# Randolph College Policy Proposal/Revision Cover Sheet

(Text will re-size as you type)

| **Policy Name** | **Proposal Type** | **Name of Lead Policy Drafter** |
|---|---|---|
| Clean Desk Policy | ☑ New policy<br>☐ Revision to existing policy<br>☐ Retirement of existing policy | Theron McLeod |
| **Brief Policy Description** | **Policy Type** | **Other Individuals Involved** |
| The Clean Desk Policy establishes guidelines to protect sensitive and legally protected information by ensuring that workspaces remain secure. | ☑ Standalone<br>☐ Part of Larger Policy Document: | Adam Fabirkiewicz, Jonathan Tyree, Tim Smith, John Keener, Erin Heller, Blair Gross |
| | **Responsible Department or Office** | **Original Submission Date** |
| | College Wide | 03/27/2025 |
| | | **Desired Implementation Date** |
| | | ASAP |

**Brief Rationale for Policy** Include any external mandates, regulations, accreditation factors, reporting, etc.

This policy supports GLBA compliance by reducing the risk of unauthorized access to sensitive data. By requiring employees to secure electronic and physical information when unattended, the policy helps safeguard nonpublic personal information. Implementing these controls aligns with regulatory expectations for safeguarding College data and maintaining a secure work environment.

**Departments or Offices of the College Impacted**

College Wide

**Existing College Policies Impacted By or Overlapping This One**

N/A

**OFFICES RESPONSIBLE FOR FIVE-YEAR POLICY REVIEW** Include brief description of how five-year policy review will be conducted.

IT Policy Committee

ASSUMING PASSAGE, YEAR AND TERM OF FIRST FIVE-YEAR REVIEW: Spring 2030

**RESOURCES NECESSARY FOR IMPLEMENTATION** Include necessary training as well as operational costs.

N/A

**NEW COMMITTEES OR GROUPS NECESSARY FOR IMPLEMENTATION** Describe the composition of necessary committees.

N/A

**APPROVAL TIMELINE** Entering a name and approval date below signifies that written approval has been communicated.

| *Approval Stage* | *Name* | *Approval Date* |
|---|---|---|
| (1) Direct Supervisor of Lead Policy Drafter (if applicable) | Theron McLeod | 3/27/2025 |
| (2) Appropriate President's Leadership Team (PLT) Member (if other than policy drafter) | Jonathan Tyree | 3/28/2025 |
| (3) First PLT Approval (prior to Public Comment Period) | | |
| (4) Second PLT Approval (following Public Comment Period) | | |
| (5) Board of Trustees (if applicable) | | |

**BEFORE SUBMISSION TO THE PLT, ENSURE THAT ● THIS FORM IS FULLY COMPLETED (I.E., IF A QUESTION IS NOT APPLICABLE, PLEASE INDICATE THAT); ● THE *APPROVAL TIMELINE* DIRECTLY ABOVE IS COMPLETED THROUGH STEP 2; ● IN THE POLICY ITSELF, (A) ALL SPECIALIZED TERMS ARE CLEARLY DEFINED AND (2) AN APPEALS PROCESS IS ADDRESSED AS APPROPRIATE.**

**VPIE COMPLETES UPON FINAL APPROVAL**

Date of final approval

Date policy goes into effect

Individual responsible for implementation

# Clean Desk Policy

---

**Purpose:** This policy outlines the expectations for maintaining a clean and secure work environment to protect sensitive College data and ensure the privacy of students, faculty, and staff.

**Scope:** This policy applies to all faculty, staff, student workers, emeriti, and vendors that have College network accounts.

---

**Policy:**

1. **Lock Computers and Devices**
   - 1.1. Lock screens
     - 1.1.1. When leaving your desk, even for short periods, lock your screen or log off of your computer.
     - 1.1.2. When leaving a mobile device unattended, lock the screen.
2. **Physically Secure Computers and Devices**
   - 2.1. When laptops are not in use, they should be stored behind a securely locked door.
   - 2.2. Tablets and other portable storage devices such as USB drives and external hard drives should also be locked away in a desk drawer, filing cabinet, or another secure location.
   - 2.3. If transporting a device, make sure to keep it locked in a secure area where it is not visible.
3. **Protect Sensitive Information**
   - 3.1. Minimize the display of data classified as **Confidential** or **Legally Protected** on your computer screen, especially in shared workspaces.
   - 3.2. Consider using a privacy filter if the contents of your screen may be visible to others.
4. **Secure Physical Documents**
   - 4.1. Clear your desk
     - 4.1.1. At the end of each day, remove all documents and papers containing sensitive information from your desk. File them securely in locked drawers or cabinets.
   - 4.2. Minimize printed documents
     - 4.2.1. Print only what is necessary.
     - 4.2.2. Do not leave printouts unattended at printers.
   - 4.3. Shred Sensitive Documents
     - 4.3.1. Shred any documents containing sensitive data before discarding them.
5. **Securing Office Locations**
   - 5.1. Lock offices and desks
     - 5.1.1. Lock your office door and desk drawers when leaving for extended periods or overnight. In shared office locations, lock the office door when you are the last to leave the space.
   - 5.2. Secure PawPass and Keys
     - 5.2.1. Do not share your PawPass or keys granting access to College systems, buildings, or sensitive areas.
     - 5.2.2. Report lost or stolen keys immediately.
   - 5.3. Be aware of your surroundings
     - 5.3.1. Be mindful of your surroundings and report any suspicious activity to Campus Security.

Randolph College employees must promptly report harmful events or policy violations involving Randolph College assets or information to their supervisor/department chair or a member of the Information Technology team. Events include, but are not limited to, the following:

- **Technology incident:** any potentially harmful event that may cause a failure, interruption, or loss of confidentiality, integrity, or availability of Randolph College information resources.
- **Data incident:** any potential loss, theft, or compromise of Randolph College information.
- **Unauthorized access incident:** any potential unauthorized access to a Randolph College information resource.
- **Facility security incident:** any damage or potentially unauthorized access to Randolph College data centers, switch closets, or phone rooms.