Computing Services Account Application
College of Engineering; University of Delaware

The units provide various computing services, web publishing, and general purpose computing. To access these services complete this form and return it to staff within your unit who handle account creation.

Instructions:
(a) Carefully read "The Policy for Responsible Computing" provided on this application.
(b) Carefully read the University’s “Code of the Web” policies at http://www.udel.edu/codeoftheweb.
(c) Sign and date the acknowledgment section, which indicates you will abide by the policies you just read.
(d) Provide all applicable information where indicated.
(e) Obtain authorization. Students obtain authorization from their faculty advisors. Staff obtain authorization from department chairs, directors or managers. Visitors and guests obtain authorization from sponsoring faculty. A valid authorizing signature must be provided where indicated.

User names: Your UDELnet username will be used where possible. Otherwise your user name will be your last name (truncated to eight characters). If that name is already in use, then the initials from your first and middle name are appended to the first six characters of your last name (e.g. John Michael Doe's user name would be doejm).

Passwords: Your initial password is randomly set and only provides access to allow you to change your password. Your initial password will be placed in your office mailbox. Otherwise, see staff in your unit who handle account creation to get your initial password.

To set a permanent password for general purpose UNIX account visit:
CCMT  https://www.ccm.udel.edu/network
ChEG:  https://www.che.udel.edu/network
MEEG:  https://www.me.udel.edu/network
MSEG:  https://www.mseg.udel.edu/network

To set a permanent password for WWW site management accounts visit:
https://www.engr.udel.edu/network

To set a permanent password for WINDOWS domain account:
You will be prompted for the new password during first login.

Records: Detach this cover page and keep for your records. Please make a copy of the completed form if you'd like to retain for your records. The original copy of this form will be maintained with your personnel records.

December 6, 2007
Name (print):

last name  first name  middle name

Advisor: ___________________________  Department: ___________________________

Graduation Year: ________________  UDELnet Username: ________________________

Office: ___________________________  UD phone: ___________________________

Classification: ( ) Faculty  ( ) Adjunct Faculty  ( ) Professional  ( ) Staff  ( ) Post Doctorate  
( ) Graduate  ( ) Undergraduate  ( ) Visiting Faculty  ( ) Visiting Professional  ( ) Guest  
( ) Other, please specify: _______________________________________________________

Specify the SERVICE you are requesting access to:  
( ) WWW content management  ( ) General Purpose Unix  ( ) Windows Domain Account  
( ) Shrek Database  ( ) Other: ____________________________________________________________

Specify the UNIT you are requesting an account for, and obtain the necessary authorizing signature(s).  
( ) CCMT  ( ) ChEG  ( ) CIEG  ( ) ENGR  ( ) MEEG  ( ) MSEG

Account authorized by: 
Advisor, Department Chair, Manager, or Director, or sponsoring faculty signature

For CCM

Dr. John W. Gillespie, Director, Center for Composite Materials

Applicant's acknowledgment: I acknowledge I read and understand the "Policy for Responsible Computing at the University of Delaware" and the UD “Code of the Web”, and I will comply with all applicable policies.

Applicant's signature _______________________  Date _______________________

Policy for Responsible Computing at the University of Delaware


PREAMBLE

In keeping with the University’s commitment to preserve and protect academic freedom and to promote the free exchange of ideas in an open collegial community, the University respects the reasonable privacy expectations of its employees and students in all communications by mail, telephone, and other electronic means, subject only to applicable state and federal laws, University policies and regulations, and system maintenance requirements.

Access to computing and information resources is provided for students, faculty and staff within institutional priorities and financial capabilities. The Policy for Responsible Computing at the University of Delaware contains the governing philosophy for regulating faculty, student, and staff use of the University's computing resources. It spells out the general principles regarding appropriate use of equipment, software, and networks. By adopting this policy, the Faculty Senate recognizes that all members of the University are also bound by local, state, and federal laws relating to copyrights, security, and other statutes regarding electronic media. The policy also recognizes the responsibility of faculty and system administrators to take a leadership role in implementing the policy and assuring that the University community honors the policy.

