1.0 Purpose

The purpose of this policy is to define standards for network and Email account eligibility, lifecycle, and security at Cape Cod Community College. These standards are designed to minimize the College’s potential exposure to damages which may result from unauthorized use of College resources. Potential damage includes the loss of sensitive or company confidential and financial data, intellectual property, damage to public image and critical systems.

2.0 Scope

The scope of this policy includes all staff, faculty and students who have or are responsible for an account at Cape Cod Community College.

Note: All faculty, staff and students are bound by the Cape Cod Community College Information Technology Resource Use Policy. That policy can be viewed at http://www.capecod.edu/web/guest/admin/it/documentation

3.0 Account Eligibility and Life

Faculty, staff, and registered students are eligible for a Cape Cod Community College Network and Email Account. The table below indicates the duration of the account and the source of the information for creation of the account:

<table>
<thead>
<tr>
<th>Account Type</th>
<th>Duration of the account</th>
<th>Where we get the information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered Student</td>
<td>Until graduation, or unregistered for three consecutive semesters, or account unused for one full academic year</td>
<td>Student Information System</td>
</tr>
<tr>
<td>Faculty</td>
<td>Until termination of employment or removal from the DCE Seniority List.</td>
<td>Office of Human Resources</td>
</tr>
<tr>
<td>Emeriti/Retirees</td>
<td>Perpetual or when the account goes unused for one year</td>
<td>Office of Human Resources</td>
</tr>
<tr>
<td>Staff</td>
<td>Until termination of employment</td>
<td>Office of Human Resources</td>
</tr>
</tbody>
</table>
Staff and Faculty Account Creation and Termination Procedures

Full-Time Faculty and Full/Part-Time Staff: The HR Office notifies IT when new staff and full time faculty are hired and requests that IT create an email address. When a Full-Time Faculty or Full/Part-Time staff member ends employment with the College HR contacts IT and requests that their account be deleted. There are instances, however, where at the request of the employee’s department head the College will maintain the account in an active status for a temporary period until a replacement (new hire) is in place.

Adjunct Faculty: The HR Office notifies IT when adjuncts are hired and requests that IT create an email address. The adjuncts maintain their email address as long as they remain employed by the College and remain active on the DCE Seniority List. When they are no longer employed, HR contacts IT and requests that their email address be deleted.

Emeriti/Retirees: Emeriti and retirees maintain their college accounts until they either indicate they no longer wish to maintain the account or have not accessed the account for one year. Many of our retirees remain actively involved with the College throughout retirement and this is a means to stay in contact.

Student Account Creation and Termination Procedures

All registered students at Cape Cod Community College are provided a network and Email account. Email is an official means of communication for students at Cape Cod Community College. All official College email is sent to each student’s email address. Examples of the types of emails sent to student accounts are:

- Invitations to register
- Responses to inquiries about registration, admissions, records, and financial aid
- Messages from faculty regarding coursework
- Notices of scholarship, educational, and financial aid opportunities and deadlines

Student Account Creation

Student accounts are generated through an automated process. Each day the student information system generates a request of the network active directory to create a network and email account for all students who have registered for courses in the previous 24 hours and do not currently have an account.

Student Account Termination

A utility application is run against the active directory network and email accounts at the end of each semester. The utility looks for students who have not accessed their accounts in the past academic year and deletes the accounts of those who met that criterion.

Further, a comparison of the student information system at the start of each semester identifying those students who have not registered for a course in the past three semesters (Spring, Summer,
and Fall) with those in active directory is conducted to eliminate student accounts that are active, but the students have not registered for a class in the past three semesters.

4.0 Account Passwords

All user accounts at Cape Cod Community College must meet the following level of password complexity:

All passwords must be at least 8 characters in length.
Passwords must not have been used in 4 previous passwords.
Passwords cannot be changed more than once in a single day.
Passwords must not contain the individual’s name or account name.
Passwords must contain at least (3) of the following (4) character groups:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Numerals (0 through 9)
- Non-alphabetic characters (such as !, $, #, %)

Mandatory Password Change

All user-level passwords are forced to be changed at least once each year. This is a minimum requirement. Users are encouraged to change their passwords more frequently.

General Password Construction Guidelines

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - The user’s ID, or subset thereof.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
Here is a list of "don’ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).

Passwords should not be written down or stored on-line. If one feels the password must be written down it should be placed in a location not associated with the computer such as a purse or wallet and the paper on which it is written should not be associated with the college or also contain the user login ID. When the password is fully memorized the paper should be destroyed.

5.0 Generic Accounts

Generic accounts are accounts that are assigned to groups or programs to enable members of those groups and programs to access College resources. Generic accounts must be highly controlled or expire when the need for the account ends.

Highly Controlled Generic Accounts

Highly controlled generic accounts are provided to a specific office or department for extended periods. The department or office personnel control the account absolutely, never conveying the account password to users. For example, the general public can use the CCCC library. The Library maintains a generic account. When a member of the general public wishes to use a computer in the library the library staff member will log onto the computer using the generic account and log off when the member of the general public is done.

Another example is a generic account provided to a specific office to be distributed for a specific purpose. The Partner programs and WERC are provided generic accounts.

Expiring Generic Accounts

The College often holds events, seminars, and other activities that require non-domain users to access computers. For these events the event coordinator fills out a Temporary Generic Account Form from the Outlook Public Folders or the Faculty Drive requesting the account. The account is created for the specific dates of the event and expires automatically at the end of the event.

6.0 Activity Timers
To improve security on the College network, all office desktop computers on the campus are configured to require the user to login after 60 minutes of inactivity. Following 60 minutes or more of inactivity, the inactivity timer will automatically lock the computer so no one else can access confidential data on the machine.

When the faculty and staff members return, they will continue working where they left off by pressing Ctrl + Alt + Delete and entering their password. The inactivity timer will not suspend or stop computer processes or applications running on the computer. Upon logging back in the user will be put into the computer's previous state prior to the inactivity timer execution.

External email access through Outlook Web Access has a 30 minute inactivity time out.