Delaware State University

University Area(s) Responsible: Office of Human Resources; Division of Information Technology

Policy Number & Name: 4-05: Misuse of Confidential Information Policy

Approval Date: 3/31/11

Revisions: _____

Related Policies and Procedures: _____

Purpose

To ensure that information that has been identified as confidential is not misused therefore protecting the privacy and reputation of Delaware State University, its employees and its students.

Policy

Delaware State employees must not misuse confidential information (employee, student, and University). This includes attempting to gain access to confidential information to which they have no authorized access; keeping and sharing confidential information they have received or come across by accident; sharing confidential information they have authorized access to. University employees with authorized access are strictly prohibited from sharing confidential information about the University, its employees and its students with University members who have not been authorized to see and use such information. Employees are also strictly prohibited from sharing DSU confidential information with outside parties such as contractors, consultants, etc. Entities outside the University will have access to University confidential information that is allowed by law after following the proper steps to request it. A violation of this policy will result in disciplinary action up to and including termination of employment.

Definitions

Confidential Information - non-public information about a person or an entity that, if disclosed, could result in criminal or civil liability, or harm the person or entity's financial standing, accreditation, employability, privacy or reputation. Delaware State University is legally and contractually bound to protect some types of confidential information. There are other instances in which the University will require protection of confidential information beyond legal or contractual requirements as an additional protection.

Confidential Information includes but is not limited to:

- Any information that could harm the University, its students and its employees
- Certain Policies and Procedures (internal policies & procedures; Board of Trustees and administrative minutes)
- payroll records, salary and non-public benefits information
- Social Security numbers, driver's license numbers, state identification card numbers, passport numbers
- all information, materials, data and records designated confidential by a University unit, by law or by contract, including information obtained by the University from third parties under non-disclosure agreements or any other contract that designates third party information as confidential
- credit and debit card information, and financial account information
- personnel records, including but not limited to information regarding an employee's work history, credentials, salary and salary grade, benefits, length of service, performance, and discipline
- individual criminal background check information
- individual conflict of interest information
- individually identifiable biometric information
- computer system passwords and security codes
- unpublished grant proposals and unpublished research data
- unpublished manuscripts and correspondence
- budgetary information
- departmental information
- University planning information
- non-public financial, procurement, health/safety, audit, insurance and claims information
- internal investigation information, pre-litigation, and non-public litigation and administrative agency charge, audit and inquiry information
- student records, including but not limited to student education records within the protection of FERPA
- proprietary or intellectual property in which the University asserts ownership that is created by University employees in connection with their work
- non-public law enforcement records generated or maintained by the Department of Public Safety
- all University attorney-client communications and University attorney work product
- non-public donor and alumni information

- Employee patient care records including patient benefit plan enrollment, claims, billing matters, and data concerning human research subjects
- medical records, personally identifiable medical information, and all information designated as "Protected Health Information" under the Health Insurance Portability and Accountability Act (HIPAA), or otherwise protected by law

In order to prevent the misuse of confidential information Delaware State Employees **must not**:

- Use information viewed or retrieved in an unauthorized or unlawful manner for their personal benefit or the benefit of others
- Access information not directly related or relevant to his/her specifically assigned duties and responsibilities
- Disclose, discuss and/or provide confidential information to any individual not authorized to view or access that data, including but not limited to third parties, volunteers, contractors, vendors and other University employees
- Engage in careless, negligent, or improper handling, storage or disposal of confidential data, including electronically stored and/or transmitted data, printed documents and reports containing confidential information
- Delete or alter information without authorization
- Create and/or disseminate false or misleading information about the University, its employees and its students

Guidelines to Ensure the Appropriate Use and Handling of Confidential Information:

1. All employees required to handle confidential information must safeguard such information and only use it or disclose it as expressly authorized or specifically required in the performance of their job duties.

2. Employees with authorized access codes to use systems that generate, store or manage confidential information have the responsibility of preserving the confidentiality of such codes to prevent any unauthorized use by others. Those employees who negligently or intentionally share their passwords or accounts with anyone else will be held responsible for any resulting misuse of the system by others.

3. Employees who suspect or become aware that his/her access codes have been compromised must inform their supervisor right away.

4. Employees with authorized access are strictly prohibited from accessing University databases and administrative systems for the purpose of allowing others to view the information in those databases and/or systems.

5. Employees with access to confidential information are expected to know and understand security requirements that have been established to protect such information in whatever medium used (printed, electronic or voice recorded).

6. Employees working with confidential information must ensure that their computer screens are positioned so that only authorized users can view confidential information. Flash-drives, CD's, DVD's, laptops, must be protected at all times and must not be shared with unauthorized employees.

7. Confidential information must be discarded in accordance with the University's Records Management Policies and Procedures. Confidentiality must be preserved at all times.

8. Employees handling confidential information will be trained in their appropriate handling. Those employees who are placed into positions that require adherence to government-mandated compliance (e.g., HIPAA, Medicare Compliance, grant and contract administration, pathogens or select agents) will be subject to strict procedures for handling such materials, must attend all mandated training sessions, and comply with compliance-specific policies and applicable law.

9. Any violations of this policy must be reported immediately to the corresponding unit/department head or their immediate supervisor in their absence.

10. Employee misuse of confidential information and/or the systems in which the information is stored is a serious breach of job responsibilities and will result in discipline up to and including termination of employment.

FERPA

The Family Educational Rights and Privacy Act (FERPA), protects student education records. Student education records must not be disclosed under any circumstances unless

the student's express consent has been obtained. There are circumstances in which the University's Legal Counsel and the University's Registrar may formally authorize the disclosure of such records. In compliance with FERPA, the Registrar's Office will not disclose student directory information until it confirms that the student has not elected to block his/her directory information.