COLLEGE OF MICRONESIA-FSM
ADMINISTRATIVE PROCEDURE No. 8500

Improper Use of College IT Resources

Date Adopted:	21 May 2002
Date Revised:	11 December 2009
Date Reviewed:	28 May 2014, 30 May 2025
References:	ISO/IEC 27001 Information Security Management (as a guiding standard), FSM Cybersecurity Policy

Purpose

To provide procedural guidance for investigating and responding to the improper use of College information technology (IT) resources in alignment with Board Policy No. 8500.

Procedure

1. **Identification and Preliminary Assessment**
   - If a potential violation or misuse is reported or detected, the responsible unit supervisor or system administrator will conduct a preliminary assessment to determine if further action is required.
2. **Notification**
   - The individual(s) involved will be notified in writing or via official College email of the nature of the concern and that an investigation is being initiated.
3. **Investigation Process**
   - Copies of relevant system logs, files, or communications may be made for investigation purposes.
   - The user's data will be examined in a manner consistent with the principle of minimal necessary access and with respect for privacy.
4. **Temporary Access Restriction**
   - If deemed necessary to prevent further risk or misuse, the responsible supervisor may temporarily restrict the individual's access to IT resources. This action must be documented and communicated promptly to the affected individual(s).

5. **Reporting and Review**
   - Findings of the investigation will be reported to the Division Chair, Director of Information Technology, and the Chair of the Information and Communication Technology Committee (ICTC).
   - If no violation is confirmed, all investigative copies will be securely destroyed, and the individual will be informed accordingly.
6. **Corrective or Disciplinary Action**
   - If a violation is confirmed, appropriate disciplinary measures will be taken in accordance with College policies. These may include written warnings, access restrictions, suspension of privileges, or further personnel action.
7. **Scope of Application**
   - This procedure applies to all College IT systems including, but not limited to, cloud services, email systems, collaboration platforms, remote and mobile access, and online learning environments.

See Board Policy 8500