CYBERSECURITY INCIDENT RESPONSE PLAN

Responsible Office: Information Technology Office
Effective Date: Version: 1.0

Dhiraj Bhartu
COLLEGE OF MICRONESIA-FSM

Table of Contents

Purpose

The purpose of this Cybersecurity Incident Response Plan is to establish a structured and coordinated approach for responding to cybersecurity incidents that may affect the information systems, networks, and digital services of the College of Micronesia–FSM (COM-FSM).

This plan ensures that the College can:

- Detect cybersecurity incidents quickly
- Contain and mitigate threats effectively
- Restore affected systems and services
- Protect institutional data and technology assets
- Maintain continuity of academic and administrative operations

Scope

This plan applies to all information technology systems and digital resources owned, operated, or managed by COM-FSM, including:

- Institutional networks across all campuses
- Servers and data centers
- Cloud services and hosted platforms
- Student Information Systems
- Learning Management Systems
- Email and collaboration platforms
- Administrative and financial systems
- College-owned computers and mobile devices
- Third-party systems connected to the COM-FSM network

This plan applies to:

- Faculty
- Staff
- IT personnel
- Contractors
- Vendors with access to institutional systems

Objectives

The objectives of this Cybersecurity Incident Response Plan are to:

1. Protect the **confidentiality, integrity, and availability** of institutional data and systems.
2. Provide a **standardized process** for responding to cybersecurity incidents.
3. Minimize disruption to **academic, research, and administrative operations**.
4. Protect **student, employee, and institutional information**.
5. Ensure **timely communication and escalation** during cybersecurity incidents.
6. Strengthen institutional resilience through **continuous improvement and lessons learned**.

Definitions of Key Terms

For purposes of this Plan, the following terms apply:

- **Cybersecurity Incident:** An event that threatens the confidentiality, integrity, or availability of COM-FSM information systems, networks, or data.
- **Security Event:** An observable occurrence on a system or network that may indicate a security issue but may not meet the threshold of an incident.
- **Data Breach:** Unauthorized access, disclosure, loss, or acquisition of sensitive institutional, student, or employee information.
- **Unauthorized Access:** Access to systems, accounts, networks, or data without approval or beyond granted privileges.
- **Malware:** Malicious software intended to disrupt operations or gain unauthorized access (e.g., viruses, ransomware, spyware).
- **Phishing:** Fraudulent messages designed to trick users into revealing credentials or opening malicious content.
- **Critical System:** A system essential to academic or administrative operations (e.g., SIS, LMS, email, financial platforms, core network services).
- **Containment:** Actions taken to limit the spread or impact of an incident.
- **Eradication:** Removal of the root cause of an incident (e.g., malware removal, disabling compromised accounts, patching vulnerabilities).
- **Recovery:** Restoring affected services, systems, and data to normal operation and validating they are stable and secure.

Cybersecurity Incident Response Team (CSIRT)

The College will maintain a Cybersecurity Incident Response Team responsible for managing and coordinating responses to cybersecurity incidents.

Core Members

Role	Primary Responsibilities
Director of Information Technology	Incident Response Lead; authorizes major containment actions; coordinates with senior administration; ensures documentation and post-incident review.
Network Administrator	Network monitoring, containment, and traffic controls (firewalls, blocks, segmentation); supports incident evidence collection related to network activity.
Systems / Server Administrator	Supports eradication and recovery for servers, core services, backups, and authentication systems; applies patches and configuration fixes.
Service Desk / IT Support Representative	Receives and records reports; guides users on immediate actions; supports endpoint isolation, password resets, and incident ticket tracking.
Communications Representative	Coordinates internal and external communications as authorized; prepares notices and status updates; supports stakeholder messaging.
Senior Administration Representative	Executive decision making for high/critical incidents; approves business-impacting actions; supports external notifications when required.
Legal / Compliance Advisor (as needed)	Advises on breach notification obligations, records retention, and coordination with authorities; reviews external communications where appropriate.

Additional personnel may be involved depending on the nature and severity of the incident.

Types of Cybersecurity Incidents

Cybersecurity incidents at COM-FSM include any event that threatens the confidentiality, integrity, or availability of institutional systems or data. These may involve malware infections, phishing attempts, unauthorized access, system outages, data breaches, or compromise of network infrastructure. Incidents can affect critical systems such as the Student Information System, Learning Management System, email services, administrative platforms, and campus networks.

