Information Security Policy

April 6, 2010

1. Introduction

The purpose of this Security Policy is to establish direction and requirements to ensure that the appropriate steps and precautions are followed when access is granted to Dominican University (DU) computer systems and networks.

This Security Policy applies to all employees (staff, faculty, and students), contractors, consultants, temporaries, transitioned, and other personnel at DU, including personnel affiliated with third parties that access DU's computer systems and networks. This policy also applies to all computer and data communication systems owned by and/or administered by DU.

The intention of this policy is to specify DU's commitment to the protection of data and information resources. All university information is a "University Asset" and is to be protected appropriately. Inappropriate use exposes DU to risks including virus attacks, compromise of computers, network and communication systems and services, and legal liability.

Access to data, computer, network and communication systems is granted on a need-to-know basis. Only people who have a requirement for information are granted access to it. The level of access is determined by the function that is being performed. Access to information is not granted without business justification.

All electronic and telephonic records are considered university records and should be transmitted only to individuals who have a business need to receive them. All messages created, sent or retrieved electronically or through the voice mail system are the property of the university, and are subject to review.

The IT Department will have the ability to monitor any DU system, platform or network to ensure compliance with all university policies. In the event of suspected or reported abuse, IT will initiate the appropriate steps to monitor such activity.

The Security Policy will be enforced. Security violations may result in disciplinary action being taken, up to and including termination. If activities that violate criminal statutes are involved, criminal penalties may be sought.

2. General PC Usage and Password Management

The policy is to establish direction and requirements to ensure that the appropriate steps and precautions are followed when managing passwords for access to DU systems. Each employee will be assigned a unique user account/ID. Employees are responsible for all data processed under their account. Passwords are an important aspect of security, as they are the front line protection for user accounts. A poorly chosen password may result in compromise or risk to university data, computer, network or communication systems.

YOU are responsible for all data processed under your login ID and Password!

Passwords should **NEVER** be shared with another individual, including co-workers or supervisors/managers.

- Employees should not post password(s) where others can view them.
- Employees should not store passwords in a file on any DU system.
- Passwords must not be inserted in e-mail messages or other forms of electronic communications.
- Employees should immediately change passwords at any time they suspect it has been compromised and report the incident to IT.
- Do not use the same password for DU computer, network or communication systems that is used for non-university accounts (personal e-mail, web sites, etc.).
- All employees must change their passwords, on the DU network, at least once every 90 days.
- Passwords must be a minimum of 8 characters and can not contain any part of the User ID.
- Passwords must meet 3 of the following 4 complexity requirements:
    1. Upper Case, A….Z
    2. Lower case, a…z
    3. Base 10 digits, 0…9
    4. Non-alphanumeric, !,$,#,%
- When selecting password(s), employees must choose something not easily recognized. Do not use names such as: pets, nicknames, family members, meaningful places, or significant dates, etc. Do not choose consecutive word or number patterns such as aaabbb, 123321, etc.
- Avoid constructing fixed passwords by combining a set of characters that do not change with a set of characters that predictably change (e.g. abcjan, abcfeb).
- The initial password, set by IT, will be valid only for the first initial log in. At that time, you will be forced to choose another password before access will be granted to the system or network.
- Do not use the 'remember password' feature of applications that require authentication.
- Boot up protection passwords are not permitted on DU equipment.

Password resets will ONLY be performed for the employee's own Login Account that has been specifically assigned to him/her. For example, resets will not be completed if requested by one individual on behalf of another employee. This restriction also includes supervisors/managers that may request password information for individuals within their organization.

When leaving a workstation, logout/logoff or lock the PC.

Configure your computer to use automatic screen saver desktop locking. The default locking time should be set to no more than 5 minutes.

(Right click on the desktop area, choose Properties, Screen Saver, and click Password protected.)

3. Termination Process

At the time of termination, all university provided equipment must be returned to the university. If the equipment is not returned, the cost of the equipment may be deducted from the employee's final compensation payment. In addition, if the computer equipment is lost, stolen or damaged, the employee may be responsible for replacement cost of the unit.

Immediately upon notification of an employee or contractor leaving the university, for any reason, all user accounts will be disabled. IT will follow up with the manager to reclaim all assigned computer equipment so that it can be reconfigured and re-deployed.

