

Minimum Information Security Environment Policy

POLICY:

The College has both the right and the obligation to manage, protect, secure, and control the electronic information resources of the College.

Rationale:

The Directory of Information Technology, as Chief Information Officer, is responsible for ensuring that Darton College has adequate information security in order for system and data to be available for appropriate purposes. The basic standards and guidelines described in this policy provide for the minimum acceptable environment for operating and accessing information systems.

Standards & Procedures:

Standards:

Authorized Access to Information Systems (Accounts). Authorized access to the College's information systems is the granting of authority to approach, enter, make use of, and exit the College's information systems. Access is accomplished via an account, which is a record kept by operating systems for each authorized user of information systems for the purpose of identification, administration and security. Users are required to obtain proper authorization prior to accessing the College's information systems.

Guidelines establishing eligibility to receive authorized access:

- a) Every College employee or student eligible to register may be granted access to College information systems.
- b) Users shall not be granted access in excess of the level required to perform their job responsibilities
- c) Individuals providing services to the College may with appropriate authorization be granted access to College information systems
- d) Users shall not misrepresent their identity or relationship to the College when accessing the information systems
- e) Users shall not access information systems that they are not authorized to access

Configuration for Network Connection. Configuration refers to the version of operating system that is installed on your workstation, desktop or laptop computer. As each operating system version may handle other applications in a different manner, users must ensure that they check the current procedure for securing each device to determine the correct accompanying versions of Microsoft Servers, Exchange, AntiVirus and VPN client needed for access to the Darton Network. Users should be aware that a local decision to continue use of a non-supported version of operating system could result in denial of network connection due to increased risk of new security holes that will not be addressed by the software vendor.

Passwords and Userids (Authentication Methods). A userid and password is one method (and the one most commonly recognized by the average user) of authentication. A userid is the name by which the person is known and addressed on the College's information systems. The password – used in conjunction with the userid – is a unique string of characters that a user enters as an identification code. Users must follow standards for creating passwords as defined in the "Create or Change a Password" document (see link in **Procedures** section). Other recognized forms of authentication include, but are not limited to, smart cards, swipe cards, one-time passwords, digital signatures, and/or digital keys and biometrics. Users must have a valid method of authentication before they will be authorized to access the information systems.

Guidelines regarding the use of userids and passwords:

- a) Users must not use accounts or passwords that they have not been authorized to use, or have not been assigned to them
- b) Users shall not give passwords to unauthorized users
- c) Users shall not share userids and passwords
- d) Users must effectively control the creation, use and maintenance of passwords in order to prevent unauthorized access and destruction, modification or deletion of sensitive data
- e) Users are responsible for securing their passwords from inadvertent disclosure
- f) Users are responsible for any activity carried out under their account identification.

Software Licensing. Valid licenses are required for each end user for all commercially developed software operating on systems used by that user. Responsibility for centrally managed and distributed software lies with OIT. Departments are responsible for approving and retaining documentation on software (other than centrally managed) installed on devices within their areas of responsibility. As a minimum departments should be able to show original licensing materials (packaging, hologram software seal, authorization codes, etc.), date of installation and serial number of equipment (or Darton Inventory number) that the software was installed on. Departments are responsible for developing and managing their own procedures for collecting and maintaining licensing records. All students and personnel shall abide by software copyright laws and shall not obtain, install, replicate, or use software except as permitted by the software licensing agreements.

Using Personally Owned Software. To protect the integrity of the College information resources, students and personnel shall not use personally owned software on College owned equipment. This includes purchased and licensed applications; shareware; freeware; downloads from bulletin boards, Internet, Intranet, FTP sites, local area networks (LANs) or wide area networks (WANs); and other personally-owned or controlled software (unless otherwise authorized by the Chief Information Officer or his / her designees).

Physical Security. Physical security refers to the protection from harm or loss of the pieces of equipment that constitute an information system environment or personal computing device. Information system must be safeguarded in a way that minimizes the risk of abuse, theft and destruction.