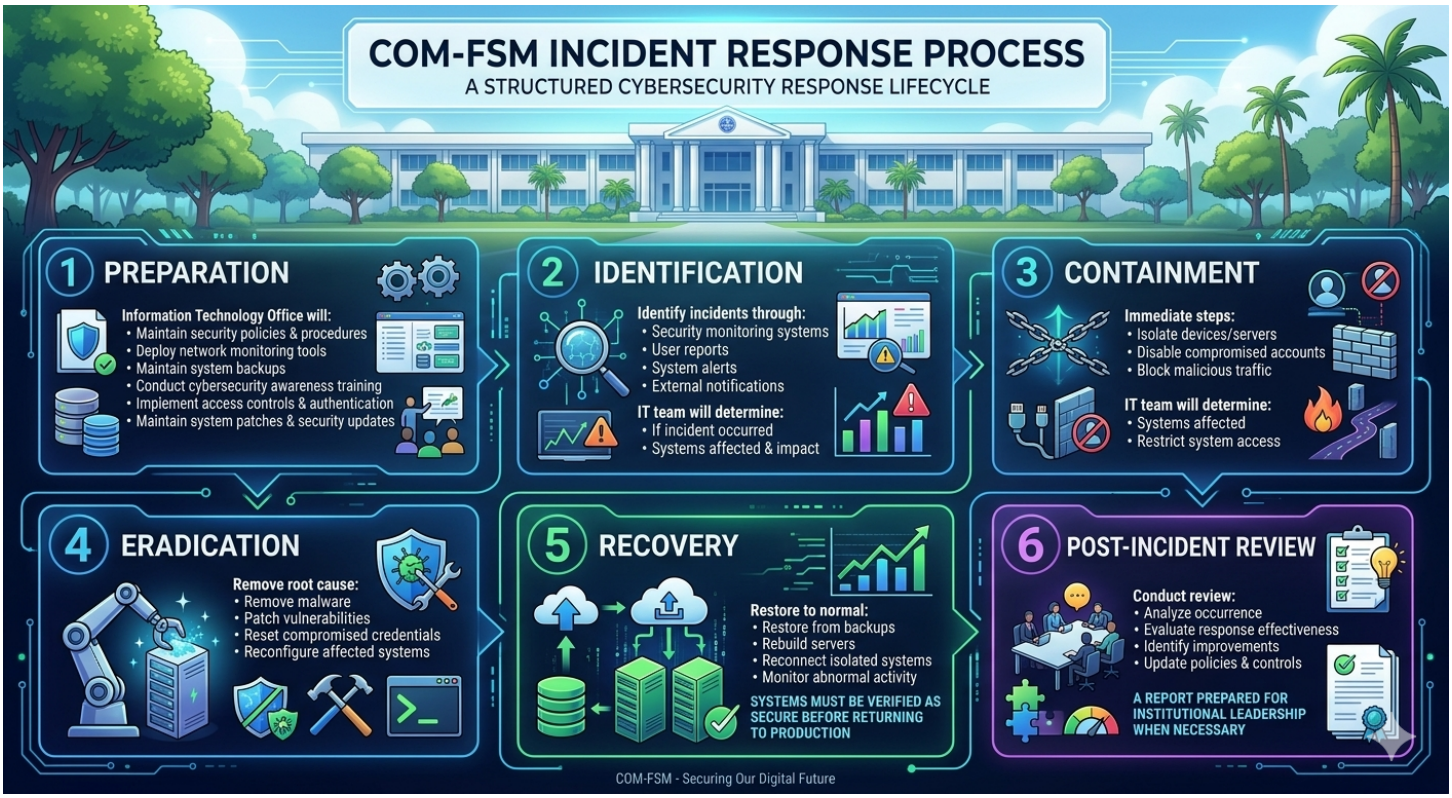
Incident Severity Levels

Incident severity is used to prioritize response actions, resources, and escalation. Severity is determined by operational impact, data sensitivity, scope (single user vs. multiple campuses), and whether mission-critical systems are affected.

