Incident Response Plan for Mozart ltd

1. Purpose

This Incident Response Plan (IRP) establishes a framework for Mozart ltd to effectively detect, respond to, and recover from cybersecurity incidents. As a B2B software company handling Personally Identifiable Information (PII), our ability to respond swiftly and effectively to security incidents is crucial for maintaining client trust, business continuity, and compliance with applicable regulations.
The plan outlines roles, responsibilities, and procedures to ensure a coordinated response to security events, minimizing potential damage, reducing recovery time, and preventing similar incidents in the future. This document serves as a guide for all Mozart ltd employees, particularly those designated as part of the Incident Response Team.

2. Scope

This Incident Response Plan applies to all Mozart ltd information systems, data assets, cloud services, and SaaS applications used by our remote workforce, including but not limited to our cloud-hosted customer-facing applications, communication platforms (Slack/Teams, Email, Zoom/Meet), and any systems processing PII. The plan covers incidents affecting the confidentiality, integrity, and availability of Mozart ltd's information assets regardless of the geographic location of employees or systems.

3. Incident and Event Definitions

For the purposes of this plan, a security "event" is defined as any observable occurrence in a system or network that could potentially impact security. A security "incident" is an event that has been confirmed to adversely affect the confidentiality, integrity, or availability of Mozart ltd's information systems or data. Examples include unauthorized access to systems, data breaches involving PII, malware infections, denial of service attacks, and violations of security policies that impact business operations or customer data.

4. Incident Reporting

All employees at Mozart ltd are responsible for promptly reporting suspected security incidents or unusual activities. Reports should be made to the IT Security Lead through Slack/Teams or email at security@Mozart ltd.com. If communication platforms are compromised, alternative reporting methods include phone calls or SMS to the IT Security Lead. Employees should provide as much detail as possible about the suspected incident without conducting their own investigations.
External parties, including clients and vendors, can report potential security incidents by emailing security@Mozart ltd.com or contacting their Mozart ltd account manager. The IT Security Lead will review all reports within 4 business hours to determine if they constitute actual security incidents requiring activation of the response procedures outlined in this plan.

5. Severity Levels

Security incidents are categorized into severity levels to ensure appropriate resource allocation and response:

5.1 Critical (Level 1)

- **Definition**: Severe impact on business operations, extensive system compromise, or unauthorized access to PII data
- **Examples**:
  - Confirmed data breach involving customer PII
  - Ransomware affecting multiple systems
  - Compromise of cloud environments hosting customer-facing applications
  - Targeted attack affecting business continuity
- **Response Time**: Immediate (within 1 hour)
- **Notification**: Executive team, affected customers, and potentially regulatory authorities

5.2 High (Level 2)

- **Definition**: Significant impact on specific systems or limited data exposure
- **Examples**:
  - Compromise of a single employee account
  - Localized malware infection
  - Unauthorized access to non-production systems
  - DDoS attack affecting availability but not data integrity
- **Response Time**: Urgent (within 4 hours)
- **Notification**: Department heads and IT management

5.3 Medium (Level 3)

- **Definition**: Limited impact on non-critical systems or suspicious activities requiring investigation
- **Examples**:
  - Suspicious login attempts
  - Phishing emails targeting employees
  - Policy violations with potential security implications
  - Non-sensitive data exposure
- **Response Time**: Same business day
- **Notification**: IT Security Lead and relevant team leaders

5.4 Low (Level 4)

- **Definition**: Minimal impact, routine security events
- **Examples**:
  - Failed login attempts below threshold
  - Minor policy violations
  - Easily contained malware on a single workstation

- **Response Time**: Within 24-48 hours
- **Notification**: Documented for review in regular security meetings

6. Escalation and Internal Reporting

Initial incident reports will be assessed by the IT Security Lead who will determine the incident severity level and activate the Incident Response Team as appropriate. For Critical (Level 1) and High (Level 2) incidents, the IT Security Lead will notify the CTO or CEO immediately, who may then convene an emergency leadership meeting. The Incident Response Team will provide regular status updates to leadership based on severity: hourly for Critical incidents, every 4 hours for High incidents, and daily for Medium incidents.
Escalation paths should follow the organizational structure but may skip levels in urgent situations. If the primary contact is unavailable, team members should contact the next person in the escalation path. For incidents involving potential legal or regulatory implications, the escalation must include Mozart ltd's legal counsel or compliance officer at the earliest possible stage to ensure proper handling of communication and documentation.

