Access Control Policy

FitZone Health & Wellness Pvt. Ltd.

1. Purpose/Objective

The purpose of this Access Control Policy is to establish a framework for managing and controlling access to FitZone's information systems, applications, data, and physical facilities. This policy aims to:

- Ensure that only authorized individuals have access to information systems and data based on legitimate business needs
- Implement the principle of least privilege, granting minimum access rights necessary for job functions
- Protect the confidentiality, integrity, and availability of member data, business information, and IT resources
- Prevent unauthorized access, data breaches, and insider threats
- Establish clear processes for granting, reviewing, modifying, and revoking access rights
- Ensure compliance with ISO 27001:2022, DPDP Act 2023, and other applicable regulations

---

2. Scope

This policy applies to:

- **Personnel:** All FitZone employees (permanent, temporary, contract), trainers, nutritionists, front desk staff, management, IT staff, interns, third-party vendors, contractors, and any individuals requiring access to FitZone systems or facilities
- **Access Types:**
  - Logical access: IT systems, applications, databases, networks, cloud services
  - Physical access: Office premises, server rooms, data centers, restricted areas

    - Data access: Member personal information, health records, payment data, business confidential information
- **Systems and Applications:**
    - Membership management system (GymTech Solutions platform)
    - Mobile applications (staff and member-facing)
    - Payment processing systems
    - Email and communication platforms
    - Cloud services (AWS)
    - Network infrastructure
    - CCTV and surveillance systems
    - Biometric access control systems
    - HR and payroll systems
    - Financial systems
- **Locations:** All 5 FitZone fitness centers across Mumbai, Pune, and Bangalore

---

3. Policy Statement

3.1 Access Control Principles

FitZone's access control framework is based on the following fundamental principles:

3.1.1 Principle of Least Privilege

- Users shall be granted the minimum level of access rights necessary to perform their job functions
- Access beyond business requirements must be explicitly justified and approved
- Default access level for new users should be "read-only" unless write/modify access is required

3.1.2 Need-to-Know Basis

- Access to sensitive data (member personal information, health records, payment data, financial information) shall be restricted to individuals with legitimate business need

- Casual browsing or curiosity-driven access to member data is prohibited

3.1.3 Segregation of Duties

- Critical business functions shall be divided among multiple individuals to prevent fraud and errors
- No single individual should have complete control over critical transactions (e.g., payment processing requires separate authorization and execution roles)
- System administrators must not have access to production financial data without business justification

3.1.4 Role-Based Access Control (RBAC)

- Access rights shall be assigned based on predefined roles aligned with job functions
- Standard roles minimize administrative overhead and ensure consistency
- Users may be assigned to multiple roles if job responsibilities require

3.1.5 Defense in Depth

- Multiple layers of access controls shall be implemented (network, application, data level)
- Authentication mechanisms shall be strengthened for access to sensitive systems (multi-factor authentication)

---

4. Access Control Roles and Responsibilities

4.1 Standard Access Roles

FitZone defines the following standard access roles:

Role Name	Job Functions	Systems Access	Data Access	Approval Required
Member Services - Front Desk	Membership registration, check-in, class bookings, basic inquiries	Membership system (limited), Payment terminals, Email	Member basic information (name, contact, membership status), Class schedules	Direct Manager

Role Name	Job Functions	Systems Access	Data Access	Approval Required
Personal Trainer	Fitness assessments, training plans, progress tracking	Membership system (trainer module), Mobile app	Member fitness data, health assessments, training records for assigned clients only	Fitness Manager
Nutritionist	Dietary consultations, meal planning	Membership system (nutrition module), Mobile app	Member health data, dietary restrictions, nutrition plans for assigned clients only	Wellness Manager
Front Desk Supervisor	Team management, member issue resolution, reporting	Membership system (extended access), Payment systems, Reporting tools	Member information, financial reports (location-level), Staff schedules	Location Manager
Location Manager	Operations management, staff oversight, financial management	Full location systems access, HR portal, Financial systems	All member data for assigned location, Financial data, Staff information	Regional Manager
IT Support	Technical support, system maintenance, troubleshooting	All IT systems (administrative access), Network infrastructure	System logs, Configuration data, Limited member data for troubleshooting only	IT Manager
IT Administrator	System administration, security management, infrastructure	Full administrative access to all IT systems	All data for legitimate administrative purposes, Audit logs	CISO
Finance Team	Billing, accounts,	Financial systems,	Financial data, Payment	Finance Manager