4. Laptops

Laptop computers and other portable equipment are both valuable and portable, thus a prime target for theft. These resources are provided to employees to assist in performing their jobs more effectively. The use of a laptop has nothing to do with status or position. Business justification must be provided and will be based on travel, or remote access requirements.

Employees are responsible for any assigned equipment and are expected to secure this equipment at all times. Below are guidelines to minimize portable equipment theft or damage:

- Keep your portable equipment with you at all times when traveling.
- Portable equipment must not be left in privately owned, rented or university vehicles.
- Portable equipment must be taken home when the employee leaves the office or secured in a locked drawer or cabinet.

Employees in the possession of laptops, and other transportable computers containing sensitive DU information must not check these computers in airline luggage systems. To avoid damage and theft, these computers must remain in the possession of the traveler as hand luggage.

If equipment is lost or stolen, the assigned employee could be held responsible for replacement.

5. Personal Computer Software

DU licenses the use of computer software from a variety of outside companies. DU does not own this software or its related documentation and unless authorized by the software developer, does not have the right to reproduce it except for backup purposes.

With regard to Client/Server and network applications, DU employees shall use the software only in accordance with the license agreements.

DU employees shall not download or upload unauthorized software over the Internet.

DU employees learning of any misuse of software or related documentation within the University shall notify the department manager or IT.

According to applicable copyright law, persons involved in the illegal reproduction of software can be subject to civil damages and criminal penalties including fines and imprisonment. DU does not condone the illegal duplication of software. DU employees who make, acquire, or use unauthorized copies of computer software shall be disciplined as appropriate under the circumstances. Such discipline may include termination.

Any doubts concerning whether any employee may copy or use a given software program should be raised with IT before proceeding.

Removal or Disabling of Software – In order to protect and secure the DU computing environment, IT requires the installation and execution of certain types of software on its servers, network elements, and end-user PCs. This software includes, but is not limited to, computer virus protection software and software used to detect illegal and/or inappropriate files and computer programs. Any employee who removes, disables, or otherwise prevents the execution of this type of software without prior written consent from IT will be considered in violation of this policy and subject to disciplinary action.

Security or Privacy Invasion Software - Some software is developed to break system security and invade privacy. Such software does not play a role at DU for any reason. Installation and/or use of these types of software packages is strictly prohibited.

Right to Audit - DU has the right to audit all resources to ensure compliance with the DU Software Policy and may permit the software licensors and their agents to audit some or all resources to ascertain compliance with their license, purchase, or other applicable agreements.

6. Remote Access Policy

Remote access to all DU's university resources is to be used for business purposes only. Sensitive (confidential or secret) DU information must not be read, discussed, or otherwise exposed on airplanes, restaurants, public transportation, or in other public places.

Employees attending to DU business at alternative work sites should use only DU provided computer software, hardware, and network equipment. Similarly, **employees SHOULD NOT bring their own computers into the office** to process or otherwise handle DU information without prior approval from the IT Department.

The standard DU virtual private network (VPN) solution will be used when accessing internal DU systems over broadband (DSL, Cable Modem, etc.).

Remote access is not a university standard and employees will not be granted remote access without the appropriate business justification and approvals. DSL/Cable modems must be used in conjunction with a firewall and a virtual private network (VPN) connection on the involved computers. It is prohibited to access any DU university resource using unsecured wireless communication mechanisms.

Employees must not leave personal computers unattended with a VPN connection activated. Leaving a computer active in this fashion could allow unauthorized persons to gain access to the involved system and connected network(s).

7. Remote Access from a Home Computer

Remote access via a Home computer will only be granted to those providing a strong business case and receiving management approval. Access from a home computer will only be via the supported virtual private network (VPN) product. This requires the employee to have an internet connection established prior to initiating the VPN connection. The internet connection can be over DSL, Cable modem, or other broadband method. It is prohibited to access any DU university resource using unsecured wireless communication mechanisms. If a wireless network is involved, it must support

and be utilizing WPA with at least 128 bit hexadecimal encryption. The home computer is required to have Firewall and Anti-Virus software employed.

DISCLAIMER: Due to the fact that most home PC configurations are unique, the IT Department does not know in advance what software or hardware on an individual's PC that may be affected by the installation of software from Dominican University. Therefore, any software product installed or configured on an employee's home PC via the Home PC documentation is **NOT** supported by DU's IT resources. This includes any system files, application files, or drivers that are modified during installations.