7. Incident Documentation

All security incidents must be thoroughly documented from initial detection through resolution and post-incident review. The IT Security Lead will maintain a secured incident log using our approved documentation system, accessible only to authorized team members. Documentation should include timestamps, discovered evidence, actions taken, communications, and team members involved. Screen captures, system logs, and other technical evidence should be preserved with chain of custody maintained.
For Critical and High severity incidents, more detailed documentation is required, including impact assessment, timeline of events, and external communications. At the conclusion of incident handling, the IT Security Lead will compile a comprehensive incident report that includes root cause analysis, effectiveness of response actions, and recommendations for preventing similar incidents. This documentation may be required for legal proceedings, insurance claims, or regulatory compliance, and must be retained according to Mozart ltd's data retention policy.

8. Incident Response Process

8.1 Summary

The Mozart ltd incident response process follows a six-phase approach: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. This structured methodology ensures we address security incidents comprehensively while minimizing business disruption, particularly for our remote workforce and cloud-based operations. The process is designed to be flexible enough to address various types of incidents while providing clear guidance on necessary actions at each stage.

8.2 Detailed Process

8.2.1 Preparation

- Maintain current contact information for all response team members
- Ensure remote access capabilities for incident responders
- Deploy and maintain monitoring solutions for cloud environments and SaaS applications
- Conduct quarterly reviews of this incident response plan
- Provide security awareness training to all employees twice yearly
- Establish relationships with external security resources for complex incidents

8.2.2 Identification

- Validate the reported incident and determine its scope and severity
- Assign an incident handler to lead the response effort
- Create an incident ticket in the tracking system
- Collect initial forensic data without disrupting evidence
- Determine the incident's severity level using criteria in Section 5
- Identify affected systems, applications, and data (particularly PII)
- Document initial findings and activate appropriate team members

8.2.3 Containment

- Implement short-term containment measures to limit damage:
    - Isolate affected systems from the network where possible
    - Temporarily disable compromised user accounts
    - Block malicious IP addresses or domains
    - Take snapshots of cloud environments for forensic purposes
- Implement long-term containment:
    - Apply emergency patches or configuration changes
    - Enhance monitoring on similar systems
    - Implement additional authentication measures
- Preserve evidence in accordance with forensic best practices
- Document all containment actions with timestamps

8.2.4 Eradication

- Remove malware, unauthorized accounts, or other artifacts from affected systems
- Reset credentials for compromised accounts
- Patch vulnerabilities that were exploited
- Validate that all malicious components have been removed
- Scan systems to ensure complete remediation
- Document all eradication actions

8.2.5 Recovery

- Restore systems from known clean backups if necessary
- Implement additional security controls as needed
- Monitor recovered systems for signs of compromise
- Gradually return systems to production with heightened monitoring

- Verify that normal operations have been restored
- Confirm that PII data is properly secured

8.2.6 Lessons Learned

- Schedule a post-incident review meeting within one week of resolution
- Analyze the incident's root cause and response effectiveness
- Document findings and recommendations
- Update the incident response plan based on lessons learned
- Implement preventative measures
- Share appropriate insights with the broader team
- Create follow-up tasks with assigned owners and deadlines

8.3 Incident Response Meeting Agenda

For Critical and High severity incidents, the Incident Response Team will conduct regular meetings. A suggested agenda includes:

