Acceptable Use Policy (AUP)

FitZone Health & Wellness Pvt. Ltd.

1. Purpose/Objective

The purpose of this Acceptable Use Policy is to establish guidelines and rules for the appropriate and secure use of FitZone's information technology resources, including computer systems, networks, Wi-Fi infrastructure, applications, and data. This policy aims to:

- Protect the confidentiality, integrity, and availability of FitZone's information assets and member data
- Ensure compliance with legal, regulatory, and contractual obligations
- Prevent misuse of IT resources that could harm FitZone's reputation, operations, or security posture
- Define acceptable and unacceptable behaviors when using FitZone's IT infrastructure
- Establish accountability and consequences for policy violations

2. Scope

This policy applies to:

- **Personnel:** All FitZone employees (trainers, nutritionists, front desk staff, management, IT staff), contractors, interns, temporary workers, and third-party vendors
- **Systems and Resources:** All IT resources owned, leased, or managed by FitZone including:
  - Membership management system and customer databases
  - Mobile applications (staff and member-facing)
  - Company-provided tablets and workstations at front desk
  - Personal devices used for work purposes (BYOD - see related BYOD Policy)

    - Corporate Wi-Fi network (staff network)
    - Guest Wi-Fi network (available to members)
    - Email systems and communication platforms
    - Cloud services and SaaS applications
    - Physical network infrastructure (routers, switches, access points)
    - CCTV systems and surveillance footage
    - Biometric access control systems
- **Locations:** All 5 FitZone fitness centers across Mumbai, Pune, and Bangalore, including any future locations
- **Data:** All business data, member personal information, health records, payment information, and intellectual property

---

3. Policy Statement

3.1 Authorized Use

FitZone IT resources are provided for **legitimate business purposes only**. Authorized uses include:

- Accessing membership management system to perform job-related tasks (registrations, class bookings, payment processing)
- Using mobile applications for scheduling, communication, and operational tasks
- Accessing email and approved communication tools for work-related correspondence
- Utilizing Wi-Fi for business activities including member services
- Accessing training materials, policies, and work-related documentation
- Reasonable personal use of Wi-Fi during breaks is permitted, provided it does not:
    - Interfere with work responsibilities
    - Violate any provisions of this policy
    - Consume excessive bandwidth affecting business operations

3.2 Prohibited Activities

The following activities are **strictly prohibited** when using FitZone's IT resources:

3.2.1 Security Violations

- Attempting to gain unauthorized access to systems, networks, or data not required for job functions
- Sharing login credentials, passwords, or authentication tokens with others
- Circumventing or disabling security controls, firewalls, or access restrictions
- Using default or weak passwords (see Access Control Policy for password requirements)
- Installing unauthorized software, applications, or browser extensions without IT approval
- Connecting unauthorized devices to the corporate network without IT Department permission
- Attempting to intercept, monitor, or capture network traffic or communications
- Port scanning, vulnerability scanning, or penetration testing without explicit written authorization from IT Security
- Creating, distributing, or executing malicious code (viruses, malware, ransomware, trojans)

3.2.2 Data Protection Violations

- Accessing, copying, or sharing member personal data, health information, or payment details without legitimate business need and proper authorization
- Storing sensitive member data (PAN, Aadhaar, health records, payment information) on personal devices, USB drives, or unauthorized cloud services
- Sending member data via personal email accounts, WhatsApp, or unsecured messaging platforms
- Taking screenshots or photographs of member data displayed on screens

- Leaving workstations unlocked or unattended with member data visible
- Printing member data unnecessarily or leaving printed documents unattended
- Sharing member information with unauthorized third parties or family/friends
- Discussing member confidential information in public areas where others can overhear

3.2.3 Network and System Misuse

- Using peer-to-peer (P2P) file sharing applications on FitZone networks
- Streaming video content, online gaming, or other bandwidth-intensive activities that impact business operations
- Setting up unauthorized wireless access points, routers, or hotspots
- Bridging corporate network to guest Wi-Fi or external networks
- Using corporate network to host personal websites, servers, or services
- Deliberately introducing network congestion or attempting denial-of-service attacks
- Tampering with network equipment, cables, or infrastructure