8. Email Usage Policy

All electronic records are considered university records and will be transmitted only to individuals who have a business need to receive them. All messages created, sent or retrieved electronically are the property of DU.

- Treat Electronic Mail as Public Communications: Employees must consider electronic mail to be the equivalent of an electronic postcard. Unless the content is encrypted, employees must refrain from sending credit card numbers, passwords, or other university sensitive data via electronic mail.

- Message Content Restrictions: Employees are prohibited from sending or forwarding any messages via DU's systems that a reasonable person would consider to be defamatory, harassing, or explicitly sexual. Employees are also prohibited from sending or forwarding messages that would be likely to offend on the basis of race, gender, national origin, sexual orientation, religion, political beliefs, or disability. Profanity, obscenities or derogatory remarks should not be used. Such remarks, even when made in jest, may create legal problems such as trade libel and defamation of character. Special caution is warranted because backup and archival copies of electronic mail may actually be more permanent and more readily accessible than traditional paper communications.

- Notification of Content Monitoring for Mail Transmissions: DU may employ automatic content scanning tools to identify select keywords, file types, or other information for security purposes. The IT Department will periodically conduct content monitoring.

- Certain Inbound Attachments Prohibited*:* Executable and EML attachments on inbound Internet electronic mail messages sent to DU employees will be automatically deleted. If a formatted file, an executable program, or other non-text message must be sent, the sender must utilize other methods approved by IT.

- Personal Use of Electronic Mail Systems: The DU electronic mail systems are primarily intended for business purposes. Any personal use must not interfere with normal business activities, must not involve solicitation, must not be associated with any for-profit outside business activity, and must not potentially embarrass DU.

- Subscriptions: Employees should subscribe only to business-related user groups or distribution lists.

- Using a Mail Account Assigned to Another Individual: Employees must not use an electronic mail account assigned to another employee to either send or receive messages. If there is a business requirement to read another's mail, while the employee is away on vacation for instance, message forwarding must be used.

- Reporting Offensive Electronic Mail Messages: Employees are encouraged to communicate directly to IT or Human Resources, instances of offensive electronic mail messages.

9. Internet Access Policy

DU computer, network and communication systems will be used for business or academic purposes only. Use of DU's information systems to access the Internet for personal gain or profit is unacceptable and may be considered cause for disciplinary action up to and including termination.

All users of the Internet should be aware that firewalls can create a detailed audit log reflecting transmissions of both in-bound and out-bound traffic. DU reserves the right to disclose any transaction log records to law enforcement, government officials, or to other third parties without notification to or permission from an employee. DU routinely logs web sites visited, files downloaded, time spent on the Internet, and related information.

Information on the DU Intranet may be disseminated only to authorized persons. Employees cannot forward information appearing on the Intranet to third parties without the express authorization of the Intranet site owner and IT. Employees will not publicly disclose internal DU information via the Internet that may adversely affect customer relations, or public image.

Using computers attached to DU's systems or networks to access the Internet is permissible only when users go through a DU firewall. Other ways to access the Internet, such as dial-up connections with an Internet Service Provider (ISP), are prohibited.

Virus screening software must be installed and enabled on all DU computer systems.

Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or any DU electronic communications system is prohibited. The employee's name, electronic mail address, organizational affiliation, and related information included with messages or postings will reflect the actual originator of the messages or postings. Use of anonymous FTP log-ins, anonymous UUCP log-ins, HTTP (web) browsing, and other access methods established with the expectation of anonymity, is prohibited.

Copyrights*:* Dominican University (DU) strongly supports strict adherence to software vendors' license agreements. When DU computers or network resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. Likewise, off-hours participation in pirate software bulletin boards and similar activities represents conflict of interest with DU work, and is therefore prohibited. Reproduction, forwarding, or in any other way republishing or redistributing words, graphics, or other materials must be done only with the permission of the author/owner. Employees should assume that all materials on the Internet are copyrighted unless specific notice states otherwise. When information from the Internet is integrated into internal reports or used for other purposes, all material will include labels such as "copyright, all rights reserved" as well as specifics about the source of the information (author names, URL, dates, etc.).

Examining Records: At any time and without prior notice, DU management reserves the right to examine electronic mail messages, electronic files on personal computers, web browser cache files, web browser bookmarks, logs of web sites visited, and other information stored on or passed through DU computers or systems. Such management access assures compliance with internal

policies, assists with internal investigations, and assists with the management of DU information systems.

