NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

State of North Carolina

Clean Desk Procedure

Statewide Information Technology Procedure

Version 1.0

December 2025

Document Information

Revision History

Date	Version	New or Revised Requirement	Description	Author
Dec 18, 2025	1.0	New	Procedure Creation	OPDP

Document Details

Department Name	Office of Privacy and Data Protection
Owner	Martha K. Wewer
Title	Clean Desk Procedure
Publication Date	Dec 18, 2025
Next Review	Dec 18, 2026
Document Type	Procedure
Document Number	1
Version	1.0

Table of Contents

Purpose

Pursuant to N.C.G.S. § 143B-10(j)(3) and the Statewide Information Security Manual (SISM) the N.C. Department of Information Technology is authorized to develop, document, and disseminate internal policies and procedures. The purpose of this procedure is to ensure that State employees protect Confidential, sensitive, and proprietary Information by keeping workspaces (desks and screens) clear of Confidential Information when unattended or not in use, thereby mitigating any risk of loss, improper disclosure or compromise of Confidential Information. This procedure establishes the minimum requirements for a clean desk. Agencies may create procedures with stricter requirements in accordance with laws and regulations applicable to that agency.

Content Lead

N.C. Department of Information Technology, Office of Privacy and Data Protection (OPDP)

Scope

This policy applies to all employees, contractors, and temporary staff who handle information on behalf of the State.

Procedure

Workstation Security

Staff must clear desks of papers, notebooks, and any removeable media containing Confidential Information when leaving their workspace unattended, even temporarily. Confidential Information may be locked in file drawers and keys must remain on the staff at all times. Offices storing Confidential Information must be locked. Employees should work with their managers to identify secure storage needs.

Computers must be locked and secured whenever unattended. Employees who regularly work with Confidential Information should use a “privacy screen” where possible to prevent unintended exposure of Confidential Information or “Data Spillage.” Keys and access cards must be stored securely and not left out. ID badges must be worn above the waist at all times in accordance with the Physical and Environmental Protection Policy. Passwords, Personal Identification Numbers (PINs), and/or other login credentials must not be left on sticky notes posted on or under a computer, nor may they be left written down in an openly visible location.

Employees must use “secure printing” to print documents containing Confidential Information where available. Community printers and faxes must be cleared of papers containing Confidential Information as soon as they are printed to ensure that sensitive documents are not left in trays for the wrong person to pick up. Employees who have a private printer within their assigned workstation or private office must take proper action to ensure documents containing Confidential Information are not left unattended and are secured in a locked area or locked office.

Sharing of Physical Documents or Media

Confidential Information should be shared only with those individuals who are authorized to view the information. In accordance with the Media Protection Policy documents, files, or media (USB, Disks, external hard drives) containing Confidential Information to be shared with a staff member must be encrypted and must not be left unattended. Physical documents containing Confidential Information may be labeled with the optional “Confidential Information Coversheet” (Appendix A) before being handed over to a staff member.

End of Day/Shift Procedure

All documents containing Confidential Information must be stored in locked cabinets or shredded once no longer needed. Laptops should be locked or shutdown and taken home. Whiteboards containing information must be erased. Printers should be checked for unclaimed documents. Unclaimed documents from printers and fax machines should be placed in the shred bin.

Visitors and Shared Spaces

Visitors must be escorted at all times in accordance with the Physical and Environmental Protection Policy. Conference rooms should be checked after meetings to ensure no materials are left behind. Whiteboards must be erased.

Proper Disposal

Physical materials containing Confidential Information must be shredded or properly destroyed in accordance with the state Data Classification and Handling policy and the State's Data Retention Guidelines. Staff should ensure that materials are not subject to the Public Records Act, litigation hold, or any other records retention requirements before disposing. Employees should contact their Records Officer regarding agency retention requirements.

Roles and Responsibilities

The Office of Privacy and Data Protection is responsible for this procedure and its enforcement in collaboration with the Office of General Counsel and the Enterprise Security and Risk Management Office (ESRMO). Employees should report any incident of noncompliance with this procedure as a security incident via the ServiceNow portal.

Regulations and Applicable Laws

- N.C.G.S. § 143B-10(j)(3)
- The Statewide Information Security Manual
- NIST Special Publication 800-53 Revision 5, Security and Privacy Controls

Enforcement

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

Procedure Review Cycle

The Clean Desk Procedure will undergo a periodic review at annual intervals, or as changes are required. Updates to the procedure will be determined based upon the nature of the change, the procedure and requirements driven by need.

Any identified changes, or outdated information within the procedure will be addressed promptly. This may involve revisions, additions, or removals as needed to ensure that policies remain current and relevant.

The following roles provide leadership and management over this policy in accordance with the NCDIT Policy Management Policy:

- Statewide Chief Information Officer
- Statewide Chief Information Security Officer
- Statewide Chief Privacy Officer
- Department of Information Technology, General Counsel
- Department of Information Technology, Human Resources

Definitions

Data Spillage

The transfer of classified or Confidential Information to unaccredited or unauthorized systems, individuals, applications, or media. A spillage can be from a higher-level classification to a lower one.

Confidential Information

Refers to all information about the organization, its operations, clients, or employees that is subject to reasonable efforts by the organization to maintain its confidentiality and that is not typically disclosed by custom or law to people who are not affiliated with the organization but does not qualify as a trade secret.

References

Statewide Data Classification and Handling Policy
Statewide Information Security Manual
Statewide Glossary of IT Terms

APPENDIX A

North Carolina Department of Information Technology
Office of Privacy and Data Protection
Confidential Information Cover Sheet

To be used on all documents containing Confidential Information

DOCUMENTS ENCLOSED ARE SUBJECT TO THE NC STATEWIDE DATA CLASSIFICATION AND HANDLING POLICY

Contents shall not be disclosed, discussed or shared with individuals unless they have a direct need to know in the performance of their official duties. Deliver this/these document(s) directly to the intended recipient. DO NOT drop off with a third party.

The enclosed document(s) may contain personal, sensitive, confidential or privileged information and should be treated as such. Unauthorized disclosure of this information may result in CIVIL and CRIMINAL penalties. If you are not the intended recipient or believe that you have received this document(s) in error, do not copy, disseminate or otherwise use the information and contact the owner/creator or your Privacy Liaison regarding the document(s) or report the disclosure to the Office of Privacy and Data Protection at opdp@nc.gov

COVERSHEET END