3.2.4 Inappropriate Content and Communication

- Accessing, downloading, storing, or distributing illegal, offensive, or inappropriate content including:
  - Pornographic, sexually explicit, or adult content
  - Content promoting violence, hatred, discrimination, or harassment
  - Pirated software, movies, music, or copyrighted materials
  - Gambling or betting websites (except for occasional personal use during breaks)
- Sending harassing, threatening, abusive, or discriminatory messages via email or messaging platforms
- Engaging in cyberbullying, trolling, or online harassment of colleagues, members, or competitors

- Making defamatory statements about FitZone, its employees, or members on social media or online forums
- Representing personal opinions as official FitZone positions without authorization

3.2.5 Unauthorized Business Activities

- Using FitZone IT resources for personal business ventures, side businesses, or commercial activities
- Soliciting or conducting personal sales, fundraising, or political campaigns
- Job searching or recruiting for external organizations during work hours (occasional personal use during breaks is acceptable)
- Engaging in cryptocurrency mining or blockchain operations

3.2.6 Legal and Regulatory Violations

- Any activity that violates Indian laws including:
  - Information Technology Act, 2000 and amendments
  - Digital Personal Data Protection Act (DPDP Act), 2023
  - Payment and Settlement Systems Act, 2007
  - Indian Penal Code provisions related to cyber crimes
- Violating software licensing agreements or intellectual property rights
- Engaging in insider trading or unauthorized disclosure of confidential business information
- Money laundering, fraud, or other financial crimes

3.3 Wi-Fi Network Usage

3.3.1 Staff Wi-Fi Network

- Staff network access is granted based on job role and requires authentication with individual credentials
- Staff are responsible for activities conducted under their credentials
- Sharing staff Wi-Fi credentials with members, visitors, or unauthorized persons is strictly prohibited

- Staff network must not be used for illegal downloads, streaming copyrighted content, or accessing inappropriate websites

3.3.2 Guest Wi-Fi Network (Member Use)

- Guest Wi-Fi is provided as a courtesy to members and is subject to acceptable use guidelines
- Guest network is isolated from corporate systems and member data
- Members using guest Wi-Fi agree not to:
  - Attempt to access other users' devices or data on the network
  - Conduct any illegal activities including hacking, fraud, or downloading illegal content
  - Consume excessive bandwidth that impacts other users (streaming limits may apply)
  - Use the network for commercial purposes or business operations
- FitZone reserves the right to monitor guest network traffic for security purposes and may block or restrict access for policy violations
- Members have no expectation of privacy on guest Wi-Fi; all network activity may be logged

3.4 Email and Communication Systems

- Corporate email accounts are for business communication; reasonable personal use is permitted during breaks
- Employees must use professional language and maintain courteous tone in all business communications
- Automatic email forwarding to external personal accounts is prohibited
- Large attachments (>10MB) should be shared via approved file-sharing methods, not email
- Phishing emails or suspicious messages must be reported immediately to IT Security (security@fitzone.in) without clicking links or opening attachments
- Email retention policy requires business-critical emails to be retained per Records Retention Policy; casual correspondence may be deleted after 90 days

3.5 Mobile Devices and BYOD

- Employees using personal devices (smartphones, tablets, laptops) to access FitZone systems must comply with the BYOD Policy
- Personal devices must have screen lock enabled (PIN, password, biometric)
- Lost or stolen devices with access to FitZone systems must be reported immediately to IT Department
- FitZone reserves the right to remotely wipe corporate data from lost/stolen devices

3.6 Social Media Usage

- Personal social media use during work hours should be limited to breaks and should not interfere with job performance
- Employees are free to use social media on personal time but must not:
  - Disclose confidential FitZone information, member data, or business strategies
  - Post negative or defamatory content about FitZone, colleagues, or members
  - Use FitZone's name, logo, or brand without authorization from Marketing Department
  - Claim to represent FitZone's official position unless explicitly authorized
- If identifying as a FitZone employee on social media, include disclaimer: "Views expressed are my own and do not represent FitZone Health & Wellness"
- Authorized social media representatives must follow Social Media Guidelines (separate document)

3.7 Monitoring and Privacy

Users should have no expectation of privacy when using FitZone IT resources. FitZone reserves the right to:

- Monitor network traffic, internet usage, and email communications for security, compliance, and operational purposes
- Log and audit access to systems, applications, and member data