Level	Criteria / Examples	Typical Response
Low	Single user/device; minimal impact; no evidence of sensitive data exposure (e.g., blocked phishing email, minor malware detection contained by antivirus).	IT handles during normal operations; document and close with user guidance.
Medium	Limited spread; departmental impact; suspected account compromise; repeated phishing; localized service degradation.	Accelerated response; containment steps (password resets, isolation); CSIRT lead informed.
High	Significant disruption; multiple systems/users affected; confirmed compromise of administrative accounts; outage of critical services (SIS/LMS/email) for extended periods; credible indication of sensitive data exposure.	Immediate coordinated response; activate CSIRT; escalate to senior administration; consider external specialists and service providers.
Critical	College-wide impact; multi-campus network compromise; ransomware impacting mission-critical systems;	Full incident response activation; executive oversight; coordinated

	confirmed major data breach; legal/regulatory implications.	communications; engage external response support and notify authorities if required.

Incident Response Process



The incident response process provides a structured approach for identifying, containing, mitigating, and resolving cybersecurity threats at COM-FSM. The Information Technology Office leads this process, supported by the Cybersecurity Incident Response Team (CSIRT). The process includes detecting incidents, reporting them promptly, assessing severity, implementing containment measures, restoring affected systems, documenting actions taken, and reviewing lessons learned to improve future responses.

Incident Reporting

All faculty, staff, and students must report suspected cybersecurity incidents immediately.

Reports should include:

- Description of the issue
- Date and time observed
- System or device affected
- Any actions already taken

Reports can be submitted through:

- IT Helpdesk
- Email to the Information Technology Office
- Direct communication with IT staff

Communication and Escalation

For significant incidents, communication may involve:

- Senior Administration
- Campus leadership
- External cybersecurity specialists
- Internet service providers
- Government authorities if required

Public communication regarding cybersecurity incidents will be coordinated by authorized institutional leadership.

Documentation and Record Keeping

All cybersecurity incidents must be documented by the Information Technology Office.

Documentation will include:

- Incident description
- Timeline of events
- Systems affected
- Actions taken
- Resolution details
- Lessons learned

Records will be securely maintained for institutional reference and future improvements.

Continuous Improvement

The Cybersecurity Incident Response Plan will be reviewed periodically to ensure effectiveness.

Updates may occur due to:

- Changes in technology infrastructure
- Emerging cybersecurity threats
- Lessons learned from past incidents
- Institutional policy updates

Appendix A: COM-FSM Campus Network Infrastructure

The College of Micronesia–FSM operates a distributed network infrastructure across multiple campuses within the Federated States of Micronesia. The Information Technology Office manages connectivity, systems, and cybersecurity protections across these locations.

Primary Campuses

Campus	Location	Description
National Campus	Pohnpei	Main administrative and academic campus hosting core institutional systems
Chuuk Campus	Chuuk State	Regional campus providing academic and student services
Kosrae Campus	Kosrae State	Regional campus providing academic and student services
Yap Campus	Yap State	Regional campus providing academic and student services
FMI Campus	Yap State	Fisheries and Maritime Institute
CTEC Campus	Pohnpei	College of Micronesia Career & Technical Education Center

Network Management Responsibilities

The Information Technology Office is responsible for:

- Campus network connectivity
- Internet service management
- Server and system administration
- Network security monitoring
- Incident detection and response
- Infrastructure upgrades and maintenance

Network infrastructure may include:

- Core switches and distribution switches
- Wireless access points
- Gateway servers
- Firewalls
- Authentication services
- VPN services
- Internet gateways

Appendix B: Internet Connectivity

Reliable internet connectivity is essential for academic delivery, institutional administration, and digital learning platforms.

Primary Internet Connectivity

COM-FSM campuses may utilize a combination of connectivity solutions including:

- **Satellite Internet (Starlink)**
- **Local telecommunications providers**
- **Campus gateway servers**
- **Network load balancing or failover systems**

Connectivity Security Considerations

To protect institutional networks, the Information Technology Office implements:

- Network firewalls
- Traffic monitoring
- Intrusion detection
- Access controls
- Secure gateway configurations

In the event of a cybersecurity incident involving internet connectivity, IT staff may:

- Temporarily isolate affected networks
- Restrict external access
- Block malicious traffic
- Coordinate with service providers for mitigation

Appendix C: Critical Institutional Systems

Certain systems are considered **mission-critical** to the operation of the College of Micronesia–FSM. Cybersecurity incidents affecting these systems require **priority response and escalation**.

Student Information System (SIS)

The SIS manages essential academic and administrative records including:

- Student registration
- Enrollment records
- Academic transcripts
- Student billing
- Institutional reporting

Protection of student data is a **high institutional priority**.

