Home Folders

Each employee is provided a Home Folder, which resides on one of the college’s servers. This folder is included in our routine backup.

Employees are encouraged to delete non-work related files such as music or movie files or out-of-date files. Our backup process saves those files, in addition to the work-related items, on media tapes. The presence of non-work related items causes our backup routine to utilize resources that are best used elsewhere.

Outlook Web Access (OWA)

Employees are able to access their e-mail via the internet through the Outlook Web App (OWA) feature. Note that this is not a connection to the network — only e-mail.

With internet connectivity, such as DSL, the employee can open an internet browser and navigate to www.chipola.edu/faculty-staff.htm and then left click on the Web Mail link.

A log on window similar to the one shown below will be displayed. The User name field requires the employee’s network user name, and the Password field requires the employee’s network password.

Network Security

In response to the ever increasing concern regarding information and data security, you may be asked to provide proof of your identity before your network account is unlocked or password is reset. This proof may be something as simple as listing the last four digits of your Social Security number, which we have on file via the CAP #1.2 form that each employee must complete.

Also keep in mind that your account name and your password are the keys to the network, which is vulnerable if accessed by students, non-Chipola employees, etc. Due caution should be exercised when handling your network password, as well as your mainframe password.

Wireless Access Points

Wireless access points are available in many of the campus buildings. Chipola’s WiFi is broadcasting as CHIPOLA.

The Identity Services Engine Guest Portal will be presented as a webpage. The user has two options for accessing the Internet through the portal: a college provided user name and password (as described previously for your student network account) or the Self Service link.

The Self Service option requires the user to provide First Name, Last Name, Email Address, Phone Number, and Time Zone. The Self Registration screen will then present a user name and a password that the user must use to log into the Guest Portal.

After logging in with those credentials, the user will be presented with an Accept or Decline window that explains that the user must accept the terms and conditions set forth in the CAP 1.2 Acceptable Use Policy in order to continue. A copy of that policy can be obtained from our Help Desk, as stated on the screen.

This brochure is intended to provide Chipola College employees with some helpful tips on how to successfully log on to the college’s computer network.

It also contains information about obtaining assistance for computer-related issues.

This document does not replace the CAP #1.2 form (“Network, Internet and Lab Use Acceptable Use Procedure”) or any acceptable use policies currently in use by the college.
Once the Log On screen is displayed:
1. Type your user name into the first field.
2. Type the password that has been provided to you by Information Systems as your initial password.
3. Make sure Chipola is the default domain listed.
4. Click the arrow button or hit Enter on the keyboard.

Chipola College employees are required to complete the CAP #1.2 form (AKA IMM-29), which is named Network, Internet and Lab Use Acceptable Procedure. This form outlines the acceptable use policies and standards that are presently in effect at the college. Each employee should complete the form and obtain the required signatures and then return it to the Information Systems Department.

Employees are then assigned a network account and an e-mail account if approved by their department supervisor.

New Account Set Up

When an account is initially set up, Information Systems will select the option “User must change password at next logon”.

During the logon process, after clicking okay, the employee will be presented with a window that states the password must be changed before the user can log in for the first time. This is a security precaution, and it allows the new employee to create a password.

The employee should hit the OK button at the prompt. A new window will be presented with the Change Password fields.

Change Password

The Change Password window that is presented upon first logon when your account’s password is set with the “must change” option should look similar to the example shown below.

![Change Password Window](image)

The first field will present your user name. The next field (Old password) will display your current password as dots.

The New password field will require a password that meets our standards, as described in the next section.

The password is case sensitive and must be at least eight characters with characters selected from at least three of the four complexity categories.

Selecting items from 3 of the 4 categories will satisfy the requirement.

Some examples of passwords meeting the requirements are:
- Good4you (8 characters and 3 categories used)
- $amPi34U (8 characters and 4 categories used)
- Mon-day-1 (9 characters and 4 categories used)
- t3mPor4r^2 (10 characters and 4 categories used)

Retype the new password in the Confirm Password field. These two fields must match exactly.

When you have completed all fields, hit arrow key on the screen or the Enter key on your keyboard.

Password Expiration

Our password policy expires the passwords every 60 days. The network system will provide the user with a warning at about 14 days prior to the event.

The system will store the last 24 passwords used, so the user will not be able to reuse a password that falls within that list.

To change an expired password, users must be on campus and logged onto a networked computer. If off-campus, users may change the password prior to expiration by using Outlook Web App’s (OWA) Options feature.