COLLEGE OF MICRONESIA-FSM

ADMINISTRATIVE PROCEDURE No. 8300

Administrative Data

Date Adopted:	21 May 2002
Date Revised:	11 December 2009, 11 March 2022
Date Reviewed:	28 May 2014, 25 January 2022, 12 June 2025
References:	General Data Protection Regulation (GDPR), SO/IEC 27001: Information Security Management Systems, NIST Cybersecurity Framework (CSF), EDUCAUSE Cybersecurity and Data Governance Resources

A. Access to Administrative Data

Authorized administrators, faculty, and staff are permitted to access only those data and transactions necessary for their officially assigned duties. Information may only be released per unit-specific guidelines and in line with applicable College policies on information confidentiality and access.

Systems for information management must have controls in place to trace security violations to individuals, who will be held accountable for their actions. Employees attempting unauthorized access to administrative data are subject to disciplinary actions as outlined in College policies.

Supervisor Responsibilities:

1. Conduct regular reviews of access permissions for their staff.
2. Ensure secure handling of administrative information by staff at the close of the workday.
3. Develop and enforce access security procedures, including educating staff on security protocols.

B. Responsibilities of Authorized Users

All authorized users granted access to information must adhere to the following:

1. Unauthorized use or distribution of information is prohibited.
2. Verification of recipient identity is required before discussing individual-specific information.
3. Non-public institutional information must not be used for personal, financial, or malicious purposes.
4. Information must not be obstructed from legitimate institutional use.

C. Handling of Confidential Information

Unauthorized access or disclosure of confidential information is strictly prohibited and may be in violation of local, state, or federal laws.

Guidelines for Confidential Data Management:

1. Computer screens should be positioned to prevent unauthorized viewing.
2. Printed output containing sensitive information must be managed with the same caution as digital data files.
3. External storage devices (USB drives, external hard drives, etc.) containing sensitive information should be securely stored in locked areas.
4. Non-electronic records of administrative data must be protected against unauthorized access, accidental loss, or environmental damage.

D. Disposal of Confidential Information

All paper and microfiche documents containing sensitive or confidential information must be destroyed via shredding or incineration to prevent unauthorized access.

Proper disposal of digital media (hard drives, USB drives) with administrative or confidential data should be conducted according to secure erasure procedures available through the College's IT Office.

E. Data Integrity

Maintaining data integrity is essential. This will be achieved through adherence to proper database maintenance protocols and timely software updates. Testing standards must clearly differentiate between test and production data, ensuring new procedures are tested in a controlled environment before going live.

Employees are responsible for protecting the integrity, accuracy, and confidentiality of all data they handle.

F. Backup and Storage

Data should be protected against loss through regular backups onto secure, removable media. Data centers must have weatherproof and fireproof storage for critical backup media to ensure durability and availability in emergencies.

See Board Policy 8300