COLLEGE OF MICRONESIA-FSM

BOARD POLICY No. 8900

Cybersecurity

Date Approved: 09-11 June 2026

Date Revised: 09-11 June 2026

Date Reviewed: 09-11 June 2026

Reference: NIST Cybersecurity Framework, ISO/IEC 27001, EDUCAUSE Security Guide, FSA, Australian Cyber Security Centre, University of Colorado Colorado Springs, Dakota State University, Carnegie Mellon University, University of Auckland

1. **Purpose**
   This policy establishes the framework for protecting the information systems, networks, and digital resources of the College of Micronesia–Federated States of Micronesia (COM-FSM). It ensures the confidentiality, integrity, and availability of College data and supports the secure delivery of academic and administrative services.

2. **Scope**
   This policy applies to all faculty, staff, students, contractors, and third-party vendors who access or use COM-FSM information systems. It covers all College technology resources, including networks, servers, cloud platforms, email systems, learning management systems, student information systems, and college-owned devices.

3. **Policy Statement**
   COM-FSM is committed to maintaining a secure and resilient technology environment. All users are responsible for safeguarding College systems and data and must comply with established cybersecurity practices and procedures.

4. **Roles and Responsibilities**
   a. Cybersecurity is a shared responsibility across the college.

      i. **Information Technology Office**
      The Information Technology Office is responsible for implementing and maintaining cybersecurity controls, monitoring systems, managing risks, and responding to cybersecurity incidents.

ii. **Faculty, Staff, and Students**
All users must:

- Protect their login credentials
- Use systems responsibly
- Report suspected cybersecurity incidents promptly

iii. **Third-Party Vendors**
Vendors must comply with COM-FSM cybersecurity requirements and protect College systems and data.

5. **Core Security Principles**
   a. COM-FSM will implement and maintain controls to:

      i. Protect institutional data from unauthorized access or disclosure
      ii. Secure systems and networks from threats
      iii. Control and manage user access
      iv. Ensure appropriate use of institutional technology resources
      v. Detect and respond to cybersecurity incidents
      vi. Maintain continuity of critical systems

6. **Acceptable Use**
College technology resources must be used for legitimate academic, administrative, and operational purposes.

Unauthorized software installation is prohibited. All software must be approved and, where applicable, registered with the Information Technology Office. College employees with administrative access must coordinate with IT prior to installing software.

Non-educational software, including games, is not permitted unless approved for academic use. Software that promotes violence, contains pornographic material, or is otherwise inappropriate is strictly prohibited.

Violations may result in disciplinary action, including suspension of system access.

7. **Cybersecurity Incident Reporting**
   a. All suspected cybersecurity incidents must be reported immediately to the Information Technology Office. Examples of reportable incidents include:

      I. Suspicious emails or phishing attempts
      II. Malware infections
      III. Unauthorized system access

IV. Data breaches or data exposure
V. Lost or stolen devices containing College data

b. The College will follow the procedures outlined in the **COM-FSM Cybersecurity Incident Response Plan** when responding to cybersecurity incidents.

8. Cybersecurity Awareness and Training

The College will promote cybersecurity awareness through training and communication to ensure users understand their responsibilities.

9. Compliance

Failure to comply with this policy may result in disciplinary action in accordance with College policies and procedures.

Violations may also lead to suspension of system access or other corrective actions.

See Administrative Procedure No. 8900