

# Lebanese American University

## Information Security Regulations

### Clean Desk Regulations

**Last Updated:** April 2017  
**Version 1.2**

#### **Overview**

Clean desk regulations can be an important tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such regulations can also increase employee's awareness about protecting sensitive information.

#### **Purpose**

The purpose for the clean desk regulations is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about LAU, employees, intellectual property, students and suppliers is secure in locked areas and out of site.

#### **Scope**

The clean desk regulations apply to all LAU employees and affiliates.

#### **Regulations**

##### ***Secure Sensitive and Confidential Information***

Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when the desk is unoccupied.

##### ***Locked Desktops or Laptops***

All computers, laptops and input devices must be locked with password when unoccupied.

##### ***File Cabinets Locked***

File cabinets containing restricted or sensitive information must be kept closed and locked when not in use or when not attended.

##### ***Keys for Access Restricted Areas***

Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

##### ***Writing Down Passwords***

Users must not write their passwords down unless they have effectively concealed such passwords in seemingly unrelated characters or they have used a coding system to conceal the password.

##### ***Printouts removed from Printers***

Printouts containing restricted or sensitive information should be immediately removed from the printer.

##### ***Whiteboards with Restricted Data***

Whiteboards containing restricted and/or sensitive information should be erased.

***Mass Storage Devices***

Treat mass storage devices (DVD, CD, or USB drives) as sensitive and secure them in a locked space/container.

***Disposal of Important Documents***

Restricted and/or sensitive documents should be shredded prior to the disposal.