Delaware State University

University Area(s) Responsible: Department of Enterprise Risk Management
Policy Number & Name: 07-39 Clean Desk Policy
Approval Date: 07/15/16
Next Review Date: 07/15/18

I. Purpose

The purpose for this policy is to establish a culture of security and trust for all campus community members at Delaware State University (the "University"). An effective clean desk effort involving the participation and support of all University faculty, staff, student workers, contractors and vendors can greatly protect sensitive information within our campus community. Everyone should familiarize themselves with this policy.

The main goals of the clean desk policy are to:

a. Produce a positive environment where information security is a priority;
b. Reduce the threat of a security incident due to the mishandling of non-public information; and
c. Prevent the theft of sensitive information, which can be subject to abuse.

II. Scope

All faculty, staff, student workers, contractors and vendors working on behalf of the University are subject to this policy.

III. Definitions

Non-Public Personal Information

Non-public Personal Information is any data or information considered to be personal in nature and not subject to public availability.

Personal information includes, but is not limited to:

- Individual names
- Social Security numbers
- Credit or debit card numbers
- State identification card numbers
- Driver's license numbers
- University identification numbers
- Health records

IV. Policy

The following directives must be adhered to by all individuals subject to this policy to ensure the safekeeping of non-public information:

a. Prior to an extended period away from a workspace, all sensitive working papers are expected to be placed in locked cabinets or drawers. A closed and locked office door also satisfies this directive.
b. At the end of the working day faculty, staff, student workers, contractors and vendors are expected to organize their workspace and to put away all office papers.
c. Time should be allocated to clear away paperwork and reduced clutter.
d. Refer to the University's Document Retention Policy to determine how long records should be retained. If a document is past its retention period, it should be disposed of properly. All documents containing non-public information **must** be shredded prior to disposal.
e. Consider scanning documents and filing them electronically.
f. Use recycling bins for documents when they are no longer needed. Documents containing non-public information **must** be shredded prior to recycling.
g. All desks and filing cabinets that contain sensitive information must be locked at the end of the day.
h. All portable computing devices such as laptops or PDA devices should be locked up when not in use to prevent unauthorized access.
i. Mass storage devices such as CDROM, DVD or USB drives containing non-public information should be considered sensitive and secured in a locked drawer.

V. Enforcement

a. Periodic desk top audits will be performed to determine adherence to this policy. These audits will be unannounced.
b. Any University faculty, staff or student worker found to have violated this policy may be subject to progressive disciplinary action, up to and including termination of employment.