Clean Desk Policy	**6-013** **TECHNOLOGY SERVICES** **December 2019**

POLICY

1.01 Confidential/regulated written materials that are unsecured constitute a security risk to OSU Institute of Technology (OSUIT). A clean desk policy is necessary to minimize the risk of information security vulnerabilities in the workplace. This policy will also serve to increase employees' awareness concerning the necessity of protecting printed versions of confidential/regulated information in fulfillment of state law (62 O.S § 34.32) requiring compliance with ISO standards 27001/17799 as well as protecting basic privacy of the individuals whose confidential/regulated information OSUIT collects.

1.02 This policy is applicable to all OSUIT employees, vendors, and partners with access to OSUIT information resources. In addition to protecting privacy, mitigating risks, and reducing vulnerabilities, it also engenders a positive image of OSUIT as our employees are serving our stakeholders.

PROCEDURES

2.01 Each individual has the responsibility for ensuring that all confidential/regulated information, paper-based or electronic, is secure at all times and remains in the office of the Data Custodian.
2.02 When working with a student or employee, documents that do not pertain to the current person being helped should not be visible to them.
2.03 Computer workstation screens must be locked when a workspace is unoccupied.
2.04 Computer workstations should be shut down completely at the end of the workday.
2.05 Any confidential/regulated information must be removed from the desktop and locked in a drawer for any periods the desk is unoccupied and at the close of business.
2.06 File cabinets containing confidential/regulated information must be kept closed and secured when not in use or unattended.
2.07 Keys to locked confidential/regulated storage units must not be left unattended.
2.08 Passwords must not be accessible on sticky notes or other written format in an accessible location.
2.09 Printouts containing confidential/regulated information should be immediately removed from printers or fax machines.
2.10 Upon reaching the end of the applicable retention period for confidential/regulated information, documents must be shredded and disposed of by confidential means. Under no circumstances should paper or digital media containing confidential/regulated information be disposed of in the regular waste baskets or bins.

2.11 Digital storage devices such as USB drives containing confidential/regulated information must be stored in a locked drawer.

2.12 Time must be allocated to accommodate the securing of confidential/regulated information within the custodial department. Confidential/regulated paper documents should not be taken off the OSUIT campus.

Approved: August 2017
Revised: December 2019