**MOMENTUM SPORTS**

**Information Security & Data Privacy Policy**

**Effective Date:** January 2026

**Version:** 1.0

**Document Owner:** Chief Operating Officer

**Review Cycle:** Annual

# 1. PURPOSE AND SCOPE

## 1.1 Purpose

This Information Security & Data Privacy Policy establishes Momentum Sports' commitment to protecting the confidentiality, integrity, and availability of information assets, and ensuring compliance with applicable data protection regulations across our operating territories in Australia, North America, Europe, and the Pacific region.

## 1.2 Scope

This policy applies to:

* All Momentum Sports full-time employees (16 core team members)
* Contractors, casual workers, and business partners
* All information systems, databases, and digital assets
* Customer data (18,485+ direct customers)
* Reseller partner data (701 reseller organizations)
* E-commerce platforms and transaction systems
* All geographic locations where Momentum Sports operates

## 1.3 Regulatory Framework

Momentum Sports complies with:

* Australian Privacy Act 1988 and Privacy Principles (APPs)
* European Union General Data Protection Regulation (GDPR)
* Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)
* U.S. state privacy laws where applicable
* Payment Card Industry Data Security Standard (PCI DSS)

# 2. GOVERNANCE AND ACCOUNTABILITY

## 2.1 Roles and Responsibilities

### Data Protection Officer (DPO)

* Oversees data privacy compliance across all territories
* Serves as point of contact for regulatory authorities
* Conducts privacy impact assessments
* Manages data breach response procedures

### Information Security Manager

* Implements and maintains security controls
* Monitors security incidents and threats
* Manages access control systems
* Coordinates security awareness training

### Management Team

* Ensures adequate resources for security and privacy programs
* Approves major security investments and initiatives
* Reviews security metrics and incident reports quarterly
* Champions security culture throughout the organization

### All Employees, Contractors, and Partners

* Complete mandatory annual security awareness training
* Report suspected security incidents immediately
* Follow data handling procedures
* Maintain confidentiality of access credentials
* Comply with acceptable use policies

## 2.2 Policy Review

This policy shall be reviewed annually or following:

* Significant security incidents
* Major regulatory changes
* Substantial business model changes
* Technology infrastructure updates

# 3. DATA CLASSIFICATION AND HANDLING

## 3.1 Data Classification

|  |  |
| --- | --- |
| **Classification** | **Description and Handling Requirements** |
| **RESTRICTED DATA** | **Includes:** Payment card information, bank account details, authentication credentials, social security/tax ID numbers  **Handling:** Encrypted at rest and in transit; access limited to authorized personnel only; never stored in plain text |
| **CONFIDENTIAL DATA** | **Includes:** Customer personal information, purchase history, reseller contracts and pricing, employee information, business financial data  **Handling:** Access on need-to-know basis; encrypted when transmitted; secure deletion when no longer needed |
| **INTERNAL DATA** | **Includes:** Internal communications, draft documents, operational procedures, non-sensitive business analytics  **Handling:** Restricted to Momentum Sports personnel and authorized partners; not for public disclosure |
| **PUBLIC DATA** | **Includes:** Marketing materials, public website content, published product catalogs, press releases  **Handling:** May be freely shared; ensure accuracy before publication |

## 3.2 Data Minimization Principle

Momentum Sports collects only the personal data necessary for:

* Order processing and fulfillment
* Customer service and support
* Reseller relationship management
* Legal and regulatory compliance
* Legitimate business operations

# 4. INFORMATION SECURITY CONTROLS

## 4.1 Access Control

### User Authentication

Multi-factor authentication (MFA) required for:

* E-commerce administrative systems
* Customer database access
* Financial systems
* Email and cloud storage containing confidential data

Additional authentication requirements:

* Strong password requirements: minimum 12 characters with complexity rules
* Password rotation every 90 days for privileged accounts
* Account lockout after 5 failed login attempts

### Authorization and Least Privilege

* Role-based access control (RBAC) implemented across all systems
* Access granted based on job function and business need
* Privileged access limited to essential personnel
* Regular access reviews conducted quarterly
* Immediate access revocation upon termination or role change

## 4.2 Network Security

* Enterprise-grade firewalls at all network entry points
* Intrusion detection and prevention systems (IDS/IPS)
* Network segmentation: separation of e-commerce from internal corporate network
* Isolated payment processing environment (PCI DSS compliant)
* 24/7 security event logging and monitoring
* Annual penetration testing by qualified third parties