1. **Incident Status Update** (5 minutes)
    - Current understanding of the incident
    - Timeline of known events
2. **Technical Assessment** (10 minutes)
    - Systems and data affected
    - Current containment status
    - Evidence collected
3. **Response Actions** (15 minutes)

- Actions taken since last meeting
- Effectiveness of current measures
- Proposed next steps

4. **Business Impact Assessment** (5 minutes)
    - Customer impact
    - Operational disruption
    - Financial implications
5. **Communication Plan** (10 minutes)
    - Internal stakeholder updates
    - External communications needed
    - Customer and regulatory notifications
6. **Resource Requirements** (5 minutes)

- Additional personnel needed
- External assistance requirements
- Tools or systems needed

7. **Action Items** (5 minutes)
    - Assign specific tasks with owners
    - Set deadlines for completion
    - Schedule next meeting

9. Special Considerations

9.1 Internal Issues

When responding to incidents involving Mozart ltd employees, additional confidentiality measures must be implemented. Only the minimum necessary team members should be informed, typically limited to the IT Security Lead, HR representative, and a member of executive leadership. Documentation should be segregated from standard incident records and access restricted. If employee misconduct is suspected, HR policies must be followed in parallel with technical response actions, and legal counsel should be consulted before taking any actions that could affect employee rights or privacy.

9.2 Compromised Communications

If Mozart ltd's primary communication channels (Slack/Teams, email, or Zoom/Meet) are compromised or suspected to be compromised, the Incident Response Team will immediately establish alternate communication methods. This may include pre-designated personal email addresses, encrypted messaging applications, or direct phone calls. A separate emergency contact list with alternative communication details is maintained by the IT Security Lead and shared with essential team members. Team members should verify identities through pre-established authentication questions when using alternative channels.

9.3 External Communications and Breach Reporting

All external communications regarding security incidents must be coordinated through a single point of contact, typically the CEO or designated communications lead. No employee should discuss the incident with customers, partners, or the public without explicit authorization. For incidents involving PII data breaches, Mozart ltd will comply with all applicable notification laws and regulations, which may require timely disclosure to affected individuals and regulatory authorities. The IT Security Lead, in conjunction with legal counsel, will determine notification requirements based on the nature of the breach and jurisdictions involved.

9.4 Mitigation and Remediation

Long-term mitigation strategies will be developed based on root cause analysis of significant incidents. The IT Security Lead will work with relevant teams to implement technical solutions, policy changes, or additional controls to prevent recurrence. For incidents affecting cloud-based resources or SaaS applications, Mozart ltd will coordinate with vendors to ensure appropriate remediation measures are implemented. All remediation activities will be tracked to completion with regular status updates provided to leadership until all identified vulnerabilities have been addressed.

9.5 Cooperation with Customers, Data Controller and Authorities

For incidents involving customer data or systems, Mozart ltd will collaborate transparently while maintaining appropriate confidentiality. When acting as a data processor, we will promptly notify the data controller in accordance with contractual obligations and provide necessary information to support their compliance requirements. If regulatory authorities become involved, Mozart ltd will designate specific team members to serve as points of contact and coordinate our

cooperation efforts. All communications with external parties will be documented, and we will balance transparency with the need to protect sensitive security information.

10. Response Team Members

The Incident Response Team consists of the following roles:

Role	Responsibilities	Primary Contact	Backup Contact
Incident Response Lead	Overall coordination of response efforts, severity assessment, and team activation	IT Security Lead	CTO
Technical Lead	Technical investigation, containment, and eradication	Senior DevOps Engineer	Senior Developer
Communications Coordinator	Internal and external communications, stakeholder updates	CEO	COO
Legal/Compliance Advisor	Regulatory compliance, legal implications	Outside Counsel	CEO
Executive Sponsor	Resource allocation, high-level decisions	CTO	CEO
Documentation Specialist	Maintaining incident records, documentation	IT Admin	Office Manager

For specific contact details, refer to Appendix A.

