	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	Clear Desk and Clear Screen	Last Review date	19/5/2021
	Policy Number	IT-12	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

Overview:

Clear Desk and Clear Screen policy are to establish a culture of security and trust for employees at The University of Sharjah. An effective clean desk and clear screen policy involving the participation and support of the University of Sharjah's faculty, staff and students can greatly protect paper and electronic documents that contain Restricted Use Data about students, employees, alumni, and contractors. All users that handle data should familiarize themselves with the guidelines of this policy.

Scope:

This policy applies to anyone who uses UoS information assets including Faculty, staff, students, visitors, and contractors. The policy applies to the individual, groups and committees.

Purpose:

The purpose of the University of Sharjah's Clear Desk and Clear Screen Policy is to provide users with information on Clear Desk and Clear Screen processes to ensure the protection of the University of Sharjah's information and information assets.

Definitions

1. SLA: Service Level Agreement
2. NDA: Non-Disclosure Agreement

Policy

Clear desk policy:

1. All University of Sharjah's faculty and staff must abide by the governing rules mentioned in this policy in relation to securing information either manual or electronic.
2. All confidential printed/ electronic/digital business/Academic documents such as (but not limited to) SLAs, Contracts, NDAs, Invoices, Employee Records, Account Numbers, Personal Information, Medical Information, Financial information, etc. should be filed and kept in a secured file cabinet.
3. The digital format of the important business/ academic documents should be stored securely. Wherever required it should be secured using appropriate encryption.
4. Any important business information printed or digital, that is no longer needed, must be discarded securely by using appropriate shredders or degaussing/ clinically wipe data tools.
5. Use secure recycling bins in the premises for any bulk printed papers that are no longer

needed. Use shredder/ degaussing device to dispose papers / USB / CD / Hard disks with sensitive data imprinted.

6. Avoid printing off any important business email for reading. Printing unnecessary information generates clutter and can reveal sensitive business information if not adequately secured.

7. No document should be left unattended at a photocopying machine.

8. While away from your desk for a short duration such as during lunch/tea breaks, away for meetings, sensitive business information shall be kept in locked drawers.

9. The employee must not leave portable communication devices such as smartphones, iPads, data cards, etc. unattended and physically lock these devices while away from the office premises.

10. Public display of confidential/ internal data must be avoided. Critical information should not be written on paper chits (passwords and other confidential information) should not be stuck to the desks or computers of the employees. .

11. Make sure that removable media is locked away when not in use. Staff should not do not leave CDs, DVDs, and Memory Sticks in drive bays, USB drives, or plugged into devices.

12. Always ensure that keys to locked filing cabinets or drawers are kept in a secure location.

13. Ensure that all office areas are secured when not in use. There should be a "last person out" routine so that everyone understands their responsibilities for locking doors, closing windows, and setting security alarms.

14. Remove all information from flipcharts and wipe down whiteboards.

Clear screen policy:

1. While away from your desk for a short duration such as during lunch/ tea breaks, away for meetings, laptops/ desktops/ IT client devices/ access screens should be locked. E.g.: in windows systems, Win+L can be used to lock a system. A similar method for Mac Systems is to press and hold the power key for more than one second.

2. Any system not locked and left idle shall be configured to auto-lock in 15 mins. A password shall be prompted to log in to the system again.

3. Laptops must be physically secured and used responsibly to prevent compromise of sensitive information or unauthorized network access.

4. Screens should be angled away from the view of unauthorized persons.

5. Make sure that you shut down your computer at the end of the working day

6. Delete any electronic data from the recycle bin of any communal computers that you use.
7. Work from home same guidelines to be followed – ref remote work policy for details

Reference

Sl No	Standard Name	Control Reference
1	ISO 27001:2013	A.11.2.9