## 4.3 Data Encryption

Encryption Standards:

* Data in transit: TLS 1.3 minimum for all web traffic
* Data at rest: AES-256 encryption for databases containing personal data
* Full disk encryption on all laptops and mobile devices
* Encrypted backups of all critical systems

Payment Card Security:

* PCI DSS Level 2 compliance maintained
* No storage of CVV/CVC codes
* Tokenization of payment card data
* Point-to-point encryption (P2PE) for card transactions
* Annual PCI compliance validation

## 4.4 Endpoint Security

* Antivirus/anti-malware software on all endpoints
* Automatic security updates and patch management
* Device encryption required for all portable devices
* Mobile device management (MDM) for company-issued devices
* Data loss prevention controls and monitoring

# 5. DATA PRIVACY PRINCIPLES

## 5.1 Lawful Basis for Processing

Momentum Sports processes personal data based on:

* Contract performance (order fulfillment, customer service)
* Legitimate business interests (business analytics, fraud prevention)
* Legal obligations (tax, accounting, regulatory compliance)
* Consent (marketing communications, optional services)

## 5.2 Individual Rights

Momentum Sports respects and facilitates the following data subject rights:

### Right to Access

* Individuals may request copies of their personal data
* Response within 30 days of verified request
* Provided free of charge (first request)

### Right to Rectification

* Individuals may request correction of inaccurate data
* Updates processed within 10 business days

### Right to Erasure ("Right to be Forgotten")

* Honored where legally permissible
* Exceptions for legal obligations and legitimate business needs
* Confirmation provided within 30 days

### Right to Data Portability

* Available for customer and reseller data
* Provided in structured, machine-readable format (CSV, JSON)

## 5.3 Consent Management

* Clear opt-in for marketing communications
* Easy unsubscribe mechanism in every communication
* Separate consent for different communication types
* Granular cookie consent controls on websites
* Consent records maintained with timestamp and audit trail

# 6. DATA RETENTION AND DISPOSAL

## 6.1 Retention Periods

|  |  |
| --- | --- |
| **Data Category** | **Retention Period** |
| **Customer Data** | Active accounts: Duration of relationship plus 7 years; Inactive accounts: 3 years from last transaction |
| **Transaction Records** | 7 years (tax and legal requirements) |
| **Reseller Partner Data** | Duration of relationship plus 7 years; Contract documents: 7 years post-termination |
| **Employee Data** | Duration of employment plus 7 years; Payroll records: 7 years |
| **System Logs** | Security logs: 1 year; Access logs: 90 days; Application logs: 30 days |

## 6.2 Secure Disposal

* Electronic data: Secure deletion using industry-standard wiping tools
* Hard drives and storage media: Physical destruction or certified wiping
* Paper documents: Cross-cut shredding
* Certificate of destruction obtained for third-party disposal services

# 7. THIRD-PARTY MANAGEMENT

## 7.1 Vendor Due Diligence

All vendors handling sensitive data undergo security and privacy assessment before engagement, including:

* Review of vendor security certifications (ISO 27001, SOC 2, etc.)
* Data processing agreement (DPA) required for all processors
* Insurance verification for vendors handling sensitive data
* Annual security questionnaires and compliance verification

Critical Vendors Subject to Enhanced Review:

* E-commerce platform providers
* Payment processors
* Cloud service providers (hosting, storage)
* Customer relationship management (CRM) systems
* Shipping and logistics partners

## 7.2 Data Processing Agreements

All third-party processors must sign agreements including:

* Scope and purpose of data processing
* Data security obligations and standards
* Data breach notification procedures (within 24 hours)
* Audit rights and compliance verification
* Data deletion obligations upon contract termination

# 8. E-COMMERCE AND TRANSACTION SECURITY

## 8.1 Website Security

* HTTPS encryption for all pages
* Security headers (HSTS, CSP, X-Frame-Options)
* Regular vulnerability scanning
* Web application firewall (WAF) and DDoS protection
* Secure session management with appropriate timeouts

## 8.2 Customer Account Security

* Password strength requirements enforced
* Account lockout after failed login attempts
* Password reset via verified email only
* Optional two-factor authentication (2FA)
* Suspicious activity monitoring and alerts

## 8.3 Payment Processing

* PCI DSS Level 2 compliance maintained
* Payment data never stored on Momentum Sports servers
* Tokenization for recurring payments
* 3D Secure authentication where available
* Fraud detection and prevention tools

