**Computing Resources**

**Date Adopted:** 21 May 2002
**Date Revised:** 11 December 2009
**Date Reviewed:** [Latest Review Date]
**References:** Library Bill of Rights, Lab Conduct and Responsibilities, FSM Data Protection Regulations, ISO 27001 Compliance

### **A. Definition**

Computing resources include all hardware, software, network infrastructure, cloud-based services, and collaboration platforms provided by the College of Micronesia-FSM. This includes on-campus servers, cloud-based applications (e.g., Google Workspace), internet access, and virtual machines.

### **B. General Use**

The computing resources of the College of Micronesia-FSM are provided primarily for academic, research, and administrative purposes. Users must adhere to responsible and ethical use policies. Prohibited activities include:

* Using computing resources for commercial purposes without explicit institutional approval.
* Violating international copyright laws.
* Monopolizing shared resources, such as bandwidth and computing power.

School-related work has priority over personal use. If required, non-academic users may be asked to relinquish access.

### **C. Security and Compliance**

* Users must not attempt to circumvent, defeat, or subvert security measures.
* Unauthorized access to restricted systems is strictly prohibited.
* Multi-factor authentication (MFA) is required for access to critical systems.
* The College reserves the right to monitor network activity for compliance and security purposes.

### **D. Learning Resources Center (LRC)**

* The LRC provides open access to computing resources for academic research and coursework.
* Users must demonstrate competency in basic computing through training or certification.
* Only academic and educational research is permitted on LRC computers.
* External storage devices must be scanned for malware before use.

### **E. Classroom and Business Labs**

* Computer labs are for instructional and research purposes.
* Business computer labs require prior approval for non-instructional use.
* Software installations must be authorized by IT staff.

### **F. Network and IT Infrastructure**

* Personal devices may connect to the network but must adhere to security policies.
* Running unauthorized servers or using institutional networks for illegal activities is prohibited.
* IT staff will perform periodic security audits and software updates.
* Remote access is permitted only through an institution-approved VPN.

**See Administrative Procedure 8200 for additional details.**