10. Administrative Access Rights

Administrative rights, both domain and local, will be strictly monitored. Domain rights will be granted by department need. Local administrative rights will not be granted without business justification, manager approval, and IT approval. The most common request for Admin rights is related to software installs. DU strictly adheres to software license agreements and monitors software running on all DU computer systems. In general, the IT Group should be the only ones performing software installations.

Please see section 5 for more details regarding Personal Computer Software.

DU IT reserves the right to access, both physically and remotely, all DU computer equipment for support and administrative purposes. With the exception of normal password protection, any employee who tampers with their DU computer in such a way as to prevent the IT Department from gaining this access, including but not limited to removal of Domain Administrator Rights from the PC, will be considered in violation of this policy and subject to disciplinary action.

11. Computer Network Integrity Policy - Disruption of Service

The DU computing network consists of Local Area (LAN) and Wide Area (WAN) Network segments between buildings on the Main Campus and to the Priory Campus. This network depends on many services and network devices to perform its function effectively. Adding, changing, or deleting/removing any of its dependent services or devices can cause disruption of service on the network. These services/devices may be workstations, printers, terminal servers, routers, switches, hubs, network cabling, or any other network appliance. In a complex network with many hosts, services, and network devices, it is often difficult to ascertain what impact a disruption of service may have on the network or its users. Therefore, any disruption of service of any networked device is expressly prohibited.

The following list is a sample of situations that could cause disruption of the DU computing network. If you are uncertain or not sure if your actions will cause a disruption to the network, please contact IT for clarification. Assumptions, for all intents and purposes, that result in disruption to the DU computing network will be considered a violation of this policy.

- Introducing a new server to the network. This includes installation of any server operating system.
- Introducing a new router, switch, hub, or any other network or IP addressable device to the network.
- Unplugging the network connection for a server, printer, or any other network device.
- Rebooting a server, printer, or any other network device.
- Attempting to remotely reboot a server, printer, or any other network device.

Change Requests

Any additions, changes, or deletions/removal of workstations, printers, terminal servers, switches, hubs, routers, network cabling, or any other network appliances that have connections to the DU computing network must be coordinated and approved by IT .

Disciplinary Action

Any employee who violates the policies of this section may be subject to revocation of their computer account, suspension, and/or termination of employment.

Right to audit

DU has the right to audit all resources connected to the computing network to ensure compliance with this policy.

12. Non-adherence of Security Policy

Dominican University (DU) computer, network and communication systems must be used for business or academic purposes only. If abuse of DU computer, network and communication systems is suspected, any manager, in an employee's management chain, may request a review of an employee's system usage. Actions that violate this security policy may subject the data and other assets of the university to exposure or damage.

Security violations or abuse include, but are not limited to, the following:

- Failure to logoff/lock a desktop/laptop when an employee is not in control of it.
- Using or obtaining access to another employee's Login Profile other than your own.
- Sharing a Login Profile password with another employee.
- Granting access to university data to any employee without written authorization.
- Examining or altering university data without appropriate access or authorization.
- Processing any financial or maintenance transactions for personal gain or related accounts.
- Processing any financial or maintenance transactions for the purpose of sharing with immediate family relations for personal gain.
- Installing non-approved software or hardware on desktops, laptops, systems or network.
- Any attempt to compromise internal or external computer or network systems.
- Failure to report potential or actual information concerning security violations, risks, or exposures.
- Surfing Internet web sites that could be considered offensive to other employees.

EXPECTATIONS for all DU Employees:

- ✓ Read and understand the University Information Security Policy.
- ✓ Use only university-licensed and approved software. It is against the law to make unauthorized copies and against university policy to install unapproved software.
- ✓ All hardware and software should be requested and purchased through IT through e-mail or by calling the IT HelpDesk at 708-524-6888.
- ✓ Use a computer for business purposes only. DU is not responsible for any personal data or software stored on a PC or the network.
- ✓ NEVER share your password with anyone, including co-workers or supervisors/managers.
- ✓ Do NOT post passwords where others can view them.
- ✓ Request all access to university resources via the IT HelpDesk through e-mail or by calling 708-524-6888.

The Security Policy will be enforced. Security violations may result in disciplinary action being taken, up to and including termination. If activities that violate criminal statutes are involved, criminal penalties may be sought.