CLOUD COMPUTING AND SAAS GOVERNANCE POLICY

JANUARY 2026

POLICY NUMBER: TMG-SEC-040
APPROVAL AUTHORITY: BOARD OF DIRECTORS

THE MAZI GROUP

1. PURPOSE

This Cloud Computing and SaaS Governance Policy establishes guidelines for the secure and effective use of cloud services at The Mazi Group. As we leverage cloud technologies across our brands—Mazi Beauty, Glam Switch, On The Go Mists, and Upvendo—proper governance ensures security, compliance, and cost optimization.

2. SCOPE

This policy applies to:

- All cloud services (IaaS, PaaS, SaaS)
- All cloud providers
- All employees using or managing cloud services
- All brands and business units
- All data stored or processed in the cloud

3. CLOUD SERVICE MODELS

3.1 Infrastructure as a Service (IaaS)

- Virtual machines, storage, networking
- Examples: AWS EC2, Azure VMs, Google Compute
- Company responsible for OS, applications, data

3.2 Platform as a Service (PaaS)

- Development platforms, databases, middleware
- Examples: Azure App Service, AWS Lambda, Heroku
- Company responsible for applications and data

3.3 Software as a Service (SaaS)

- Complete applications delivered via cloud
- Examples: Salesforce, Microsoft 365, Workday
- Company responsible for data and configuration

4. CLOUD STRATEGY

4.1 Approved Cloud Providers

- Primary providers approved by IT
- Evaluated for security, compliance, reliability
- Contractual agreements in place
- New providers require approval

4.2 Cloud-First Approach

- Evaluate cloud options for new systems
- Consider cloud migration for existing systems
- Balance benefits with security and compliance needs

5. CLOUD SERVICE PROCUREMENT

5.1 Approval Process

- All cloud services require IT approval
- Security assessment for new services
- Privacy impact assessment if personal data involved
- Legal review of terms of service
- Finance approval for costs

5.2 Shadow IT Prevention

- Unauthorized cloud services prohibited
- Discovery and monitoring for shadow IT
- Process for requesting new services
- Education on risks of unauthorized services

5.3 Vendor Assessment

- Security certifications (SOC 2, ISO 27001)
- Data protection practices
- Compliance with relevant regulations

- Business continuity capabilities
- Data portability and exit provisions

6. SECURITY REQUIREMENTS

6.1 Access Control

- Strong authentication required
- Multi-factor authentication (MFA) for all cloud services
- Single sign-on (SSO) where possible
- Least privilege access
- Regular access reviews

6.2 Data Protection

- Encryption of data at rest and in transit
- Key management practices
- Data classification applied to cloud data
- Data loss prevention controls

6.3 Network Security

- Secure connectivity to cloud services
- Network segmentation
- Firewall and security group configuration
- Monitoring and logging

6.4 Configuration Management

- Secure baseline configurations
- Configuration monitoring
- Change management for cloud resources
- Infrastructure as code where applicable

7. DATA GOVERNANCE

7.1 Data Location

- Know where data is stored
- Comply with data residency requirements
- EU data in EU regions where required
- Document data locations

7.2 Data Classification

- Apply data classification to cloud data
- Restrict sensitive data to approved services
- Additional controls for confidential data

7.3 Data Retention and Deletion

- Apply retention policies to cloud data
- Ensure data can be deleted when required
- Verify deletion from backups

8. COMPLIANCE

8.1 Regulatory Compliance

- Ensure cloud services support compliance needs
- GDPR, CCPA, PCI DSS as applicable
- Industry-specific requirements
- Audit and reporting capabilities

8.2 Contractual Requirements

- Data processing agreements
- Security commitments
- Audit rights
- Breach notification
- Liability provisions

9. SAAS MANAGEMENT

9.1 SaaS Inventory

- Maintain inventory of all SaaS applications
- Track users, costs, and data
- Regular review of SaaS portfolio
- Consolidate redundant applications

9.2 SaaS Security

- SSO integration where possible
- MFA required
- Security configuration review
- API security

9.3 SaaS Administration

- Designated administrators
- User provisioning and deprovisioning
- Regular access reviews
- Configuration management

10. COST MANAGEMENT

10.1 Cost Visibility

- Track cloud spending
- Allocate costs to business units
- Regular cost reporting
- Budget monitoring

10.2 Cost Optimization

- Right-size resources
- Use reserved instances where appropriate
- Shut down unused resources

- Regular optimization reviews

11. BUSINESS CONTINUITY

11.1 Availability

- Understand provider SLAs
- Design for high availability
- Multi-region deployment for critical services
- Monitor availability

11.2 Backup and Recovery

- Backup cloud data
- Test recovery procedures
- Consider multi-cloud for critical data
- Document recovery procedures

11.3 Exit Strategy

- Plan for provider exit
- Ensure data portability
- Avoid vendor lock-in where possible
- Document exit procedures

12. MONITORING AND LOGGING

- Enable logging for all cloud services
- Centralize log collection
- Monitor for security events
- Retain logs per policy
- Regular log review

13. INCIDENT RESPONSE

- Include cloud in incident response plans
- Understand provider incident procedures

- Coordinate with providers during incidents
- Document cloud-specific response procedures

14. ROLES AND RESPONSIBILITIES

14.1 IT/Cloud Team

- Manage cloud infrastructure
- Implement security controls
- Monitor and optimize
- Support cloud users

14.2 Security

- Assess cloud security
- Define security requirements
- Monitor for threats
- Respond to incidents

14.3 Business Units

- Request cloud services through proper channels
- Comply with cloud policies
- Manage costs within budget

15. RELATED POLICIES

This policy should be read in conjunction with:

- TMG-SEC-014: Vendor and Supplier Management Policy
- TMG-SEC-016: Data Privacy and Protection Policy
- TMG-SEC-017: Cybersecurity and IT Security Policy
- TMG-SEC-019: Third-Party Data Sharing and Processing Agreements

16. POLICY REVIEW

This policy shall be:

- Reviewed annually by IT and Security
- Updated for technology and regulatory changes
- Approved by CTO and CISO
- Communicated to relevant teams

17. DEFINITIONS

- **IaaS:** Infrastructure as a Service - cloud-based computing resources.
- **PaaS:** Platform as a Service - cloud-based development platforms.
- **SaaS:** Software as a Service - cloud-based applications.
- **Shadow IT:** Technology used without IT approval.
- **SSO:** Single Sign-On - one login for multiple applications.

For questions about this policy, contact:
Technology Department
technology@mazigroup.us