INCIDENT RESPONSE AND DATA BREACH NOTIFICATION PROCEDURES

JANUARY 2026

POLICY NUMBER: TMG-SEC-020
APPROVAL AUTHORITY: BOARD OF DIRECTORS

THE MAZI GROUP

1. PURPOSE

This policy establishes The Mazi Group's procedures for responding to security incidents and data breaches, including notification requirements under applicable laws. A swift, coordinated response is essential to minimizing harm to affected individuals, protecting company assets, and meeting legal obligations across all brands: Mazi Beauty, Glam Switch, On The Go Mists, and Upvendo.

2. SCOPE

This policy applies to:

- All security incidents affecting The Mazi Group systems or data
- All data breaches involving personal information
- All employees, contractors, and third parties
- All brands and business units
- All geographic locations and regulatory jurisdictions

3. INCIDENT CLASSIFICATION

3.1 Security Incident

Any event that threatens the confidentiality, integrity, or availability of information systems or data, including:

- Malware infections
- Unauthorized access attempts
- Denial of service attacks
- Phishing attacks
- Lost or stolen devices
- System vulnerabilities exploited

3.2 Data Breach

Unauthorized access to, acquisition of, or disclosure of personal information that compromises security, confidentiality, or integrity, including:

- Unauthorized access to personal data
- Theft of personal data

- Accidental disclosure of personal data
- Loss of unencrypted devices containing personal data
- Ransomware affecting personal data

3.3 Severity Levels

Level	Description	Response Time
Critical	Active breach, widespread impact, sensitive data exposed	Immediate (within 1 hour)
High	Confirmed breach, limited scope, personal data at risk	Within 4 hours
Medium	Potential breach, investigation needed	Within 24 hours
Low	Minor incident, no personal data impact	Within 72 hours

4. INCIDENT RESPONSE TEAM

4.1 Core Team

- **Incident Commander:** CISO or designated security leader
- **Security Lead:** Security operations manager
- **Privacy Lead:** Data Protection Officer
- **Legal Lead:** Chief Legal Officer or designee
- **Communications Lead:** CMO or PR director
- **IT Operations Lead:** CTO or IT director

4.2 Extended Team (as needed)

- Brand representatives
- Customer service leadership
- Human resources (if employee data involved)
- Finance (if financial data involved)
- External forensics firm
- External legal counsel
- Law enforcement liaison

5. INCIDENT RESPONSE PHASES

5.1 Phase 1: Detection and Reporting

Detection Sources

- Security monitoring and SIEM alerts
- Employee reports
- Customer complaints
- Third-party notifications
- Law enforcement notification
- Media reports

Reporting Requirements

- All employees must report suspected incidents immediately
- Report to security@mazigroup.us or security hotline
- Do not attempt to investigate independently
- Preserve evidence

5.2 Phase 2: Assessment and Triage

- Confirm incident is real (not false positive)
- Determine incident type and severity
- Identify affected systems and data
- Assess scope and potential impact
- Activate incident response team
- Begin incident documentation

5.3 Phase 3: Containment

Short-term Containment

- Isolate affected systems
- Block malicious IP addresses
- Disable compromised accounts
- Preserve evidence before changes

Long-term Containment

- Apply temporary fixes
- Implement additional monitoring
- Prepare for eradication

5.4 Phase 4: Eradication

- Remove malware and artifacts
- Close vulnerabilities exploited
- Reset compromised credentials
- Patch affected systems
- Verify eradication complete

5.5 Phase 5: Recovery

- Restore systems from clean backups
- Rebuild systems if necessary
- Verify system integrity
- Monitor for recurrence
- Return to normal operations

5.6 Phase 6: Post-Incident

- Conduct post-incident review
- Document lessons learned
- Update procedures and controls
- Complete regulatory notifications
- Close incident

6. DATA BREACH ASSESSMENT

6.1 Breach Determination

Assess whether a breach has occurred by determining:

- Was personal information involved?
- Was the data accessed, acquired, or disclosed?

- Was the data encrypted or otherwise protected?
- What is the likelihood of harm to individuals?

