TECHNICAL SAFEGUARDS SUMMARY

Dhiraj Bhartu
COLLEGE OF MICRONESIA-FSM

Table of Contents

TECHNICAL SAFEGUARDS SUMMARY

SECTION 1: COM-FSM TECHNICAL AND ADMINISTRATIVE SAFEGUARDS

This document summarizes the administrative, technical, and operational safeguards implemented by the College of Micronesia-FSM to protect customer information and non-public personal information (NPI) in accordance with the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule (16 CFR Part 314.4).

The safeguards described herein support the College's Written Information Security Program and demonstrate implementation of controls related to access management, data protection, monitoring, incident response, and ongoing cybersecurity oversight.

1. **User Authentication**
   - Systems require unique user IDs and passwords
   - Password controls are enforced across institutional systems (email, Moodle, administrative systems)
   - Default passwords are changed upon first login
   - Passwords must meet minimum complexity requirements

2. **Access Control and Permissions**
   - Role-based access control is implemented across systems
   - Access is granted based on job responsibilities (least privilege principle)
   - Administrative access is restricted to authorized IT personnel
   - Periodic reviews of user access are conducted

3. **Account Provisioning and Deactivation**
   - User accounts are created based on authorized requests from HR or department heads
   - Access is modified when roles change
   - Accounts are disabled upon employee separation or inactivity

4. **System Monitoring Practices**
   - System logs are generated for authentication and administrative activities
   - IT staff monitor logs periodically for unusual activity
   - Security updates and patches are applied regularly

5. **Network and Infrastructure Security**
   - Firewalls are in place to protect institutional networks
   - Anti-virus and endpoint protection are deployed on institutional devices
   - Network access is restricted and monitored

6. **Data Protection Measures**
   a) **Data Inventory and Classification**
      - The College maintains awareness of systems containing student, employee, financial aid, and institutional information
      - Institutional systems containing sensitive information are identified and reviewed periodically by IT personnel and relevant operational offices
      - Sensitive institutional data includes student academic records, financial aid information, employee records, and institutional financial information
      - Data is maintained within authorized institutional systems and environments
   - Data in transit is protected using secure protocols (HTTPS, TLS)
   - Institutional systems are hosted in secure environments
   - Backups are performed regularly to ensure data recovery

7. **Multi-Factor Authentication (MFA)**
   a) **Secure Disposal of Information**
      - User accounts are disabled when no longer required
      - Obsolete devices and storage media are securely wiped, reimaged, or physically disposed of prior to reassignment or disposal
      - Physical records containing sensitive information are disposed of using secure disposal practices where applicables
   - MFA is currently implemented for selected systems (e.g., email and where applicable)
   - The College is actively evaluating expanded MFA implementation across critical systems

8. **Vulnerability and Security Assessment**
   a) **System Change Management and Security Review**
      - System updates, infrastructure modifications, and application changes are reviewed by IT personnel prior to implementation
      - Security patches and software updates are applied periodically to reduce operational and cybersecurity risks
      - The College evaluates opportunities to strengthen security controls based on operational experience, emerging threats, and institutional technology changes

   Physical records containing sensitive information are disposed of using secure disposal practices where applicables
   - The College maintains system updates and patch management practices
   - Formal vulnerability assessment and penetration testing are under evaluation as part of ongoing cybersecurity improvements

SECTION 2: COM-FSM CRITICAL SYSTEMS INVENTORY

System	Owner	Data Type	Location
Student Information System (SIS)	Registrar / IT	Student records, academic data	On-premise server
Moodle LMS	IT Department	Course data, student submissions	On-premise server
Email System	IT Department	Institutional communications	Cloud
Financial System	Business Office	Financial and payroll data	On-premise
HR System	Human Resources	Employee data	On-premise
Network Infrastructure	IT Department	Institutional network traffic	Campus-wide

These systems contain or process sensitive institutional data and are subject to security safeguards under the College's Information Security Program.

SECTION 3: COM-FSM SYSTEM MONITORING & OVERSIGHT

The College maintains monitoring practices to ensure the security and integrity of its information systems.

- System logs are generated and retained for key systems
- IT personnel review logs periodically to identify unusual or unauthorized activity
- Administrative actions are logged and monitored
- System performance and security updates are regularly reviewed
- Network monitoring tools are used to observe traffic and detect anomalies

SECTION 4: INCIDENT RESPONSE PRACTICES

The College follows structured procedures for responding to cybersecurity incidents.

- Detection - Incidents may be identified through system alerts, user reports, or IT monitoring.
- Containment - Affected systems are isolated to prevent further impact.
- Investigation - IT staff assesses the scope, cause, and potential data exposure.
- Notification - Relevant stakeholders, including leadership, are informed. External notifications are made where required.
- Recovery - Systems are restored using secure backups and verified for integrity.
- Review - Post-incident analysis is conducted to improve controls and prevent recurrence.

SECTION 5: SECURITY AWARENESS AND TRAINING

The College promotes employee awareness regarding the protection of institutional and customer information through operational guidance, onboarding practices, and periodic communications.

Security awareness topics include:

- Password security and account protection
- Appropriate handling of sensitive information
- Phishing and suspicious email awareness
- Acceptable use of institutional systems
- Reporting suspected cybersecurity incidents

Relevant guidance and operational communications are maintained by responsible offices and IT personnel.

SECTION 6: SERVICE PROVIDER AND VENDOR OVERSIGHT

The College utilizes third-party service providers and technology vendors that support institutional operations and information systems. The College evaluates vendor services and operational security considerations as part of procurement, implementation, and ongoing operational oversight where applicable.

Examples of supported services may include:

- Cloud-based email services
- Financial and HR systems

The College expects service providers handling institutional information to maintain appropriate safeguards to protect sensitive data.

Relevant guidance and operational communications are maintained by responsible offices and IT personnel.

SECTION 7: EVALUATION AND CONTINUOUS IMPROVEMENT

The College recognizes cybersecurity as an ongoing operational responsibility and periodically evaluates the effectiveness of its safeguards and security practices.

The Information Security Program may be adjusted based on:

- Operational reviews and monitoring activities
- Changes to institutional systems or infrastructure
- Emerging cybersecurity risks and threats
- Security incidents or operational observations
- Recommendations from audits, assessments, or compliance reviews

The College continues to evaluate enhancements including expanded multi-factor authentication, vulnerability assessment practices, and additional cybersecurity governance measures.