

BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

JANUARY 2026

POLICY NUMBER: TMG-SEC-015

APPROVAL AUTHORITY: BOARD OF DIRECTORS



THE MAZI GROUP

1. PURPOSE

This Business Continuity and Disaster Recovery Plan establishes The Mazi Group's framework for maintaining critical business operations during disruptions and recovering from disasters. This plan ensures that our brands—Mazi Beauty, Glam Switch, On The Go Mists, and Upvendo—can continue serving customers and stakeholders even in adverse circumstances.

2. SCOPE

This plan applies to:

- All operations of The Mazi Group and its subsidiaries
- All brands and business units
- All facilities, systems, and critical processes
- All employees and key contractors
- All geographic locations: United States, Canada, European Union, and Latin America

3. OBJECTIVES

- Protect the safety of employees and stakeholders
- Minimize disruption to critical business operations
- Ensure rapid recovery of essential functions
- Protect company assets and reputation
- Meet contractual and regulatory obligations
- Maintain customer confidence and relationships

4. POTENTIAL DISRUPTION SCENARIOS

4.1 Natural Disasters

- Earthquakes
- Hurricanes and severe storms
- Floods
- Wildfires
- Pandemics and health emergencies

4.2 Technology Disruptions

- Cyberattacks and ransomware
- System failures and outages
- Data center incidents
- Network disruptions
- Cloud service provider outages

4.3 Operational Disruptions

- Supply chain failures
- Key supplier bankruptcy
- Manufacturing facility incidents
- Transportation disruptions
- Utility failures (power, water, telecommunications)

4.4 Human-Caused Events

- Workplace violence
- Civil unrest
- Terrorism
- Labor disputes
- Key personnel loss

5. BUSINESS IMPACT ANALYSIS

5.1 Critical Business Functions

Function	RTO	RPO	Priority
E-commerce platforms	4 hours	1 hour	Critical
Payment processing	4 hours	0	Critical
Upvendo POS systems	2 hours	0	Critical
Customer service	8 hours	4 hours	High

Order fulfillment	24 hours	4 hours	High
Manufacturing	72 hours	24 hours	High
Financial systems	24 hours	4 hours	High
HR and payroll	72 hours	24 hours	Medium

5.2 Critical Dependencies

- Cloud infrastructure (AWS, Azure, Google Cloud)
- Payment processors
- Key manufacturing partners
- Logistics providers
- Telecommunications providers
- Key raw material suppliers

6. BUSINESS CONTINUITY STRATEGIES

6.1 Technology Continuity

- Multi-region cloud deployment for critical systems
- Automated failover for critical applications
- Regular data backups with off-site storage
- Redundant network connections
- Disaster recovery site for critical systems

6.2 Operational Continuity

- Multiple manufacturing partners in different regions
- Safety stock for critical materials
- Alternative logistics providers
- Distributed fulfillment capabilities
- Remote work capabilities for office functions

6.3 Workforce Continuity

- Cross-training for critical roles

- Succession planning for key positions
- Remote work infrastructure
- Emergency communication systems
- Employee assistance programs

7. DISASTER RECOVERY

7.1 IT Disaster Recovery

Data Backup

- Daily incremental backups
- Weekly full backups
- Geographic replication of critical data
- Regular backup testing and verification
- Encrypted backup storage

System Recovery

- Documented recovery procedures for all critical systems
- Recovery environment maintained and tested
- Automated recovery scripts where possible
- Recovery testing at least annually

Recovery Priorities

1. Network and infrastructure
2. Security systems
3. Critical business applications
4. Communication systems
5. Supporting systems

7.2 Facility Recovery

- Identify alternative work locations
- Agreements with co-working spaces
- Mobile office capabilities
- Equipment and supply reserves

8. CRISIS MANAGEMENT

8.1 Crisis Management Team

- CEO (Crisis Leader)
- COO (Operations Lead)
- CTO (Technology Lead)
- CFO (Finance Lead)
- CLO (Legal Lead)
- CHRO (People Lead)
- CMO (Communications Lead)
- Brand Leaders (as needed)