6.2 Risk of Harm Assessment

Consider factors including:

- Type and sensitivity of data
- Number of individuals affected
- Whether data was actually accessed vs. potentially exposed
- Whether data was encrypted
- Identity and intent of unauthorized accessor
- Steps taken to reduce harm

7. NOTIFICATION REQUIREMENTS

7.1 Regulatory Notification

GDPR (EU)

- Notify supervisory authority within 72 hours
- Unless breach unlikely to result in risk to individuals
- Document all breaches regardless of notification

US State Laws

Jurisdiction	Timeframe	Notes
California	Most expedient time possible	AG notification if 500+ CA residents
New York	Most expedient time possible	AG, DFS notification required
Other states	Varies (30-90 days typical)	Check specific state requirements

Canada (PIPEDA)

- Notify Privacy Commissioner as soon as feasible
- If breach creates real risk of significant harm

PCI DSS

- Notify payment brands immediately
- Engage PCI Forensic Investigator

7.2 Individual Notification

When Required

- GDPR: When breach likely to result in high risk
- US: When breach involves specified personal information
- Canada: When breach creates real risk of significant harm

Notification Content

- Description of the incident
- Types of information involved
- Steps taken to address the breach
- Steps individuals can take to protect themselves
- Contact information for questions
- Information about credit monitoring (if offered)

Notification Methods

- Direct notification (email, mail) preferred
- Substitute notice if direct not feasible
- Website posting
- Media notification for large breaches

7.3 Third-Party Notification

- Notify affected business partners
- Notify service providers if their systems involved
- Coordinate with joint controllers

8. COMMUNICATION

8.1 Internal Communication

- Brief executive leadership

- Inform board as appropriate
- Update employees on need-to-know basis
- Prepare customer service teams

8.2 External Communication

- Prepare holding statements
- Designate spokespersons
- Coordinate with PR/communications
- Monitor media coverage
- Prepare FAQ for customer inquiries

8.3 Law Enforcement

- Determine if law enforcement notification appropriate
- Coordinate with legal counsel
- Preserve evidence for potential investigation
- May delay individual notification if law enforcement requests

9. DOCUMENTATION

9.1 Incident Log

Maintain detailed log including:

- Timeline of events
- Actions taken
- Decisions made and rationale
- Personnel involved
- Evidence collected
- Communications sent

9.2 Breach Register

Maintain register of all breaches including:

- Facts of the breach
- Effects of the breach

- Remedial actions taken
- Notification decisions and rationale

9.3 Record Retention

- Retain incident records for minimum 6 years
- Retain breach documentation per regulatory requirements
- Preserve evidence securely

10. BRAND-SPECIFIC CONSIDERATIONS

10.1 Glam Switch

- Biometric data breaches require special handling
- Illinois BIPA notification requirements
- AI model compromise assessment

10.2 Upvendo

- PCI DSS breach procedures for payment data
- Coordinate with restaurant clients
- End consumer notification coordination

10.3 E-commerce (Mazi Beauty, On The Go)

- Payment card breach procedures
- Customer account compromise response
- Order data protection

11. THIRD-PARTY INCIDENTS

- Require prompt notification from service providers
- Assess impact on our data
- Coordinate response with third party
- Determine our notification obligations
- Document third-party incident handling

12. TESTING AND TRAINING

12.1 Testing

- Annual tabletop exercises
- Periodic technical response drills
- Test notification procedures
- Update procedures based on test results

12.2 Training

- Incident response team training
- Employee awareness on reporting
- Executive briefings on roles
- Regular refresher training

13. ROLES AND RESPONSIBILITIES

13.1 CISO

- Lead incident response
- Coordinate technical response
- Brief executive leadership
- Approve containment actions

13.2 DPO

- Assess breach notification requirements
- Coordinate regulatory notifications
- Advise on individual notification
- Maintain breach register

13.3 Legal

- Advise on legal obligations
- Coordinate with external counsel
- Manage law enforcement interactions

- Review notifications

13.4 All Employees

- Report suspected incidents immediately
- Cooperate with investigations
- Preserve evidence
- Maintain confidentiality

14. RELATED POLICIES

This policy should be read in conjunction with:

- TMG-SEC-015: Business Continuity and Disaster Recovery Plan
- TMG-SEC-016: Data Privacy and Protection Policy
- TMG-SEC-017: Cybersecurity and IT Security Policy
- TMG-SEC-044: Crisis Management and Communication Plan

15. POLICY REVIEW

This policy shall be:

- Reviewed annually by Security, Privacy, and Legal
- Updated after significant incidents
- Updated for regulatory changes
- Tested through regular exercises

16. DEFINITIONS

- **Security Incident:** Event threatening confidentiality, integrity, or availability of systems or data.
- **Data Breach:** Unauthorized access to or disclosure of personal information.
- **Personal Information:** Information identifying or relating to an individual.
- **Containment:** Actions to limit the scope and impact of an incident.
- **Eradication:** Removal of threat actors and vulnerabilities.

For incident reporting, contact:

Security Department

security@mazigroup.us | Security Hotline: [NUMBER]