Data Breach & Recordkeeping Policy

Organization: WealthMeUp, Inc. ("WMU")
Effective Date: 10.01.2024
Owner: CTO / Security & Compliance Lead
Approved By: CEO

1. Purpose

This policy establishes WMU's standards and procedures for identifying, reporting, investigating, responding to, resolving, and documenting data breaches, and for retaining security and business records in compliance with SOC 2, GDPR, CCPA, and applicable contractual requirements.

2. Scope

This policy applies to all employees, contractors, and third-party service providers that access, store, process, or transmit WMU data, including:

- Consumers, merchants, and partner data
- Sensitive and regulated financial information
- Authentication and system access logs
- Data stored or processed in WMU-owned or cloud-hosted systems

3. Regulatory and Compliance Basis

WMU's data handling approach is designed to align with:

- SOC 2 Type II (controls under active implementation; certification planned as WMU scales data volume with enterprise partners)
- GDPR and CCPA privacy obligations, including data subject rights
- Requirements related to regulated partners (e.g., Betterment as custodian and broker-dealer)

WMU does not participate in money transmission and does not custody investment accounts.

4. Architecture and Data Protections

- All PII in WMU systems is encrypted or tokenized.
- WMU does not store or process raw payment card data. All card data remains with regulated payment processors under PCI-DSS obligations.
- Investment account PII is held solely by Betterment, which maintains SEC and FINRA regulatory compliance.

- WMU segregates merchant data and strictly enforces least-privilege access.
- Access controls require MFA and continuous monitoring for all production systems.

5. Roles & Responsibilities

Role	Responsibilities
All Personnel	Report suspected incidents immediately. Maintain confidentiality.
Security & Engineering	Assess, contain, investigate, and document incidents. Implement remediation.
Compliance & Legal	Direct regulatory and contractual notifications. Validate reporting requirements.
Leadership	Approve response plans and ensure resource allocation.

6. Breach Identification & Response Procedures

6.1 Detection

Triggers include:

- Unauthorized access alerts
- Anomalous data transfers
- Lost or stolen devices
- Reports from partners or regulators

6.2 Initial Reporting

Immediately notify yianni@wealthmeup.ai or use internal alerting channels.

6.3 Containment

Engineering isolates impacted systems, revokes compromised credentials, and blocks malicious traffic.

6.4 Investigation

Incident Response Team:
• Determines data types and extent of exposure
• Identifies attack vector and timeline
• Assesses impact and likelihood of harm

Results are logged in the Breach Register.

6.5 Notification

Notifications will occur within statutory timeframes when required.
Potential notification groups:
• Affected consumers and merchants
• Supervisory authorities (GDPR/CCPA context)
• Strategic partners (e.g., Betterment when relevant)

External communications require Legal and Executive approval.

6.6 Remediation

• Control strengthening
• Vulnerability patching
• Continuous monitoring improvements
• Mandatory post-incident training if human error involved

6.7 Post-Incident Review

Within 30 days, the Incident Response Team submits a lessons-learned report and recommends updates to controls, training, and architecture.

7. Monitoring and Auditing Requirements

• All sensitive data access and authentication events are logged and monitored.
• Logs are retained securely and protected from tampering.
• Production access is auditable and restricted to least-privilege roles.
• SOC 2 aligned monitoring controls are continuously matured.

8. Recordkeeping & Retention

Records are retained in compliance with regulatory and contractual obligations.

Record Type	Minimum Retention
Audit and access logs	3–7 years depending on jurisdiction
Breach records & IRT reports	7 years
Merchant agreements	7 years post-termination
Data processing agreements	Life of agreement + 7 years
Employee access and privilege records	Employment duration + 2 years

Data disposal must use secure deletion or token revocation methods.

9. Data Minimization & Access

- WMU collects only data necessary for user enrollment, reward conversion, and compliance with regulated custodians.
- PII and merchant datasets are logically segmented.
- Access is revoked immediately upon role change or termination.

10. Training

All personnel must complete:
• Annual cybersecurity and data protection training
• Role-based secure development training for engineering and DevOps
• Incident reporting procedure training

11. Third-Party Security

Third parties with access to WMU data must:

- Maintain equivalent data protection standards
- Undergo periodic risk and compliance review
- Execute data processing and confidentiality agreements

12. Violations

Non-compliance may result in disciplinary action, up to and including termination, and legal action in cases of negligence or malicious intent.

13. Review Cycle

Policy is reviewed at least annually and updated to reflect:

- SOC 2 roadmap progress
- Technology changes
- Evolving regulatory requirements
- Lessons learned from continuous improvement