8.2 Crisis Response Phases

Phase 1: Detection and Assessment

- Identify and confirm the incident
- Assess scope and impact
- Activate crisis management team
- Establish command center

Phase 2: Response

- Ensure employee safety
- Implement containment measures
- Activate business continuity plans
- Communicate with stakeholders

Phase 3: Recovery

- Execute recovery procedures
- Restore critical operations
- Monitor recovery progress
- Adjust plans as needed

Phase 4: Restoration

- Return to normal operations

- Conduct post-incident review
- Update plans based on lessons learned
- Address any remaining issues

9. COMMUNICATION PLAN

9.1 Internal Communication

- Emergency notification system for all employees
- Multiple communication channels (email, SMS, phone tree)
- Regular status updates during incidents
- Clear chain of command for communications

9.2 External Communication

- Pre-approved messaging templates
- Designated spokespersons
- Customer communication procedures
- Media relations protocols
- Regulatory notification procedures
- Investor communication protocols

9.3 Contact Lists

- Crisis management team contacts
- Key vendor and partner contacts
- Emergency services contacts
- Regulatory agency contacts
- Insurance contacts

10. BRAND-SPECIFIC CONSIDERATIONS

10.1 Mazi Beauty / On The Go Mists

- Alternative manufacturing partners identified
- Safety stock of finished goods

- E-commerce platform redundancy
- Customer order communication procedures

10.2 Glam Switch

- Device firmware update capabilities
- AI service redundancy
- Customer support continuity
- Hardware supply chain alternatives

10.3 Upvendo

- POS system high availability (critical for restaurant customers)
- Offline mode capabilities
- 24/7 support continuity
- Payment processing redundancy
- Customer data protection

11. TESTING AND MAINTENANCE

11.1 Testing Program

- Annual full-scale business continuity exercise
- Quarterly tabletop exercises
- Monthly IT disaster recovery tests
- Regular backup restoration tests
- Communication system tests

11.2 Plan Maintenance

- Review and update plans annually
- Update after significant organizational changes
- Update after incidents or exercises
- Maintain current contact information
- Review vendor continuity capabilities

12. TRAINING AND AWARENESS

- Business continuity awareness for all employees
- Role-specific training for crisis team members
- Regular drills and exercises
- New employee orientation on emergency procedures
- Annual refresher training

13. INSURANCE

- Business interruption insurance
- Property insurance
- Cyber insurance
- Product liability insurance
- Review coverage annually
- Document assets and values for claims

14. ROLES AND RESPONSIBILITIES

14.1 Executive Leadership

- Approve business continuity strategy and plans
- Allocate resources for continuity programs
- Lead crisis response
- Make critical decisions during incidents

14.2 Business Continuity Manager

- Develop and maintain continuity plans
- Coordinate testing and exercises
- Provide training and awareness
- Report on program status

14.3 Department Heads

- Develop department-specific continuity plans

- Identify critical functions and dependencies
- Participate in testing and exercises
- Execute recovery procedures

14.4 All Employees

- Know emergency procedures
- Participate in drills and exercises
- Report incidents promptly
- Follow instructions during emergencies

15. RELATED POLICIES

This plan should be read in conjunction with:

- TMG-SEC-011: Supply Chain Management and Risk Mitigation Policy
- TMG-SEC-017: Cybersecurity and IT Security Policy
- TMG-SEC-020: Incident Response and Data Breach Notification Procedures
- TMG-SEC-044: Crisis Management and Communication Plan

16. PLAN REVIEW

This plan shall be:

- Reviewed and updated annually
- Updated after significant incidents or changes
- Tested through regular exercises
- Approved by executive leadership

17. DEFINITIONS

- **Business Continuity:** Capability to continue critical operations during and after a disruption.
- **Disaster Recovery:** Process of restoring IT systems and data after a disaster.
- **RTO (Recovery Time Objective):** Maximum acceptable time to restore a function after disruption.
- **RPO (Recovery Point Objective):** Maximum acceptable data loss measured in time.

- **Crisis:** An event that threatens operations, reputation, or stakeholder safety.

For questions about this plan, contact:

Operations Department
operations@mazigroup.us