11. Management Commitment

Mozart ltd's leadership is fully committed to the effective implementation of this Incident Response Plan. The executive team acknowledges that security incidents are not merely technical issues but business risks that require proper management attention and resources. Leadership will ensure availability of necessary tools, training, and personnel to execute this plan effectively. The CTO will review this plan annually to ensure it remains aligned with business objectives and the evolving threat landscape. Management further commits to supporting post-incident improvements and investing in preventative measures identified through the incident response process.

12. Exceptions

Exceptions to this Incident Response Plan may be granted only in extraordinary circumstances where following the standard procedures would cause significant business harm or impede effective incident response. All exceptions must be approved by the CTO or CEO and documented with a clear justification. Temporary exceptions should include an expiration date, and the incident documentation must clearly state which procedures were modified and why. The IT Security Lead will maintain a log of all exceptions granted and review them during the

annual plan assessment to determine if permanent modifications to the plan are warranted.

13. Violations & Enforcement

Compliance with this Incident Response Plan is mandatory for all Mozart ltd employees. Failure to report security incidents or interference with the incident response process may result in disciplinary action up to and including termination. The severity of any disciplinary action will depend on the impact of the violation on Mozart ltd's security posture, client relationships, and regulatory compliance. This enforcement policy applies equally to all employees regardless of position or tenure. Contractors and vendors working with Mozart ltd are also expected to comply with relevant aspects of this plan as outlined in their service agreements.

Appendix A - Template: Contact Information

Name	Title	Role in IRP	Primary Phone	Secondary Phone	Email	Alternative Contact
[Name]	IT Security Lead	Incident Response Lead	[Phone]	[Phone]	[Email]	[Alt. Contact]
[Name]	CTO	Executive Sponsor	[Phone]	[Phone]	[Email]	[Alt. Contact]
[Name]	CEO	Communications Coordinator	[Phone]	[Phone]	[Email]	[Alt. Contact]
[Name]	Senior DevOps Engineer	Technical Lead	[Phone]	[Phone]	[Email]	[Alt. Contact]
[Name]	Senior Developer	Backup Technical Lead	[Phone]	[Phone]	[Email]	[Alt. Contact]
[Name]	Outside Counsel	Legal/Compliance Advisor	[Phone]	[Phone]	[Email]	[Alt. Contact]

External Contacts:

- Cybersecurity Insurance Provider: [Contact Information]
- Cloud Service Provider Security Team: [Contact Information]
- Managed Security Service Provider: [Contact Information]
- Digital Forensics Firm: [Contact Information]
- Local FBI Field Office: [Contact Information]

Appendix B - Template: Incident Collection Form

Incident Details

Incident ID: [YYYY-MM-DD-XX]
Reporter Information:

- Name:
- Role:
- Contact Information:
- Date/Time of Report:

Incident Discovery:
- Date/Time Discovered:
- How Discovered:
- Systems/Data Affected:

Incident Description:
- Summary of Incident:
- Observable Symptoms:
- Suspected Cause (if known):

Impact Assessment:
- Business Functions Affected:
- Number of Users Affected:
- Customer Data Involved (Y/N):
- PII Compromised (Y/N):
- Systems Unavailable:
- Estimated Financial Impact:

Initial Response Actions

Incident Severity: [Critical/High/Medium/Low]
Incident Handler Assigned:
Initial Containment Measures Taken:
Evidence Preservation:
- Log Files Secured:
- Screenshots Captured:
- System Images Created:
- Other Evidence:

Notifications Made:
- Internal Stakeholders Notified:
- External Parties Notified:
- Time of Notifications:

Investigation Notes

Timeline of Events:
Systems Analyzed:
Indicators of Compromise Found:
Attack Vector/Root Cause (if identified):

Resolution Details

Containment Measures:
Eradication Steps:
Recovery Actions:
Confirmation of Resolution:

Date/Time of Resolution:

Post-Incident

Lessons Learned Meeting Date:
Preventative Measures Identified:
Updates Required to IRP:
Post-Incident Report Completed By:
Date: