Security Event Response and Recovery Plan

MMF Consulting Grp (Pte. Ltd.)

October 2024

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.1, CC7.4, CC7.5

Table 2: Document history

Date	Comment
Oct 15 2024	Initial document
Nov 30 2024	Policy updates and improvements

1 Security Event Response and Recovery Plan

Field	Value
ID	INCP-002
Effective Date	October 15, 2024
Last Revised	November 30, 2024
Department	Information Security
Approval	Minny Wang, Director

1.1 Purpose and Scope

This Security Event Response and Recovery Plan establishes procedures for detecting, responding to, and recovering from security incidents that may affect MMF Consulting Grp (Pte. Ltd.) systems, data, or operations. This plan applies to all employees and covers incidents involving company systems, client data, or business operations.

1.2 Background

As a compliance consulting firm handling sensitive client financial data, contracts, and vendor information, MMF Consulting Grp (Pte. Ltd.) must respond rapidly and effectively to security incidents to minimize impact on clients and business operations. This plan ensures coordinated response with clear roles, timelines, and communication protocols while meeting regulatory notification requirements.

1.3 Policy

1.3.1 Incident Classification and Response Teams

1.3.1.1 Incident Categories

- **Data Breach**: Unauthorized access to client or company confidential data
- **System Compromise**: Malware, unauthorized access, or system integrity issues
- **Service Disruption**: Outages affecting Microsoft 365, Box.com, or critical business systems
- **Physical Security**: Unauthorized access to offices, theft, or physical damage
- **Personnel Incidents**: Insider threats, social engineering, or credential compromise

1.3.1.2 Response Team Structure

- **Incident Commander**: Director (Minny Wang) - Ultimate decision authority, client communication
- **Technical Lead**: System Administrator (Yusheng Li) - Technical response, forensics, recovery
- **Legal/HR Coordinator**: HR/Legal Representative (Kelly Lee) - Regulatory compliance, personnel issues
- **24/7 On-Call**: Director and System Administrator maintain 24/7 availability

1.3.2 Incident Response Procedures

1.3.2.1 Phase 1: Detection and Initial Response (0-2 Hours)

1. **Immediate Actions**:
    - Preserve evidence and document initial findings
    - Isolate affected systems if safe to do so

- Notify System Administrator immediately
- Begin incident log with timestamps and actions taken

2. **Assessment and Classification**:
   - Determine incident type and severity level
   - Identify affected systems, data, and potential client impact
   - Activate appropriate response team members
   - Establish secure communication channel (Teams, phone)

1.3.2.2 Phase 2: Containment and Investigation (2-24 Hours)

1. **Containment Strategies**:
   - Isolate affected systems to prevent incident spread
   - Disable compromised accounts and reset credentials
   - Engage vendor support for cloud service incidents
   - Implement temporary workarounds to maintain business operations
2. **Evidence Collection**:
   - Capture system logs (Microsoft Entra, Box.com, endpoint logs)
   - Document user activities and access patterns
   - Preserve forensic images if required
   - Interview affected personnel

1.3.2.3 Phase 3: Communication and Notification (3-72 Hours)

1. **Internal Communication**:
   - All employees notified within 3 business days
   - Status updates every 24 hours during active response
   - Detailed briefings for management team
2. **Client Notification** (When Required):
   - **Data Breach**: Notify affected clients within 72 hours
   - **Service Impact**: Immediate notification for audit deadline impacts
   - **Regulatory Reporting**: Submit required notifications per applicable regulations

1.3.2.4 Phase 4: Recovery and Return to Normal Operations

1. **System Restoration**:
   - Verify system integrity before bringing back online
   - Test all security controls and monitoring systems
   - Restore data from verified clean backups if necessary
   - Update security configurations based on incident findings
2. **Monitoring Enhancement**:
   - Increase monitoring for 30 days post-incident
   - Review and update security controls
   - Implement additional preventive measures

1.3.2.5 Phase 5: Post-Incident Review and Lessons Learned

1. **Incident Analysis**:
   - Root cause analysis within 30 days
   - Timeline reconstruction and decision review
   - Cost and impact assessment
   - Documentation of lessons learned
2. **Process Improvement**:

- Update incident response procedures
- Enhance detection capabilities
- Modify security controls based on findings
- Conduct additional training if needed

1.3.3 Emergency Contacts and Escalation

1.3.3.1 Primary Contacts (24/7 Availability)

- **Director**: Minny Wang - [Contact Information]
- **System Administrator**: Yusheng Li - [Contact Information]
- **HR/Legal**: Kelly Lee - [Contact Information]

1.3.3.2 External Support Resources

- **Vendor Support**: Premier support agreements for cloud service incidents
- **Legal Counsel**: External legal support for regulatory matters
- **Cyber Insurance**: Contact carrier for significant incidents

1.3.4 Incident Documentation Requirements

- **Incident Report**: Complete within 48 hours of resolution
- **Timeline Documentation**: All actions with timestamps
- **Communication Log**: All internal and external communications
- **Evidence Preservation**: Secure storage for potential legal proceedings
- **Impact Assessment**: Document any client data, service, or operational impacts

1.4 Policy Review and Maintenance

This policy is subject to annual review and update by the System Administrator and Director.

1.5 Exceptions

All exceptions to this policy require written approval from the Director, accompanied by documented business justification and formal risk assessment. Exception requests must demonstrate that alternative controls provide equivalent security protection or that the business risk is acceptable given operational requirements. Approved exceptions include specific monitoring provisions and regular review schedules.

1.6 Violations & Enforcement

Violations of this policy are subject to disciplinary action commensurate with the severity of the breach and its potential impact on organizational security. Enforcement measures may include mandatory retraining, formal reprimands, or termination of employment, depending on the nature and frequency of violations. Failure to report security incidents or deliberate concealment of incidents may result in immediate termination and potential legal action.

2 Authorship and Approval

Last edit made by Bill Li (yushengli.tw@gmail.com) on Mon, 18 Aug 2025 18:37:06 +0800.

Approved by Yusheng Li (YushengLi@users.noreply.github.com) on Thu, 21 Aug 2025 11:54:21 +0800 in commit 8e0c1296a6a80185ef11d1631bbf6ca59ccc896b.