# 9. DATA BREACH MANAGEMENT

## 9.1 Incident Response Team

* Chief Operating Officer (Incident Commander)
* Information Security Manager
* Data Protection Officer
* External legal counsel (as needed)
* External forensics experts (as needed)

## 9.2 Breach Response Procedures

Detection and Assessment (0-2 hours):

* Identify breach scope and affected systems
* Contain breach to prevent further exposure
* Preserve evidence for investigation
* Document timeline and actions taken

Investigation (2-24 hours):

* Determine root cause
* Identify affected individuals and data categories
* Assess risk level and potential harm
* Engage external forensics if needed

Notification (24-72 hours):

Notify relevant supervisory authorities where required:

* Australian Office of the Information Commissioner (OAIC): within reasonable timeframe
* EU supervisory authorities (GDPR): within 72 hours
* Other jurisdictions per local requirements
* Notify affected individuals if high risk of harm

# 10. BUSINESS CONTINUITY AND DISASTER RECOVERY

## 10.1 Business Continuity Planning

Recovery Time Objectives (RTO) for critical systems:

* E-commerce platform: 4 hours
* Customer database: 8 hours
* Email and communications: 24 hours

Recovery Point Objectives (RPO):

* Transaction data: 1 hour
* Customer data: 24 hours

## 10.2 Data Backup

* Daily automated backups of all critical systems
* Weekly full backups with daily incrementals
* Geographically distributed backup storage
* Encrypted backup storage (AES-256)
* Quarterly backup restoration testing
* Backup retention: 30 days rolling, plus monthly for 1 year

# 11. INTERNATIONAL DATA TRANSFERS

## 11.1 Cross-Border Data Flows

Momentum Sports transfers personal data between:

* Australia (headquarters)
* North America (operations and customers)
* Europe (operations and customers)
* Pacific region (operations and customers)

## 11.2 Transfer Safeguards

For EU Data (GDPR Compliance):

* Standard Contractual Clauses (SCCs) for transfers outside EEA
* Transfer impact assessments conducted
* Data localization for EU customer data where required by contract

For Australian Data (Privacy Act Compliance):

* Overseas disclosure agreements with processors
* Reasonable steps to ensure overseas recipients comply with APPs

For Canadian Data (PIPEDA Compliance):

* Comparable level of protection ensured
* Cross-border privacy rules respected

# 12. TRAINING AND AWARENESS

## 12.1 Mandatory Training Programs

Security Awareness Training (Annual):

* Password security and authentication
* Phishing and social engineering awareness
* Data handling and classification
* Incident reporting procedures
* Remote work security

Role-Based Training:

* Data Protection Officer: GDPR and privacy law updates (ongoing)
* Development team: Secure coding practices (biannual)
* Customer service: Data privacy and customer rights (annual)
* Management: Security risk management (annual)
* Contractors: Tailored to data access level (upon engagement)

# 13. CONTACT INFORMATION

## Data Protection Officer

**Email:** privacy@momentumsports.com.au

**Phone:** [Australian office number]

**Mail:** Momentum Sports Privacy Office, [Australian Headquarters Address]

## Information Security Manager

**Email:** security@momentumsports.com.au

**Phone:** [Australian office number]

## Incident Reporting

**Email:** security-incident@momentumsports.com.au

**Phone:** [24/7 Incident Hotline]

# 14. SUPERVISORY AUTHORITIES

Individuals have the right to lodge complaints with relevant supervisory authorities:

## Australia

Office of the Australian Information Commissioner (OAIC)

**Website:** www.oaic.gov.au

**Phone:** 1300 363 992

## European Union

Individuals may contact their national data protection authority

**EDPB Website:** www.edpb.europa.eu

## Canada

Office of the Privacy Commissioner of Canada

**Website:** www.priv.gc.ca

**Phone:** 1-800-282-1376

# DOCUMENT CONTROL

|  |  |
| --- | --- |
| **Version** | 1.0 |
| **Effective Date** | January 2026 |
| **Last Review Date** | January 2026 |
| **Next Review Date** | January 2027 |
| **Document Owner** | Chief Operating Officer |
| **Approved By** | Executive Management Team |

*This policy is intended for internal use and strategic planning purposes. It should be reviewed by legal counsel familiar with privacy regulations in all operating jurisdictions before implementation.*

**END OF DOCUMENT**