**⚠️ SECURITY WARNING ⚠️**

**MOMENTUM SPORTS**

*"Built for the Journey"*

**ADMIN CREDENTIALS  
&  
ACCESS CONTROL  
MASTER LIST**

IT Security & Access Management

Last Updated: January 2026  
Version 3.2

**🔒 HIGHLY CONFIDENTIAL 🔒  
RESTRICTED ACCESS - IT ADMIN ONLY**

This document contains highly sensitive system credentials and access information.  
Unauthorized access, disclosure, or distribution is strictly prohibited.  
  
• Store in encrypted location only  
• Do not email or transmit electronically  
• Physical copies must be secured in locked cabinet  
• Report any suspected compromise immediately to CTO  
  
Authorized Access: CTO (Charlie Nguyen), IT Admin, General Manager (Alex Morgan)

# DOCUMENT CONTROL

|  |  |
| --- | --- |
| Document Title: | Admin Credentials & Access Control Master List |
| Classification: | HIGHLY CONFIDENTIAL - RESTRICTED |
| Version: | 3.2 |
| Last Updated: | January 15, 2026 |
| Document Owner: | Charlie Nguyen (CTO) |
| Review Frequency: | Quarterly (Jan, Apr, Jul, Oct) |
| Next Review Date: | April 15, 2026 |
| Authorized Viewers: | CTO, IT Admin, General Manager only |

## Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Changes | Author |
| 3.2 | Jan 15, 2026 | Updated access for Skyler Bennett (Product Manager) | C. Nguyen |
| 3.1 | Nov 20, 2025 | Added SmartRide platform credentials | C. Nguyen |
| 3.0 | Oct 1, 2025 | Annual review - removed departed employees | C. Nguyen |
| 2.9 | Jul 15, 2025 | Added Jordan Parker (HR Coordinator) | C. Nguyen |

# ACCESS CONTROL FRAMEWORK

## Access Level Definitions

|  |  |  |
| --- | --- | --- |
| Level | Description | Typical Roles |
| Level 5 Super Admin | Full system access, can create/modify/delete any data, user management, system configuration | CTO, IT Admin |
| Level 4 Executive | Department-wide access, reporting access to all modules, limited admin functions | GM, COO, CFO, Sales Director |
| Level 3 Manager | Departmental data access, team management, standard reporting, workflow approval | Department Managers |
| Level 2 Power User | Extended access within department, advanced features, limited data modification | Analysts, Controllers, Coordinators |
| Level 1 Standard User | Basic access, view and edit own data only, standard features | General staff, contractors |

## Security Policies

**Password Requirements:** Minimum 12 characters, uppercase, lowercase, number, special character. Changed every 90 days. No password reuse for 12 generations.

**Multi-Factor Authentication (MFA):** Required for Level 3+ access and all financial systems. Authenticator app preferred (Google/Microsoft Authenticator).

**Session Timeouts:** 15 minutes for financial systems, 30 minutes for other systems, 60 minutes for read-only access.

**Access Review:** Quarterly review of all access rights. Annual recertification required for Level 4-5 users.

**Separation of Duties:** No single user can initiate AND approve financial transactions >$10K. Finance Controller cannot have payment execution rights.

**Remote Access:** VPN required for all remote connections. VPN credentials separate from system credentials.

**Offboarding:** All access revoked within 2 hours of termination. Manager credentials changed immediately.

# SYSTEM INVENTORY & ADMIN CREDENTIALS

⚠️ CRITICAL: Admin credentials below provide complete system access. These credentials should NEVER be used for day-to-day operations. Use only for system maintenance, emergency recovery, or user management.

## Primary Business Systems

### 1. Enterprise ERP System (NetSuite)

|  |  |
| --- | --- |
| MISSION CRITICAL - LEVEL 5 ACCESS | |
| System URL: | https://momentum-sports.app.netsuite.com |
| Admin Username: | admin@momentumsports.com.au |
| Admin Password: | [STORED IN PASSWORD VAULT - Ref: NS-ADMIN-001] |
| Recovery Email: | it-admin@momentumsports.com.au |
| MFA Method: | Google Authenticator (CTO Phone) |
| Account ID: | TSTDRV2476892 |
| Support Contact: | NetSuite Support: 1-877-638-7848 |
| Last Password Change: | December 1, 2025 |

User Count: 45 active licenses | Key Modules: Financials, Inventory, Order Management, CRM, Purchasing

### 2. Customer Relationship Management (Salesforce)

|  |  |
| --- | --- |
| CRITICAL - LEVEL 5 ACCESS | |
| System URL: | https://momentumsports.my.salesforce.com |
| Admin Username: | sysadmin@momentumsports.com.au |
| Admin Password: | [STORED IN PASSWORD VAULT - Ref: SF-ADMIN-001] |
| Security Token: | [STORED IN PASSWORD VAULT - Ref: SF-TOKEN-001] |
| MFA Method: | Salesforce Authenticator App |
| Organization ID: | 00D5f000008rVg2EAE |
| Support Contact: | Salesforce Support Portal |
| Last Password Change: | November 18, 2025 |

User Count: 28 licenses | Integration: NetSuite (bidirectional sync)

### 3. E-Commerce Platform (Shopify Plus)

|  |  |
| --- | --- |
| HIGH PRIORITY - LEVEL 5 ACCESS | |
| Store URL: | https://momentumsports.com |
| Admin URL: | https://admin.shopify.com/store/momentum-sports |
| Admin Email: | ecommerce@momentumsports.com.au |
| Admin Password: | [STORED IN PASSWORD VAULT - Ref: SHOP-ADMIN-001] |
| MFA Method: | SMS to +61 xxx-xxx-5892 |
| Payment Gateway: | Stripe (separate admin credentials) |
| Last Password Change: | January 3, 2026 |

Annual Revenue: $29.4M B2C | Integration: NetSuite, Shipstation

# EMPLOYEE ACCESS RIGHTS MATRIX

The following matrix details system access rights for all 16 core employees. Access levels are assigned based on job function and principle of least privilege.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Employee | ID | Role | ERP | CRM | E-comm | Email | Files | Finance | HR | WMS | Analytics | VPN |
| Alex Morgan | E001 | General Manager | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| Jordan Lee | E002 | COO | 4 | 4 | 3 | 5 | 5 | 3 | 2 | 5 | 4 | 5 |
| Taylor Singh | E003 | CFO | 4 | 3 | 2 | 5 | 5 | 5 | 2 | 3 | 5 | 5 |
| Finley Adams | E004 | HR Manager | 3 | 3 | 1 | 5 | 5 | 2 | 5 | 2 | 3 | 5 |
| Riley Chen | E005 | Sales Director | 4 | 5 | 4 | 5 | 5 | 3 | 2 | 3 | 4 | 5 |
| Charlie Nguyen | E006 | CTO | 5 | 5 | 5 | 5 | 5 | 4 | 3 | 5 | 5 | 5 |
| Morgan Davis | E007 | Channel Mgr | 3 | 5 | 3 | 5 | 5 | 2 | 1 | 3 | 3 | 5 |
| Avery Wilson | E008 | CS Manager | 3 | 4 | 4 | 5 | 5 | 2 | 1 | 3 | 3 | 5 |
| Quinn Taylor | E009 | Warehouse Mgr | 3 | 3 | 2 | 5 | 5 | 2 | 1 | 5 | 3 | 5 |
| Samir Noor | E010 | Supply Chain Mgr | 3 | 3 | 2 | 5 | 5 | 3 | 1 | 5 | 3 | 5 |
| Rowan Mitchell | E011 | Marketing Mgr | 2 | 4 | 4 | 5 | 5 | 2 | 1 | 1 | 3 | 5 |
| Drew Collins | E012 | Business Analyst | 3 | 4 | 3 | 5 | 5 | 3 | 1 | 3 | 5 | 5 |
| Casey Brown | E013 | Finance Controller | 4 | 2 | 2 | 5 | 5 | 5 | 1 | 2 | 4 | 5 |
| Jamie Patel | E014 | E-commerce Mgr | 2 | 3 | 5 | 5 | 5 | 2 | 1 | 2 | 3 | 5 |
| Skyler Bennett | E015 | Product Manager | 3 | 3 | 3 | 5 | 5 | 2 | 1 | 3 | 3 | 5 |
| Jordan Parker | E016 | HR Coordinator | 2 | 2 | 1 | 5 | 5 | 1 | 4 | 1 | 2 | 5 |

**Access Level Key:** 5 = Super Admin | 4 = Executive | 3 = Manager | 2 = Power User | 1 = Standard User

**System Abbreviations:** ERP = NetSuite | CRM = Salesforce | E-comm = Shopify | Email = Microsoft 365 | Files = SharePoint | Finance = Xero/NetSuite | HR = BambooHR | WMS = Warehouse Mgmt | Analytics = Power BI | VPN = Network Access

# CRITICAL SYSTEM ACCOUNTS & CREDENTIALS

⚠️ ULTRA-SENSITIVE: The following accounts have elevated privileges. Access to these credentials must be tightly controlled and logged.