Guidelines regarding physical security:

- a) Users must implement appropriate protection measures including physical barriers, environmental detection and protection, insurance, and/or other risk management techniques.
- b) Users must not leave mobile computer systems unattended for extended periods of time and shall utilize locking devices responsibly
- c) Users shall protect information systems by utilizing protective measures such as locked screens and password-protected screen savers.

Securing College Information Systems. Securing systems refers to the protection of a computer system and its data from harm or loss, particularly the prevention of access by unauthorized individuals. Users are responsible for properly securing their information systems.

Guidelines for securing systems:

- a) Users shall not knowingly defeat or attempt to defeat the security of information systems
- b) Users must take reasonable precautions in ensuring that they do not disseminate viruses and malicious programs to other users
- c) Users must configure College mail servers to prevent them from being used as third party mail relays
- d) Users are responsible for monitoring the security of their own information systems
- e) Users who are permitted to provide network or computer based services are required to take reasonable precautions to ensure that information systems being used for this purpose are not compromised or used by unauthorized users. See [Sensitive Information Protection Policy](#) for guidelines.

Chief Information Officer (CIO). The Chief Information Officer (CIO), Director for Information Technology, has responsibility for developing and publicizing College information security policies as well as monitoring compliance with those policies and all applicable laws, rules and regulations. The CIO coordinates the standards, procedures and guidelines necessary to administer access to College information resources. The CIO works in conjunction with information resource owners, the College Data Administrators, and functional users to develop this material.

Procedures:

Create or Change a Password
Request Access to College Restricted Data
Secure Your Workstation – In development for web

Create or Change a Password

Guidelines for choosing strong passwords, instructions for changing passwords (Windows Workstations and MyDC Accounts), installing a screen password, and requesting a password reset.

About:

A password is your system's - and the College network's - security. As well as protecting your own system, securing your personal computer from outside intrusions minimizes attacks on the University network. Many attacks on personal computers are simply an attempt to locate an "entrance" into the larger College network. If an attempted attack on your machine is unsuccessful, not only have you thwarted a local intrusion, more than likely, you've protected the College network as well. Therefore, protect your computer - as well as the entire College network - by choosing a strong password for your personal computer, and changing it frequently.

***Important* - Guidelines for Creating Secure Passwords:**

Passwords should:

- be at least six characters long
- consist of mixed case (at least one each of upper and lower case)
- contain at least one non-alpha character (such as a number or symbol)
- be different for different systems - especially for Darton versus non-Darton systems
- be changed frequently

Hint: A strong password might look something like: **wh3Wdh_1**

Passwords should **not**:

- be a name (pet, family member, friend, etc.)
- contain personal information that others would know about you
- be a word that can be found in the dictionary

NOTE:

Passwords are usually configured to expire every 90 days. At the time of expiration, you will receive a notice that your password has expired and you will be prompted to change it.

Change Windows NT/2000/XP and Exchange email passwords:

1. Press **Control/Alt/Delete**.
2. Click **Change Password**.
3. Enter your **old password**, your **new password**, and then your **new password** a second time.
4. Click **OK**.

Change MyDC Passwords:

1. Login to the Luminis Portal.
2. Click on the Bweb Tab
3. Chose "Change Pin"
4. Enter your **old PIN**
5. Enter a **new pin**

6. Re-enter New PIN

Install a Screen Password:

1. Click **Start**.
2. Click **Settings**.
3. Click **Control Panel**.
4. Click **Display**.
5. Click the **Screen Saver** tab.
6. Click the **drop-down box arrow**, and then choose a **Screen Saver**.
7. Click the **Settings** tab.
8. Check the **Password Protector** box.
9. Fill in **Wait X minutes** (This is the number of minutes you want the computer to wait before displaying the screen saver.)

Help:

If you have questions please contact the Help Desk for assistance (229-317-6704) or helpdesk@darton.edu.