Role Name	Job Functions	Systems Access	Data Access	Approval Required
	financial reporting	Payment reports, Accounting software	transactions (aggregated), Member billing information	
HR Department	Employee management, recruitment, payroll	HR systems, Payroll software, Employee portal	Employee personal data, Salary information, Performance records	HR Manager
Management / Executives	Strategic decisions, business oversight	Reporting dashboards, Financial systems, BI tools	Aggregated business reports, Financial summaries, Strategic data	CEO
Auditor (Internal/External)	Compliance audits, security assessments	Read-only access to audited systems	Data relevant to audit scope	CISO + Legal
Third-Party Vendor	Contracted services (cleaning, maintenance, marketing)	Limited/no system access unless specifically required	No member data access unless covered by DPA	Procurement + IT Manager

4.2 Responsibilities

4.2.1 Access Requestor (Employee/User)

- Submit formal access request when starting employment or when job role changes
- Provide business justification for access requirements
- Acknowledge understanding of acceptable use policies
- Protect authentication credentials (passwords, tokens, access cards)
- Report suspicious access activity or compromised credentials immediately
- Return all access credentials and devices upon termination or role change

4.2.2 Line Manager / Department Head

- Review and approve access requests for direct reports
- Ensure access rights align with job responsibilities
- Notify IT Department and HR of role changes, promotions, transfers, or terminations within 24 hours
- Participate in quarterly access reviews for team members
- Ensure staff complete security awareness training

4.2.3 IT Department

- Implement approved access requests within agreed SLA (24-48 hours)
- Configure access rights according to predefined roles
- Maintain accurate records of access provisioning and changes
- Conduct periodic access rights reviews
- Revoke access immediately upon notification of termination or role change
- Monitor and log access to sensitive systems
- Respond to access-related incidents and investigations

4.2.4 Information Security Officer / CISO

- Define and maintain access control roles and permissions
- Review high-risk or sensitive access requests
- Conduct quarterly access rights audits
- Investigate unauthorized access incidents
- Recommend improvements to access control mechanisms
- Ensure compliance with ISO 27001 and DPDP Act requirements

4.2.5 Human Resources Department

- Notify IT Department of new hires, role changes, and terminations
- Ensure access requests are completed during onboarding
- Coordinate offboarding process including access revocation
- Maintain records of access approvals for compliance purposes

---

5. Access Request and Approval Process

5.1 Access Request Workflow

Step 1: Access Request Initiation

- **New Employees:** HR initiates access request as part of onboarding process
- **Existing Employees (role change):** Employee or manager submits access request via IT Service Portal or email to itsupport@fitzone.in
- **Contractors/Vendors:** Procurement or project manager submits access request with contract details

Step 2: Request Details
Access request must include:

- Employee name, ID, department, location
- Job role and reporting manager
- Requested systems/applications and access level
- Business justification for access
- Duration (for temporary access)
- Urgency and required date

Step 3: Manager Approval

- Direct manager reviews and approves/rejects request
- Manager verifies business need and appropriateness of access level
- Manager approval documented via email or IT ticketing system

Step 4: IT Security Review (for sensitive access)

- Requests for administrative access, financial systems, or direct database access require additional IT Security approval
- IT Security assesses risk and may request additional information or compensating controls

Step 5: Access Provisioning

- IT Department provisions access according to approved request
- Default passwords provided securely (not via email)
- User must change default password upon first login

- Access provisioning typically completed within:
  - Standard requests: 24-48 hours
  - Urgent requests (approved by manager): 4-8 hours
  - Sensitive access (requiring security review): 3-5 business days

Step 6: Confirmation and Documentation

- IT Department confirms access has been provisioned
- User acknowledges receipt and tests access
- Access grant recorded in access management database

5.2 Temporary/Guest Access

For contractors, auditors, or temporary workers requiring short-term access:

- **Duration:** Maximum 90 days; extension requires re-approval
- **Monitoring:** Temporary accounts are flagged for enhanced monitoring
- **Restrictions:** Limited to specific systems based on project scope
- **Automatic expiration:** Accounts automatically disabled upon expiration date
- **Renewal process:** If access is needed beyond initial period, new approval required with updated justification

5.3 Emergency Access

In urgent situations requiring immediate access (e.g., covering for absent colleague, incident response):

- **Verbal approval:** Manager may provide verbal approval documented in writing within 24 hours
- **Temporary elevation:** Access granted on temporary basis (maximum 7 days)
- **Enhanced logging:** Emergency access activities are logged and reviewed
- **Post-incident review:** Emergency access justification reviewed by IT Security

---

6. Authentication Requirements

6.1 User ID and Password Standards

6.1.1 User ID Requirements

- User IDs must be unique and tied to individual identity (no shared accounts except for approved service accounts)
- User ID format: firstname.lastname or employee ID
- Generic accounts (e.g., "frontdesk", "admin") are prohibited except for approved service accounts with documented ownership

6.1.2 Password Requirements

Minimum Standards:

- **Length:** Minimum 12 characters (14+ characters recommended)
- **Complexity:** Must contain at least three of the following:
  - Uppercase letters (A-Z)
  - Lowercase letters (a-z)
  - Numbers (0-9)
  - Special characters (!@#$%^&*)
- **History:** Cannot reuse last 5 passwords
- **Expiration:** Passwords expire every 90 days
- **Lockout:** Account locked after 5 consecutive failed login attempts (unlocked by IT support after identity verification)

Prohibited Passwords:

- Dictionary words or common passwords (e.g., "Password123")
- Personal information (name, birthday, employee ID)
- Sequential characters (e.g., "123456", "abcdef")
- Keyboard patterns (e.g., "qwerty")

Password Management:

- Passwords must never be written down or stored in plain text
- Use of approved password manager (LastPass/1Password) is mandatory for storing work passwords
- Passwords must not be shared via email, chat, or phone
- Default/temporary passwords must be changed upon first login

6.2 Multi-Factor Authentication (MFA)

Multi-factor authentication is **mandatory** for:

- All administrative accounts (IT administrators, system administrators)
- Remote access (VPN, remote desktop)
- Access to financial systems and payment platforms
- Access to systems containing sensitive member data (direct database access)
- Cloud service administrator accounts (AWS, SaaS platforms)

MFA is **recommended** for:

- All staff accessing membership management system
- Email access from non-corporate devices

Approved MFA Methods:

- SMS one-time password (OTP) to registered mobile number
- Authenticator app (Google Authenticator, Microsoft Authenticator)
- Hardware tokens (for highly privileged accounts)

6.3 Privileged Account Management

Privileged accounts (system administrators, database administrators, application administrators) require enhanced controls:

- **Separate accounts:** Administrators must have separate accounts for administrative tasks (admin account) and normal daily work (user account)
- **Enhanced authentication:** MFA mandatory for all privileged access
- **Session recording:** Administrative sessions may be recorded for audit purposes
- **Access logging:** All privileged activities logged and reviewed monthly
- **Approval workflow:** Privileged access requests require CISO approval
- **Regular review:** Privileged access reviewed monthly and recertified quarterly

---

7. Access Review and Recertification

7.1 Periodic Access Reviews

Access rights shall be reviewed on the following schedule:

Access Type	Review Frequency	Reviewer	Documentation
Standard user access (front desk, trainers, nutritionists)	Quarterly	Department Managers	Review sign-off recorded in access management system
Privileged/administrative access	Monthly	IT Security Officer	Detailed review report with findings
Terminated employee access verification	Weekly	IT Administrator	Automated report from identity management system
Contractor/vendor access	Monthly	Procurement + IT Security	Contractor access register
Financial system access	Quarterly	Finance Manager + IT Security	Finance access review report

7.2 Review Process

Step 1: Access Report Generation

- IT Department generates access rights reports listing all users and their access levels

Step 2: Manager Review

- Managers review access rights for their team members
- Verify each user's access aligns with current job responsibilities
- Identify any:
  - Excessive access (more than required)
  - Orphaned accounts (users who have left or changed roles)
  - Dormant accounts (no login activity for 60+ days)

Step 3: Action Items

- Managers document required changes (revoke, modify, retain)
- Submit review sign-off to IT Department