## Financial Systems

### Xero Accounting Platform

|  |  |
| --- | --- |
| System URL: | https://go.xero.com/app/!mUrHx |
| Admin Username: | admin@momentumsports.com.au |
| Password: | [PASSWORD VAULT - Ref: XERO-ADMIN-001] |
| Authorized Users: | Taylor Singh (CFO), Casey Brown (Controller), Alex Morgan (GM) |
| Bank Feed Access: | Commonwealth Bank, NAB, Wells Fargo (USD) |
| API Keys: | [PASSWORD VAULT - Ref: XERO-API-001 to API-003] |
| Last Audit: | December 15, 2025 |

### Payment Processing (Stripe)

|  |  |
| --- | --- |
| Dashboard URL: | https://dashboard.stripe.com |
| Account Email: | payments@momentumsports.com.au |
| Password: | [PASSWORD VAULT - Ref: STRIPE-ADMIN-001] |
| Live API Keys: | [PASSWORD VAULT - Ref: STRIPE-API-LIVE] |
| Test API Keys: | [PASSWORD VAULT - Ref: STRIPE-API-TEST] |
| Webhook Secret: | [PASSWORD VAULT - Ref: STRIPE-WEBHOOK-001] |

## IT Infrastructure & Cloud Services

### Microsoft 365 Tenant

|  |  |
| --- | --- |
| Tenant Name: | momentumsports.onmicrosoft.com |
| Global Admin: | admin@momentumsports.com.au |
| Password: | [PASSWORD VAULT - Ref: M365-ADMIN-001] |
| Admin Center: | https://admin.microsoft.com |
| Tenant ID: | a7b8c9d0-e1f2-4a5b-8c9d-0e1f2a3b4c5d |
| License Count: | 50 E3 licenses, 5 E5 licenses |
| Exchange Admin: | Same as Global Admin |
| SharePoint Admin: | Same as Global Admin |

### AWS Infrastructure

|  |  |
| --- | --- |
| Account ID: | 123456789012 |
| Root Email: | aws-root@momentumsports.com.au |
| Root Password: | [PASSWORD VAULT - Ref: AWS-ROOT-001] - EMERGENCY USE ONLY |
| IAM Admin User: | momentum-admin |
| IAM Password: | [PASSWORD VAULT - Ref: AWS-IAM-ADMIN-001] |
| Access Keys: | [PASSWORD VAULT - Ref: AWS-ACCESS-KEY-001] |
| Region: | ap-southeast-2 (Sydney) - Primary |

## HR & People Management Systems

### BambooHR

|  |  |
| --- | --- |
| System URL: | https://momentumsports.bamboohr.com |
| Admin Username: | finley.adams@momentumsports.com.au |
| Password: | [PASSWORD VAULT - Ref: BAMBOO-ADMIN-001] |
| API Key: | [PASSWORD VAULT - Ref: BAMBOO-API-001] |
| Subdomain: | momentumsports |
| Employee Count: | 16 core + 45 contractors/casual |

# ACCESS MANAGEMENT PROCEDURES

## New Employee Onboarding

|  |  |
| --- | --- |
| Timeline | Action |
| Day -3 | HR submits access request form to IT with job description and start date |
| Day -2 | IT creates accounts in all required systems based on role template |
| Day -1 | IT sends welcome email with temporary credentials (24-hour expiry) |
| Day 1 - Morning | Employee completes password setup and MFA enrollment during orientation |
| Day 1 - Afternoon | IT verifies successful login to all systems |
| Day 5 | IT reviews access with manager to confirm appropriate permissions |
| Day 30 | Automated review - confirm employee is using assigned systems |

## Employee Offboarding

|  |  |
| --- | --- |
| Timeline | Action |
| Notice Given | HR notifies IT of pending departure with last working date |
| 1 Week Before | IT prepares offboarding checklist, identifies data/knowledge transfer needs |
| Last Day - 5pm | Manager confirms employee has completed handover |
| Last Day - 6pm | IT disables all system access (except email for transition) |
| Last Day + 1 | IT resets passwords for any shared accounts employee had access to |
| Last Day + 3 | Email forwarding setup to manager (30-day auto-forward) |
| Last Day + 30 | Email account converted to shared mailbox or deleted per retention policy |
| Last Day + 90 | Final review - confirm no orphaned access, document archival complete |

## Access Change Request Process

All access changes must be requested through IT ticketing system with manager approval.

