Workstation Configurations and Installations:**
    a. CNS shall provide DYCnet configuration assistance through written instructions, phone support and hands on support in the CNS Technical Office. CNS Technicians will not make "house calls", but will configure your workstation provided that the workstation is brought in by appointment, and the hardware is in working order. CNS Technicians cannot install system hardware that requires opening up the CPU case since it invalidates the warranty and leaves DYC and the CNS Staff open to liability.
    b. Workstations that do not meet the minimum hardware or software specifications are not authorized to connect to DYCnet. Workstations found on DYCnet without up to date anti-virus or system patches shall be disconnected from the network, pending updates and re-certification by CNS prior to being reconnected to DYCnet.
    c. Requests for CNS Technical Assistance must be made to our CNS Helpdesk.

12. **Software Licensing:**
    a. DYC users must abide by all software licenses, agreements, policies, copyrights and intellectual property rights applicable to local, state, and federal laws.
    b. D'Youville does not allow the unlawful use and/or copying of copyrighted materials in hardcopy or electronic forms.
    c. The capability to access, copy, use or distribute materials does not constitute the right to legally do so if that material is legally protected by license, agreement, law or copyright.
    d. Due to security vulnerabilities, and resource constraints it may become necessary for CNS to limit the use of some software or services.

13. **Sexually explicit materials:**
    a. Monitoring of network usage is done in general terms for the purpose of determining protocol utilization, web site hit counts, caching requirements, authentication failures, and application usage. These statistics are used to justify changes in network and server configurations. If through the course of network troubleshooting illegal activity is discovered, DYC is required by law to turn over any evidence related to illegal activities when requested by local, state and federal authorities.
    b. The viewing, storage and/or trafficking in child pornography is categorically forbidden at D'Youville College. Violations of this are clearly outlined in local, state and federal laws, and shall be prosecuted to the fullest.
    c. In general, the viewing of sexually explicit materials on college owned workstations by employees is not condoned at D'Youville. Exceptions to this policy shall be granted by the Vice President for Academic Affairs; for academic purposes only. Employees in violation of this policy shall be subject to disciplinary action up to and including termination.

14. **DYCnet Network Access:**
    a. Direct DYCnet access constitutes the cabled connection of workstations in the Labs, Library, Classrooms, Offices or Dorms
    b. Remote access constitutes the access to DYCnet from a remote location off campus workstation. Remote access credentials by authorized DYC users shall not be shared with unauthorized users.
    c. Wireless access constitutes connections to DYCnet through wireless access points provided at various locations on campus. Wireless Computing is a component of DYC's Network Infrastructure and is, therefore, managed and operated by CNS. Wireless access points may not be connected to office, dorm or classroom data drops without the involvement and consent of CNS.
    d. IP Addressing and Domain Name Services (DNS) have a profound impact on the function of all network resources; therefore, CNS shall tightly control these services. Unauthorized name resolution, addressing services and protocols shall be removed from the DYCnet.
    e. Individual users shall not use their network access in dorms, classrooms or offices as a means to create bridges, or private networks for others either within DYC or external to the DYC community without prior permission from CNS.

15. **Account Administration:**
    a. The routine creation or deletion of DYCnet student accounts is performed by the CNS

Server Administrator, based on automated requests generated from the NIAS student records system.

b. Time sensitive requests to create, disable, delete or modify accounts will be performed based on directives from the Personnel Office, the President's Office or the V.P. of Operations directly to the DYCnet System Administrator.
c. Only one unique user is authorized logon access through a single user account. Group accounts shall be used for assigning system resource access rights rather than logon access.
d. Group mailboxes shall be shared by members of a group or office, as directed by the "owner" of the group mailbox, usually a department head, director or chairperson.
e. Accounts which remain inactive for a prolonged period, as determined by the system administrator, shall be disabled and moved to a temporary stale accounts holding area. Stale accounts that remain unused for an additional 30 days shall be deleted.
f. It is the responsibility of the account/mailbox owner to notify the system administrator in the event that their account or mailbox becomes disabled, full or inaccessible.
g. Graduating students and students who leave the college shall have their accounts deleted 30 days after they are marked for deletion by the NIAS student records system. This is sufficient time for students to transfer or copy any of their school related material from their home directories.
h. Faculty and staff accounts with home directories (H:\) over the maximum storage quota will be evaluated for additional storage on a case-by-case basis. Students will be required to store their data on removable storage media such as CDs, floppies or USB drives at their own expense, risk and discretion.
i. Although the system administrators do everything possible to preserve data files, ultimate responsibility for preserving user files lies with the end user.