Step 4: Remediation

- IT Department implements approved changes within 5 business days
- Dormant accounts disabled and flagged for removal

Step 5: Reporting

- IT Security compiles review summary for management
- Metrics tracked: % accounts reviewed, accounts modified/revoked, time to remediate

7.3 Automated Access Reviews

Where technically feasible, implement automated tools to:

- Flag dormant accounts (no login for 60 days)
- Identify access anomalies (user has access to systems outside their department)
- Alert on privilege creep (accumulation of access rights over time)
- Generate access certification reports

---

8. Access Modification and Revocation

8.1 Access Modification (Role Change)

When employee changes roles:

- Manager submits access modification request detailing:
  - Old role and current access
  - New role and required access
  - Effective date of change
- IT Department:
  - Removes access no longer required
  - Provisions new access as approved
  - Documents changes in access management system
- **Timeline:** Access changes completed within 24 hours of approval

8.2 Access Revocation (Termination/Resignation)

Immediate Revocation (Termination for Cause, Security Incidents):

- HR notifies IT Department and Security immediately
- IT disables all accounts and access within 1 hour
- Physical access cards deactivated immediately

- Remote access (VPN, email) terminated
- Retrieve all company devices and access credentials

Standard Offboarding (Resignation, Retirement, End of Contract):

- **Notice period (2-4 weeks before last day):**
  - HR notifies IT of planned departure date
  - IT prepares offboarding checklist
- **Last working day:**
  - All system access revoked end of business day
  - Email account converted to auto-reply (forwarding to manager for 30 days if required)
  - Physical access cards collected
  - Company devices returned
- **Post-departure:**
  - Email account retained for 30 days (read-only access for manager)
  - Data archived per retention policy
  - Accounts permanently deleted after retention period

8.3 Offboarding Checklist

IT Department ensures the following are completed:

- ☐ All system accounts disabled
- ☐ Email access revoked/converted to forwarding
- ☐ VPN/remote access terminated
- ☐ Cloud service accounts (AWS, SaaS) access removed
- ☐ Physical access badges deactivated
- ☐ Company laptop/tablet retrieved and wiped
- ☐ Mobile device (if BYOD) company data wiped remotely
- ☐ Two-factor authentication tokens deactivated
- ☐ Shared drives access removed
- ☐ Application-specific access revoked (membership system, financial systems)

☐ Manager notified of completion

9. Physical Access Control

9.1 Physical Access Zones

FitZone facilities are divided into access zones:

Zone	Description	Access Control Method	Authorized Personnel
Public Zone	Gym floor, reception, common areas	Open to members during operating hours	All members and staff
Staff Zone	Staff rooms, back office, break rooms	Biometric/card access	Employees only
Restricted Zone	IT server room, CCTV storage, management offices	Biometric + PIN	IT staff, management, authorized personnel
Highly Restricted	Financial records storage, safe	Dual authentication + key	Finance manager, CEO

9.2 Physical Access Control Mechanisms

- **Main entrance:** Member check-in via biometric fingerprint scanner or membership card
- **Staff areas:** RFID access card or biometric authentication
- **Server rooms:** Biometric + PIN + logged entry/exit
- **CCTV monitoring:** 24/7 surveillance of restricted areas with recording

9.3 Visitor Access

Visitors (vendors, contractors, auditors, guests) must:

- Sign in at reception providing name, company, purpose of visit
- Display visitor badge at all times
- Be escorted by authorized employee in staff/restricted zones
- Sign out upon departure
- Visitor logs retained for 1 year

9.4 Physical Access Reviews

- **Monthly:** Review access card/biometric enrollment list
- **Quarterly:** Verify physical access rights align with current roles
- **After-hours access:** Logged and reviewed for anomalies

---

10. Service Accounts and Non-Human Access

Service accounts (application-to-application, automated processes) require special handling:

- **Documentation:** All service accounts documented with purpose, owner, and systems accessed
- **Authentication:** Service accounts use strong, randomly generated passwords (20+ characters)
- **Storage:** Service account credentials stored in secure vault (password manager or secrets management system)
- **No interactive login:** Service accounts cannot be used for interactive user sessions
- **Monitoring:** Service account activity logged and monitored for anomalies
- **Ownership:** Each service account must have a designated owner responsible for access review
- **Review:** Service accounts reviewed quarterly; unused accounts disabled