- Review files stored on company devices or cloud services
- Inspect devices connected to FitZone networks
- Retrieve and review communications, files, or data during investigations

Monitoring purposes include:

- Detecting security incidents and unauthorized access
- Investigating policy violations or suspected misconduct
- Ensuring compliance with legal and regulatory requirements
- Maintaining network performance and availability
- Protecting FitZone's reputation and business interests

Privacy safeguards:

- Monitoring will be conducted in accordance with applicable laws and with respect for employee dignity
- Access to monitoring data will be restricted to authorized personnel (IT Security, Management, Legal, HR)
- Monitoring data will be retained only as long as necessary for legitimate business purposes
- Employees will be notified of monitoring practices during onboarding

3.8 Bring Your Own Device (BYOD) Considerations

This section provides high-level guidance; refer to the dedicated **BYOD Policy** for detailed requirements:

- Personal devices accessing FitZone systems must meet minimum security standards
- FitZone reserves the right to enforce security controls on personal devices (e.g., mobile device management)
- Employees consent to partial device management affecting business data and applications only
- FitZone is not responsible for damage to personal devices or personal data loss during security incident response

3.9 Software and Application Usage

- Only approved, licensed software may be installed on company devices
- Requests for new software must be submitted to IT Department with business justification
- Pirated, cracked, or unlicensed software is strictly prohibited
- Open-source software requires IT Security review before deployment
- Personal software (games, utility tools) should not be installed on company devices without IT approval
- Employees must comply with software licensing terms and usage restrictions

3.10 Physical Security of IT Assets

- Workstations, tablets, and devices must be physically secured when not in use (locked in drawers or secure areas)
- Devices must not be left unattended in public areas, vehicles, or unsecured locations
- Screen privacy filters should be used in public-facing areas to prevent shoulder surfing
- Visitors, members, or unauthorized persons must not be allowed access to staff workstations or back-office systems
- Lost or stolen equipment must be reported immediately to IT Department and Security Department

---

4. Roles & Responsibilities

4.1 Employees / Users

- **Read and understand** this Acceptable Use Policy and acknowledge acceptance during onboarding
- **Use IT resources responsibly** and in accordance with policy guidelines
- **Protect authentication credentials** and do not share passwords or access with others
- **Report security incidents** immediately including suspected policy violations, phishing emails, malware infections, unauthorized access

attempts, data breaches

- **Attend security awareness training** annually and stay informed about security threats
- **Secure devices and workstations** by locking screens when stepping away and logging out at end of shift

4.2 IT Department

- **Implement and maintain technical controls** supporting this policy including firewalls, web filtering, network segmentation, access controls
- **Monitor systems and networks** for security threats and policy violations
- **Investigate security incidents** and suspected policy violations in coordination with HR and Management
- **Provide guidance and support** to users regarding acceptable use questions and secure IT practices
- **Maintain audit logs** of system access and network activity for compliance and investigation purposes
- **Update policy** periodically to address emerging threats and technology changes

4.3 Management / Department Heads

- **Ensure staff awareness** of this policy through onboarding and regular reminders
- **Model appropriate behavior** by complying with policy requirements
- **Report suspected violations** to IT Department and HR Department
- **Support enforcement actions** including disciplinary measures for policy violations
- **Approve business justifications** for special IT resource requests or exceptions

4.4 Human Resources Department

- **Include policy in onboarding** and obtain written acknowledgment from new employees

- **Coordinate disciplinary actions** for policy violations in consultation with IT and Management
- **Maintain records** of policy acknowledgments and security training completion
- **Conduct exit procedures** ensuring return of company devices and termination of access for departing employees

4.5 Information Security Officer / CISO

- **Oversee policy enforcement** and coordinate security awareness initiatives
- **Conduct periodic reviews** of policy effectiveness and recommend updates
- **Lead security investigations** for serious policy violations or security incidents
- **Report to management** on compliance metrics, incidents, and policy violation trends

---

5. Exceptions and Approval Process

Exceptions to this policy may be granted in rare circumstances for legitimate business needs:

- **Exception requests** must be submitted in writing to IT Security Officer with detailed business justification
- **Risk assessment** will be performed to evaluate security implications
- **Compensating controls** may be required to mitigate risks
- **Approval authority:** IT Security Officer for standard exceptions; CISO or Senior Management for high-risk exceptions
- **Documentation:** All approved exceptions must be documented with justification, approval authority, expiration date, and review frequency
- **Periodic review:** Exceptions will be reviewed quarterly and may be revoked if business need no longer exists

