MUS Information Security Incident Response Flowchart

Campus Incident Handler

Evaluate Incident → Routine No Special Handling → New facts? → Routine Close

Evaluate Incident → Security Triage → Routine No Special Handling

CIO (MSU/UM)

Potentially Significant Incident → Confirm Significant Incident

Incident Response Team

Communication through emails, telephone calls, texts, etc.

Add Legal, Risk & Compliance, Risk Manager, RMTD and others to IRT

RMTD Forensics

Cross Functional Incident Response Coordination

Detection & Analysis | Containment, Eradication & Recovery | Post Incident Activity

RMTD cyber insurance | Notification Plan & Vendor Choice | Regulatory Legal Requirements

Lessons Learned, Update Risk Assessments, Plan Corrective Actions → Close

Executive Leadership

President

Deputy Commissioner for Budget & PLanning/CHE

Plan & Execute Management Response | Law Enforcement?

Plan & Execute Communication Internal/External

Supporting Functions

General Counsel, Risk Management

Complete RMTD 'Report of Incident' form w/ in 2 days

RMTD cyber insurance | Notification Plan & Vendor Choice | Regulatory Legal Requirements