---

11. Remote Access

Remote access to FitZone systems is permitted under the following conditions:

11.1 Remote Access Methods

Approved Methods:

- **VPN (Virtual Private Network):** Mandatory for remote access to internal systems
- **Web-based applications:** Membership system, email accessible via secure web portal
- **Mobile apps:** Official FitZone mobile application for approved staff functions

Prohibited Methods:

- Direct remote desktop (RDP) without VPN
- Unsecured protocols (Telnet, FTP without TLS)
- Third-party remote access tools (TeamViewer, AnyDesk) without IT approval

11.2 Remote Access Requirements

- **MFA mandatory:** All remote access requires multi-factor authentication
- **Corporate VPN:** Remote access to internal systems must route through corporate VPN
- **Secure device:** Remote access only from devices meeting security standards (see BYOD Policy)
- **Public Wi-Fi precautions:** Avoid sensitive transactions on public Wi-Fi; use VPN if unavoidable
- **Geographic restrictions:** Remote access from high-risk countries may be blocked
- **Session timeout:** Remote sessions automatically disconnect after 30 minutes of inactivity

---

12. Access Logging and Monitoring

12.1 Logging Requirements

The following access activities shall be logged:

- User login/logout (successful and failed attempts)
- Access to sensitive data (member health records, payment information)
- Administrative actions (account creation, permission changes, system configuration)
- Failed authorization attempts
- Privileged access sessions
- Remote access connections

12.2 Log Retention

- Access logs retained for minimum 1 year
- Logs for incidents and investigations retained per legal requirements (typically 3-7 years)

- Logs stored securely with restricted access to IT Security and authorized investigators

12.3 Monitoring and Alerting

Automated alerts triggered for:

- Multiple failed login attempts (potential brute force attack)
- Login from unusual location/device
- Privileged account activity outside business hours
- Bulk data downloads or exfiltration attempts
- Access to terminated employee accounts
- Dormant accounts suddenly becoming active

---

13. Compliance and Enforcement

13.1 Consequences of Policy Violations

Violations of this Access Control Policy will result in disciplinary action:

Examples of violations:

- Sharing passwords or access credentials
- Accessing systems or data without authorization
- Maintaining excessive access beyond business need
- Failing to report compromised credentials
- Bypassing access controls or authentication mechanisms

Disciplinary actions:

- First offense: Written warning and security awareness retraining
- Repeated violations: Suspension of access privileges, formal performance review
- Serious violations: Immediate termination, legal action

13.2 Compliance Monitoring

- Quarterly access reviews to verify policy compliance
- Annual audit of access control processes by internal or external auditors

- Metrics reported to management: access request fulfillment time, dormant accounts, orphaned access, review completion rate

---

14. Compliance References

This policy supports compliance with:

- **ISO 27001:2022:**
  - Control 5.15: Access Control
  - Control 5.16: Identity Management
  - Control 5.17: Authentication Information
  - Control 5.18: Access Rights
  - Control 8.2: Privileged Access Rights
  - Control 8.3: Information Access Restriction
  - Control 8.5: Secure Authentication
- **DPDP Act 2023:** Data security safeguards and access restrictions to personal data
- **Payment Card Industry DSS (PCI-DSS):** Access control requirements for payment card data

---

15. Related Documents

- Acceptable Use Policy
- Password Policy (may be standalone or integrated here)
- BYOD (Bring Your Own Device) Policy
- Incident Response Policy
- Identity and Access Management Procedures
- Offboarding Checklist
- Remote Access Guidelines

---

16. Policy Review and Maintenance

- **Review Frequency:** Annually or when significant changes occur (new systems, regulatory changes, organizational restructuring)

- **Update Approval:** Changes require approval from CISO and CEO
- **Version Control:** All policy versions maintained with change log
- **Communication:** Updated policy communicated to all staff with mandatory acknowledgment

---

Document Control:

Policy Owner: Chief Information Security Officer

Version: 1.0

Effective Date: November 1, 2025

Last Reviewed: October 15, 2025

Next Review Date: November 1, 2026

Approved By: Chief Executive Officer, Chief Information Security Officer