---

6. Compliance & Enforcement

6.1 Consequences of Violation

Violations of this Acceptable Use Policy will result in disciplinary action appropriate to the severity and frequency of the violation:

Minor violations (first-time, unintentional):

- Verbal warning and counseling
- Mandatory security awareness refresher training
- Increased monitoring of IT resource usage

Moderate violations (repeated minor violations or moderate-severity single violations):

- Written warning placed in employee file
- Temporary suspension of IT access privileges
- Formal performance improvement plan

Serious violations (intentional misconduct, data breaches, illegal activities):

- Suspension without pay pending investigation
- Termination of employment
- Revocation of all system access and credentials
- Legal action including:
  - Civil litigation for damages
  - Criminal prosecution under Information Technology Act, 2000, Indian Penal Code, or other applicable laws
  - Reporting to law enforcement authorities

Factors considered in determining disciplinary action:

- Intent (accidental vs. deliberate)
- Severity of harm or potential harm caused
- Whether member data or sensitive information was compromised
- Prior disciplinary history
- Cooperation during investigation
- Whether violation was reported voluntarily

6.2 Investigation Process

When policy violations are suspected:

1. **Initial report** received by IT Department, HR, or Management
2. **Preliminary assessment** conducted to determine severity and scope
3. **Evidence preservation** including logs, emails, files, and system activity
4. **Formal investigation** led by IT Security, HR, and Legal as appropriate
5. **Employee notification** and opportunity to provide explanation (unless doing so would compromise investigation)
6. **Findings documented** with evidence and recommendations
7. **Disciplinary action** determined by HR and Management based on findings
8. **Appeal process** available per HR policies if employee disputes findings

---

7. Compliance References

This policy supports compliance with the following standards and regulations:

- **ISO 27001:2022:**
  - Control 5.10: Acceptable Use of Information and Other Associated Assets
  - Control 5.15: Access Control
  - Control 5.16: Identity Management
  - Control 6.3: Information Security Awareness, Education and Training
  - Control 8.1: User Endpoint Devices
  - Control 8.16: Monitoring Activities
- **Digital Personal Data Protection Act (DPDP Act), 2023:** Principles of data minimization, purpose limitation, and security safeguards
- **Information Technology Act, 2000:** Provisions related to computer crimes, unauthorized access, and data protection
- **Payment Card Industry Data Security Standard (PCI-DSS):** Requirements for acceptable use of systems handling payment card data

---

8. Related Documents

- Access Control Policy
- BYOD (Bring Your Own Device) Policy
- Incident Response Policy
- Data Classification Policy
- Password Policy
- Network Security Policy
- Records Retention and Disposal Policy
- Social Media Guidelines
- Employee Handbook

---

9. Policy Review and Updates

- **Review frequency:** This policy will be reviewed annually or when significant changes occur to technology, threats, regulations, or business operations
- **Update approval:** Policy updates require approval from CISO, Legal Department, and Chief Executive Officer
- **Communication:** Policy updates will be communicated to all staff via email and posted on the employee portal
- **Re-acknowledgment:** Employees must re-acknowledge the updated policy within 30 days of publication

---

10. Contact Information

For questions, concerns, or to report policy violations:

- **IT Support (General Questions):** itsupport@fitzone.in | +91-22-xxxx-xxxx
- **IT Security (Security Incidents):** security@fitzone.in | +91-22-xxxx-xxxx
- **Human Resources (Policy Violations):** hr@fitzone.in | +91-22-xxxx-xxxx

---

11. Acknowledgment

I acknowledge that I have read, understood, and agree to comply with FitZone Health & Wellness Pvt. Ltd.'s Acceptable Use Policy. I understand that:

- FitZone IT resources are provided for business purposes and reasonable personal use
- I have no expectation of privacy when using FitZone systems, networks, or devices
- Violations may result in disciplinary action up to and including termination and legal prosecution
- I am responsible for protecting my authentication credentials and reporting security incidents
- I will attend required security awareness training and stay informed about security best practices

---

Employee Name: _____

Employee ID: _____

Department: _____

Signature: _____

Date: _____

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