



WESTERN NEW MEXICO UNIVERSITY

POLICY NAME	Clean Desk & Clear Screen Policy	POLICY NO.	BA467
APPROVING BODY	President/Cabinet	VERSION NO.	01
RESPONSIBLE DEPARTMENT	Business Affairs- Information Technology		
EFFECTIVE DATE	Date	REVIEW/REVISION DATE	NEW

PURPOSE:

To protect university information and information systems from unauthorized access, accidental disclosure, loss, theft, or misuse by establishing minimum requirements for securing physical workspaces, documents, and electronic devices.

POLICY:

CLEAR DESK

1. Employees must secure sensitive information on paper documents, notebooks, printouts, removable media, and other physical formats to prevent viewing or access by unauthorized individuals.
 - a. **Brief absence:** Secure or remove sensitive information from view before leaving a workspace unattended. Closing and locking an office door may be an appropriate safeguard when it prevents unauthorized access. Employees should also consider visibility through windows, glass walls, or other openings.
 - b. **Extended absence or end of day:** Store sensitive information in locked drawers, cabinets, offices, or other secure storage locations.
 - c. **Public or shared workspace:** Do not leave sensitive information exposed or unattended where unauthorized individuals may view, access, photograph, or remove information.
2. Do not leave sensitive information visible to others on desks, whiteboards, sticky notes, or other any other physical medium
3. Promptly retrieve sensitive or confidential documents from printers, copiers, scanners, and fax machines. Do not leave sensitive information unattended in shared printing areas.
4. Secure university owned or managed laptops, tablets, mobile devices, removable media, or other portable equipment when unattended. Safeguards may include using closed and locked office doors, cable locks, or lockable drawers.
 - a. When travelling, employees must maintain physical control of university devices and reasonably protect them from loss, theft, or unauthorized access. Devices must not be left unattended in vehicles, public spaces, or other locations where they could be accessed by unauthorized individuals.

CLEAR SCREEN

1. Screens should be locked for university desktops, laptops, tablets, mobile devices, and any other device capable of displaying or accessing university information whenever unattended. This is applicable to all university information not solely to sensitive information.
2. As a safeguard all devices should be set to automatically lock after a short period of inactivity, the recommended maximum inactivity period is five (5) minutes. Employees should manually lock devices rather than relying solely on automatic locking.
3. Employees should disable screen previews or notifications that could display sensitive data on locked screens or while sharing your screen during a video call.
4. As best as possible employees should position all screens to prevent unauthorized viewing when working in shared, public, or high traffic areas. Use a physical privacy filter when appropriate

ADDITIONAL STANDARDS

REMOTE & HYBRID WORKSPACES

1. Employees working remotely or in hybrid environments must lock university devices when unattended, securely store sensitive documents and removable media, and take reasonable measures to maintain a private and controlled workspace.
2. When working remotely, employees should take reasonable measures to prevent persons residing in the same household, roommates, guests, visitors, or other unauthorized individuals from viewing or accessing university information.
3. Employees must not leave sensitive documents or university devices unattended in vehicles or other unsecured locations. Devices may be left unattended in secure locations that have been listed on a remote work plan and agreement document or an employee's permanent address.
 - a. If needed, use privacy filters when working in public or shared environments.
 - b. If a remote or hybrid employee is traveling or working in a public environment all university devices should always remain in your possession. Devices should not be left unattended in hotel rooms, vehicles, or any other area.

HANDLING SENSITIVE INFORMATION

1. Do not keep passwords, authentication codes, recovery codes, security questions, or other authentication secrets in unsecured areas or leave them visible at any time.
2. Where credential storage is necessary, employees must use university-approved password managers, credential-management platforms, or other IT-approved secure storage methods. Credentials must not be stored on removable media unless the method has been approved by the university's Information Technology Department.
3. Employees must remove sensitive information from whiteboards, glass boards, conference room displays, flip charts, and other share surfaces immediately after use.
4. Employees must take reasonable precautions to prevent sensitive information from being disclosed in presentations, printed materials, photographs, screen sharing, or other forms of communications.

MISPLACED INFORMATION

1. If you discover someone else's sensitive information, employees should protect it from additional exposure and notify the appropriate supervisor or data owner immediately.
2. Employees must promptly report suspected loss, theft, unauthorized access, disclosure, or exposure of sensitive information or university devices to the procurement office, information technology department, and law enforcement if applicable.
3. Employees must not further access, copy, distribute, or disclose discovered sensitive information except as necessary to protect it or as authorized by the university.

EXPECTATIONS

1. All university employees regardless of employee classification, department or part-time/full-time status must comply with this policy. Contractors, vendors, student workers, and other covered individuals must also comply with applicable requirements under this policy
2. Supervisors should reinforce expectations and to the best of their abilities provide direct reports with the means to follow the standards outlined in this policy.

EXCEPTIONS

1. Exceptions to this policy must be documented in writing and approved in advance by both the Chief Information Officer and Vice President of Business Affairs.
2. Each exception request must identify the requirement for which an exception is requested, the business or operational justification, the duration of the exception, and any safeguards necessary to reduce associated risks.
3. Exceptions must be reviewed periodically and must be renewed or closed when the approved period expires or the justification no longer applies.

VIOLATIONS

1. Violation of this policy may result in individual trainings being provided, loss of access to university systems, data, computing resources, or other resources.

DEFINITIONS:

- Sensitive information/data: Information, in any format or medium, that is not intended for unrestricted access or disclosure and that requires protection against unauthorized access, use, disclosure, alteration, loss, or destruction because of legal or regulatory requirements, contractual obligations, institutional policy, or the potential for harm to individuals, the institution, or other parties.
- Sensitive information/data includes, but is not limited to, personally identifiable information; student education records; employee and applicant records; financial, payroll, and payment information; health and medical information; authentication credentials, passwords, and access keys; confidential research data; nonpublic institutional financial, operational, or security information; and information designated

as confidential, restricted, or otherwise protected under applicable law or institutional policy.

- Sensitive information/data may exist in paper documents, electronic files, computer screens, email, printed materials, removable media, whiteboards, presentations, conversations, photographs, or other forms of communication or storage.

DOCUMENT CONTROL REGISTER*				
For Internal Use Only – Master Document				
DOCUMENT TITLE:		DOCUMENT NO.	EFFECTIVE DATE:	
Clean Desk & Clear Screen Policy		BA467		
DOCUMENT LOCATION: (Where is this document referenced or located; include links to SharePoint or any other locations that are accessible)				
REVIEW HISTORY (Complete log for review only)				
REVIEWED	REVIEW DATE:	REVIEWED BY:		
<u>ANNUAL REVIEW</u>	<u>16-OCT-2026</u>	<u>Michael Acosta</u>		
REVISION HISTORY (For audit purposes and control tracking)				
REASON FOR REVISION: **	REVISED SECTION, PAGE#, and PARAGRAPH:	VERSION #:	REVISION DATE:	APPROVED BY:
NEW POLICY	NEW	01	16-OCT-2026	VPBA