CONTINUED on following pages.
POLICY

A. There are circumstances under which the University may have a legitimate need to read private computer data, including e-mail records or to monitor electronic transmissions. These circumstances include, (1) compliance with legal obligations in judicial proceedings; (2) requests from civil or law enforcement authorities; (3) IT system administration and maintenance, and (4) investigation of suspected violations of University policy. In such circumstances, the University will endeavor to provide fair notice of monitoring or inspection to affected employees consistent with the University's legal obligations and the goals of the investigation.

B. The University will not engage in random monitoring of written or electronic communications.

C. The following framework will apply whenever the University has a need to read private computer data, including e-mail records or to monitor electronic transmissions.

1. Necessary Action - Exceptions to the policy may be authorized only when reasonably necessary to protect the security of the University, its communications system and the academic process, and when there is good reason to believe that the individual employee or student has violated law or University regulations. For example, claims of sexual harassment where the accused may delete/erase e-mails exposing the University to adverse claims; claims of child pornography; reason to believe that a specific user is endangering the technical integrity of the University system, etc.

2. Consultation and Authorization - Exceptions to the policy may only be invoked by persons with responsibility and authority for administering the law or regulations within the University (e.g., University police, computer security officials) and only after consultation with the Provost and/or the Vice President for Administration.

3. Accountability - Normally in applying any exception to the policy, the affected individual shall be notified in advance unless conditions necessitate immediate access or notification would compromise an ongoing criminal or University investigation. Records of any exception must be kept; the records should be made accessible to the affected individual, unless such access would compromise an ongoing criminal or University investigation. Information collected must be kept secure and be used only for the intended purpose. A report will be made annually to the Faculty Senate, which will include the number of exceptions during the reporting period and the general nature of the reasons for the exceptions.

D. All members of the University community who use the University's computing and information resources must act responsibly. Every user is responsible for the integrity of these resources. All users of University-owned or University-leased computing systems must respect the rights of other computing users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements, and use any electronically transmitted information within the "Fair Use" guidelines or with the permission of the author. It is the policy of the University of Delaware that all members of its community act in accordance with these responsibilities, relevant laws and contractual obligations, and the highest standard of ethics.

E. Access to the University's computing facilities is a privilege granted to University students, faculty, and staff. Access to University information resources may be granted by the owners of that information based on the owner's judgment of the following factors: relevant laws and contractual obligations, the requestor's need to know, the information's sensitivity, and the risk of damage to or loss by the University.

F. The University reserves the right to limit, restrict, or extend computing privileges and access to its information resources. Data owners—whether departments, units, faculty, students, or staff—may allow individuals other than University faculty, staff, and students access to information for which they are responsible, so long as such access does not violate any license or contractual agreement; University policy; or any federal, state, county, or local law or ordinance.

G. University computing facilities and accounts are to be used for the University-related activities for which they are assigned. University computing resources are not to be used for commercial purposes or non-University-related activities without written authorization from the University. In these cases, the University will require payment of appropriate fees. The State-created University Charter prohibits the Management of the University to benefit any party, sect, or denomination. Employees may choose to participate in any of the above activities but cannot use University resources to support their personal activities. This policy applies equally to all University-owned or University-leased computers.
H. Users and system administrators must all guard against abuses that disrupt or threaten the viability of all systems, including those at the University and those on networks to which the University's systems are connected. Access to information resources without proper authorization from the data owner, unauthorized use of University computing facilities, and intentional corruption or misuse of information resources are direct violations of the University's standards for conduct as outlined in the University of Delaware Policy Manual, the Personnel Policies and Procedures for Professional and Salaried Staff, the Faculty Handbook, University collective bargaining agreements, and the Student Guide to University Policies and may also be considered civil or criminal offenses.

I. Implementation

Appropriate University administrators should adopt guidelines for the implementation of this policy within each unit and regularly revise these guidelines as circumstances, including--but not limited to--changes in technology, warrant. The Vice President for Information Technologies shall, from time to time, issue recommended guidelines to assist departments and units with this effort.

J. Enforcement

Alleged violations of this policy shall be processed according to the judicial processes outlined in the University of Delaware Policy Manual, the Personnel Policies and Procedures for Professional and Salaried Staff, the Faculty Handbook, University collective bargaining agreements, and the Student Guide to University Policies. The University of Delaware treats access and use violations of computing facilities, equipment, software, information resources, networks, or privileges seriously and may also prosecute abuse under Title 11, 931-941 of the Delaware Code, the Computer Fraud and Abuse Act of 1986, or other appropriate laws.