

## **Confidential Information**

### **Purpose**

Union County College is committed to promoting an environment that retains the full trust and confidence of its students, faculty, staff, and donors. To promote a respectful workplace and honor the rights of all constituents of the College community, it is essential that the confidentiality and privacy of information be maintained. As a Union County College employee who has been given access to confidential information, it is your responsibility to protect this sensitive and personal data.

### **Scope**

This policy applies to all employees, including student employees, who have access to university data containing personal, academic or financial information.

### **Policy**

- I. Confidential information is considered to be all non-public information that can be personally associated with an individual. The College relies on its employees to maintain this confidentiality and to access, use, discuss, release, and disclose this data only when it is dictated by their job duties. If access to confidential information is not required to perform the job, under no circumstances should it be accessed. If access to confidential information is necessary to carry out job responsibilities, the information should not be divulged to anyone unless it is done so through authorized protocols. Confidential information can include, but is not limited to: Names, Social Security Numbers, Addresses, Telephone Numbers, Driver's License Numbers, Credit Card Information, Enrollment Projections, Budget Projections, Grades, Payroll Information, etc. Confidential information should not be sent unprotected over the Internet, stored unencrypted on an unsecured computer or an unsecured external storage medium or device, or communicated using an unauthorized third party e-mail or social networking system.
- II. Preservation and protection of usernames and passwords ensure that only authorized users have access to our data. As user access privileges are tailored to an individual's job responsibility, sharing of usernames and passwords is prohibited. Passwords should not be composed so that they may be easily guessed, and should conform to the password creation standards set by the College. If a password should be disclosed to any other person, the employee will be held fully accountable and responsible for any use or misuse by that individual to the same extent as if that employee had performed the act. If there is reason to believe that the employee password confidentiality has been violated, the department head or supervisor must be notified immediately.
- III. Employees of Union County College must abide by the rules, regulations, policies and procedures of the College as well as all Federal and NJ State laws applicable to their position at the College. Supervisors of student employees must identify those students who have access to confidential information and ensure that they are aware of and abide by the provisions of this policy.
- IV. For College employees, breaches in confidentiality may result in disciplinary action up to and including termination of employment. A violation of this agreement may also result in criminal action if it is determined that any local, state or federal laws have been violated.
- V. In accessing College confidential information, the employee acknowledges he/she will:

- a. Access, distribute and share confidential data only as needed to conduct campus business as required by his/her job;
  - b. Respect and safeguard the confidentiality and privacy of individuals whose data is accessed;
  - c. Protect confidential information stored or displayed on the workstation;
  - d. Scan all downloads and media for viruses prior to use;
  - e. Immediately report to the department head or supervisor any and all security breaches;
  - f. Comply with all department, campus IT and business process security policies and procedures.
- VI. In accessing College confidential information, the employee also acknowledges that he/she will NOT:
- a. Discuss verbally or distribute in electronic or print formats, confidential information except as needed to conduct campus business as required by his/her position;
  - b. Gain or attempt to gain unauthorized access to campus computing systems;
  - c. Make, accept or use unauthorized copies of software or download any unauthorized programs from the Internet and ensure that license agreements are not purposefully violated;
  - d. Use or allow others to use data for personal gain;
  - e. Engage in any activity that could compromise the security or confidentiality of data;
  - f. Use another's computer sign-on or computer access codes, or provide another the use of such codes to gain access to confidential information without proper authorization;
  - g. Disclose confidential information to those not authorized to receive it.