* New system access required
* Elevated permissions (level increase)
* Additional module/feature access
* Transfer to new role/department
* Temporary access for project work
* Access removal/reduction

**Required Information:**

* Employee name and ID
* System(s) requiring access change
* Specific permissions or access level needed
* Business justification
* Duration (if temporary)
* Manager approval (digital signature or email confirmation)

*SLA: Standard requests processed within 24 hours. Emergency requests within 4 hours.*

# EMERGENCY ACCESS PROCEDURES

## Break-Glass Accounts

Break-glass accounts provide emergency access when primary administrators are unavailable. These accounts are monitored and usage triggers immediate alerts to executive team.

|  |  |  |
| --- | --- | --- |
| System | Break-Glass Account | Password Location |
| NetSuite ERP | emergency.admin@momentumsports.com.au | Physical safe + Password vault |
| Microsoft 365 | breakglass@momentumsports.com.au | Physical safe + Password vault |
| AWS Root | aws-emergency@momentumsports.com.au | Physical safe ONLY (not in vault) |
| Network Firewall | admin (local account) | Physical safe + Password vault |

## Emergency Contact Tree

In case of security incident or system compromise requiring immediate credential changes:

|  |  |  |  |
| --- | --- | --- | --- |
| Priority | Contact | Method | Availability |
| Primary | Charlie Nguyen (CTO) | +61 4xx-xxx-7821 | Available 24/7 |
| Secondary | Alex Morgan (GM) | +61 4xx-xxx-3492 | Business hours + urgent |
| Tertiary | External IT Support | support@itpartner.com.au | +61 1800-xxx-xxx |
| After Hours | IT Emergency Hotline | emergency@momentumsports.com.au | Monitored 24/7 |

## Incident Response - Compromised Credentials

1. Immediately disable compromised account(s)

2. Reset passwords for affected systems

3. Review audit logs for unauthorized access

4. Notify affected users and stakeholders

5. File incident report with details and timeline

6. Conduct post-incident review within 48 hours

7. Update this document if procedures need revision

# APPENDIX

## A. Password Vault Information

All sensitive credentials referenced in this document are stored in our enterprise password management system (1Password Teams).

|  |  |
| --- | --- |
| Password Vault: | 1Password Teams |
| Vault URL: | https://momentumsports.1password.com |
| Master Account: | Held by CTO only (air-gapped storage) |
| Access: | CTO, IT Admin (full) | GM (read-only emergency) |
| MFA: | YubiKey hardware token required |
| Backup: | Encrypted backup in physical safe (weekly) |

## B. Physical Safe Location

Critical credentials and break-glass passwords are stored in physical safe:  
  
Location: IT Server Room, Level 3, Melbourne HQ  
Safe Type: FireKing 2-hour fire rating  
Combination: Known only to CTO and GM (separate envelopes with lawyer)  
Contents: Break-glass passwords, backup encryption keys, certificate private keys  
Access Log: Maintained (sign in/out required)

## C. System Access Review Schedule

|  |  |  |
| --- | --- | --- |
| Review Type | Frequency | Responsible Party |
| User Access Rights | Quarterly | IT Admin + Department Managers |
| Admin Credentials Rotation | Every 90 days | CTO |
| This Document Update | Quarterly or after changes | CTO |
| Security Audit | Annually | External Auditor |

## D. Compliance & Regulatory Notes

Access control procedures documented in this document support compliance with:

* Australian Privacy Act 1988 (APP 11 - Security of personal information)
* PCI DSS Requirements 7 & 8 (Access control and user authentication)
* GDPR Article 32 (Security of processing) for European customer data
* ISO 27001:2013 - Access Control (A.9)
* SOC 2 Type II - Logical Access Controls

**END OF DOCUMENT**

© 2026 Momentum Sports. All Rights Reserved.

**🔒 HIGHLY CONFIDENTIAL - RESTRICTED ACCESS 🔒**