16. **Email:**
    a. Email should not be considered as private and should not contain sensitive or confidential data.
    b. D'Youville College employees are required to check their *username*@dyc.edu email on a regular basis as they do their interoffice mail, and maintain their mailbox folders appropriately to prevent their mailbox from filling up. If they are unfamiliar with using the email system it is the user's responsibility to obtain email training to improve their skills.
    c. Full employee mailboxes shall be reported to by the system administrator to the Personnel Department for written notification to be sent to the end user. The mailbox owner must contact CNS within 30 days for assistance in cleaning up the mailbox, otherwise the account/mailbox shall be deleted.
    d. D'Youville and CNS shall not be held responsible for the academic or financial consequence of missed communications due to email forwarding errors such as incorrectly typed forwarding email addresses, message size refusal or email domain resolution issues of the non-DYC email provider.

17. **SPAM:**
    a. SPAM is the excessive sending of large, malicious or unwanted emails, to include virus hoax messages and chain letters. DYCnet users are not authorized to send SPAM inside or outside of the college.
    b. SPAM or junk email sent or received by DYCnet is filtered at the perimeter of the

network based on virus related signatures, a limited list of subject line key words, and heuristics.

c. SPAM filtering shall be done in a layered approach. CNS reserves the right to filter excessive SPAM emails based on domain, IP or unique subject line to prevent the excessive consumption of server resources.
d. Users are free to filter SPAM at the client workstation level, based on the capabilities of local software and personal preferences.
e. DYC users who wish to send email to large distribution groups within the DYC community (all faculty, staff, employees, or students) should send their email to the DLManager. The DLManager will review the email contents for suitability and forward the email to the desired campus distribution list. This ensures that virus or SPAM emails do not take advantage of our email system, and that the contents of the email and recipient community are suitable.

18. **Anti-virus:**
    a. It is the responsibility of all DYCnet workstation, server and network administrators to ensure that the servers and workstations on their associated networks are running up to date anti-virus with auto-protect and auto-update features enabled.
    b. All workstations attached to DYCnet are required to run up to date Anti-virus. This includes College owned workstations as well as privately workstations directly or remotely attached to DYCnet.
    c. CNS is responsible for centrally managing or delegating the management of Anti-virus Services for employee workstations on College owned desktops and servers campus wide.
    d. The academic lab and library technicians are responsible for ensuring that the local anti-virus clients on their lab workstations remain up to date to protect those workstations and the network to which they are attached against attacks.

19. **Security:**
    a. Network monitoring, packet sniffing, port scanning and password cracking are prohibited on or through DYCnet without the permission of the DYC Network Administrator, since these activities consume excessive amounts of resources are potentially harmful to the security of the network, and may violate usage guidelines we have in place with our Internet Service Providers (ISPs).
    b. Running password cracking software anywhere on the network is a serious violation in computing policy, regardless of who is performing the scan. Anyone (including DYC technical staff) attempting password cracks must get the written permission of the associated system and network administrators prior to the scanning, since such a violation can result in the termination of employment or in the case of students, removal from school.
    c. It is the responsibility of the system and network administrators to review logs, services, filters and protocols as necessary to ensure that servers and network appliances are up to date, patched and non-essential services and protocols turned off.

20. **DO's for DYCnet use:**
    a. Check your dyc.edu email on a regular basis and delete old emails so that they will not count against your mailbox quota.

b. Check email public folders for subject related announcements.
c. Check the www.dyc.edu web site for announcements, scheduling, alerts, downloads and system updates.
d. Check your workstation for current system patches, spy ware and anti-virus updates at least once a week.
e. Use a personal firewall if running your workstation on an open network such as in the dorms or wirelessly.
f. Contact the Academic Lab or CNS Helpdesk if you are having difficulty with your account or mailbox.
g. Contact the Academic Lab or Library if you are experiencing difficulty in accessing network resources like printers, library resources, and academic applications.
h. Logout of your workstation when you are finished using it.
i. Change your account password frequently.

21. **Don’ts for DYCnet use:**
    a. Don’t copy material protected by privacy act.
    b. Don’t export restricted software or encryption standards.
    c. Don’t create an easy to guess password, share it or write it down.
    d. Don’t let your mailbox fill up.
    e. Don’t leave workstation logged in and unattended, or assume a logged in session that is not your own.
    f. Don’t abuse server or network resources such as throughput, storage, printing and email.
    g. The ability to access files, data, and other network resources doesn’t imply the right to do so legally or ethically.
    h. Don’t install or use P2P file sharing software such as Kazaa, Limeware or Gnutella unless you are aware of the consequences and know how to limit the exposure of your system on the Internet.
    i. Don’t willfully propagate malicious code, viruses or SPAM
    j. Don’t remove anti-virus protection from your workstation or attach unprotected laptops or workstations to the network.
    k. Don’t install or run rogue appliances, or services on DYCnet.
    l. Don’t use DYCnet resources for financial gain, activism or any other non-business related function without permission.