Learning Management System (LMS)

The LMS supports digital learning across the institution.

- **Moodle**

The LMS supports:

- Course delivery
- Online learning
- Assignment submissions
- Student assessment
- Faculty communication

Disruption to the LMS can significantly impact academic continuity.

Email and Collaboration Systems

Institutional email and collaboration platforms support communication across the College.

These systems may include:

- Institutional email accounts
- Calendar and scheduling services
- Document collaboration platforms
- Video conferencing systems

Email systems are common targets for:

- Phishing attacks
- Account compromise
- Malware distribution

Financial and Administrative Systems

Financial and administrative platforms support institutional operations including:

- Payroll
- Accounting
- Procurement
- Budget management
- Human resources systems

These systems contain sensitive institutional data and must be protected from unauthorized access.

Network Infrastructure Systems

The following infrastructure components are essential to institutional operations:

- Network authentication systems
- Gateway servers
- Firewalls
- Network switches and routers
- Wireless access infrastructure
- Backup and storage systems

Failure or compromise of these systems may affect **multiple campuses simultaneously**.

Appendix D: Cyber Incident Reporting Form

All suspected cybersecurity incidents should be documented using the following template.

Cybersecurity Incident Report

Date Reported:
Reported By:
Department / Campus:

Contact Email / Phone:

Incident Details

Date and Time Incident Detected:

Location (Campus / Building / Office):

System or Device Affected:

Type of Incident (Check if applicable):

☐ Phishing Email
☐ Malware / Virus
☐ Ransomware
☐ Unauthorized Access
☐ Lost / Stolen Device
☐ System Outage
☐ Data Breach
☐ Other: _____

Description of Incident

Provide a brief description of what happened:

Actions Already Taken

☐ Device disconnected from network
☐ Password changed
☐ IT Helpdesk contacted
☐ No action taken

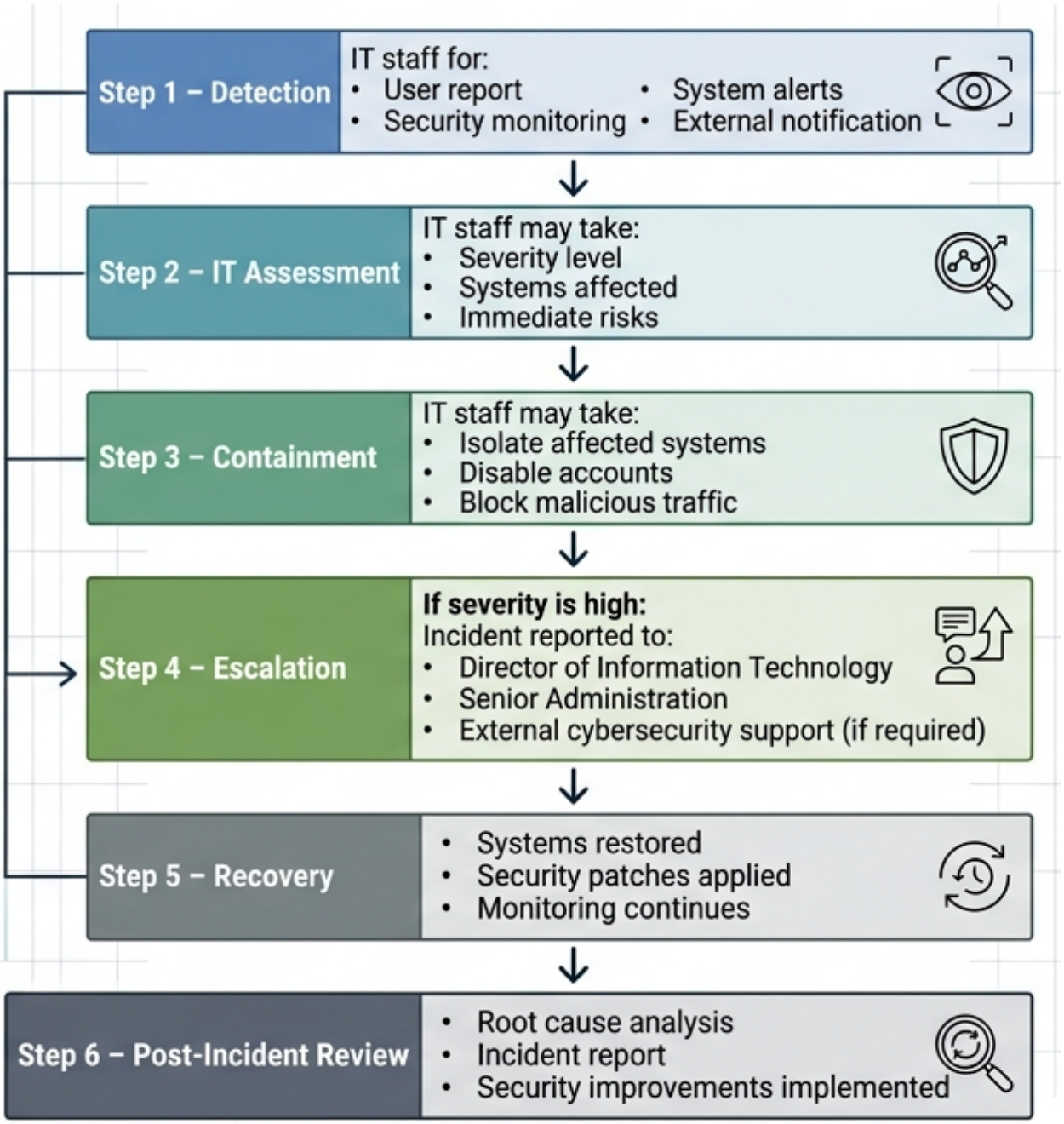
Additional Notes:

Attachments (if available)

☐ Screenshot
☐ Suspicious Email
☐ Log File

Submit this report to the **COM-FSM Information Technology Office immediately**.

Appendix E: Cybersecurity Incident Escalation Flow



Appendix F: Cybersecurity Incident Severity Matrix

This matrix helps the Information Technology Office quickly classify incidents and determine the appropriate response level.

Severity Level	Description	Examples	Response Time	Escalation
Low (Level 1)	Minor security event with minimal risk and limited impact to a single user or device.	Single malware infection, blocked phishing email, minor login anomaly.	Within 24 hours	IT Support Team
Medium (Level 2)	Incident affecting multiple users or systems but without confirmed data breach or major service disruption.	Multiple compromised accounts, malware spreading across departments, localized system outages.	Within 4 hours	Director of IT notified
High (Level 3)	Serious incident affecting critical systems or potentially exposing sensitive institutional data.	SIS compromise, LMS disruption, network intrusion, unauthorized database access.	Immediate response	Director of IT + Senior Administration
Critical (Level 4)	Institutional emergency impacting multiple campuses or major services. Potential legal or reputational impact.	Ransomware attack, large data breach, campus-wide system outage, DDoS attack.	Immediate response (within 1 hour)	President / Executive Leadership notified

Priority Systems

Incidents involving the following systems should automatically be considered **High or Critical severity**:

- Student Information System (SIS)
- Learning Management System (Canvas/Moodle)
- Email systems
- Financial systems
- Campus network gateways
- Authentication systems

Appendix G: Ransomware Response Playbook

Ransomware attacks are among the most serious cybersecurity threats facing higher education institutions.

If ransomware is suspected, the following procedures must be followed immediately.

Step 1: Identify Signs of Ransomware

Indicators may include:

1. Files suddenly encrypted or inaccessible
2. Ransom message displayed on screen
3. Rapid file renaming or file extensions changed
4. Unusual network activity

Step 2: Immediate Containment

IT staff should:

1. Disconnect affected systems from the network immediately
2. Disable shared drives
3. Block network communication from infected machines
4. Prevent further spread across campuses

Step 3: Preserve Evidence

Do **not immediately wipe systems**.

Instead:

1. Capture system logs
2. Document ransom messages
3. Record affected systems
4. Preserve evidence for investigation

Step 4: Notify Leadership

Notify immediately:

1. Director of Information Technology
2. Senior Administration
3. Institutional leadership if multiple systems are affected

Step 5: Assess Impact

Determine:

1. Number of systems affected
2. Whether backups are available
3. Whether critical systems are compromised

Step 6: System Recovery

Preferred recovery method:

1. Restore systems from secure backups
2. Rebuild affected servers if necessary
3. Reset all compromised credentials

Step 7: Security Hardening

After recovery:

1. Patch vulnerabilities
2. Strengthen authentication controls
3. Review access permissions
4. Conduct security review