



your world, seamlessly integrated.

INTEGRATED MANAGEMENT SYSTEM (IMS) MANUAL

Document Reference: WAW-ISO-IMS-2026-ULTIMATE

Effective Date: May 22, 2026

Regulatory Scope: ISO 9001, ISO 27001, ISO 14001, SOC 2

Official Contact: admin@wawlyn.com

1. EXECUTIVE POLICY STATEMENT AND SCOPE

1.1. WAWLYN Ecosystem hereby establishes this comprehensive Integrated Management System (IMS) manual to systematically eliminate operational loopholes, ensure absolute product reliability, and safeguard data integrity across our entire global footprint.

1.2. This framework universally governs our hardware design, manufacturing processes, supply chain logistics, software development lifecycle, and cloud operations. This explicitly includes our reliance on Vercel for edge deployment and Supabase for cloud database architecture.

2. QUALITY MANAGEMENT SYSTEM (QMS) - ISO 9001:2015

2.1. Uncompromising Quality: Our commitment to Quality Management ensures all hardware (Wyn Pad, Worbix, Wryny, Wypods) and software ecosystems meet exact tolerances, reliability standards, and statutory specifications.

2.2. Risk-Based Architecture (Clause 6.1): Comprehensive Failure Mode and Effects Analysis (FMEA) and Design for Manufacturability (DFM) reviews are conducted prior to any product launch, major firmware update, or manufacturing change.

2.3. Supplier Controls (Clause 8.4): All component suppliers (e.g., microprocessors, Lithium-ion batteries, AMOLED displays) are subjected to rigorous quarterly on-site and remote audits. Non-conforming suppliers are immediately excised from the supply chain and placed on a restricted vendor list.

2.4. Continuous Improvement (PDCA Cycle): Real-time field telemetry, RMA (Return Merchandise Authorization) data, and customer defect reports are algorithmically analyzed to trigger automated Corrective and Preventive Actions (CAPA) within our engineering ticketing systems.

3. INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) - ISO/IEC 27001:2022 & SOC 2

3.1. Data Centric Security: Protecting user privacy and proprietary Intellectual Property (IP) is our highest operational priority. Our ISMS is mapped to ISO 27001:2022 Annex A controls and SOC 2 Type II Trust Services Criteria (Security, Availability, Processing Integrity, Confidentiality, and Privacy).

3.2. Infrastructure Security (Supabase & Vercel): Our digital perimeter is secured via Vercel's enterprise edge network, providing inherent volumetric DDoS mitigation and Web Application Firewall (WAF) capabilities. Our data repository, Supabase, utilizes PostgreSQL with strict

Role-Based Access Control (RBAC) and Row Level Security (RLS). Database snapshots are encrypted and geo-redundant to ensure disaster recovery resilience.

3.3. Cryptography (Control 8.24): We mandate cryptographic hashing (Argon2) for user credentials, AES-256 for biometric and personal data at rest, and TLS 1.3 for all API endpoints and transit vectors.

3.4. Incident Response (Control 5.24): In the event of a security anomaly, our Security Operations Center (SOC) follows a rigid 4-tier escalation matrix, isolating compromised network nodes or blocking malicious IPs within milliseconds to prevent lateral movement or data exfiltration.

4. ENVIRONMENTAL MANAGEMENT SYSTEM (EMS) - ISO 14001:2015

4.1. Lifecycle Assessment (LCA): Every WAWLYN product undergoes rigorous LCA to evaluate its total carbon footprint from resource extraction to end-of-life disposal. We emphasize the integration of post-consumer recycled (PCR) plastics, conflict-free minerals, and sustainable packaging.

4.2. Waste Mitigation: We enforce strict zero-landfill policies at our primary assembly facilities, ensuring scrap materials are recycled, resold, or repurposed.

4.3. Continuous Monitoring: We continuously monitor Scope 1, Scope 2, and Scope 3 emissions across our entire supply chain to meet our aggressive carbon neutrality targets.

5. AUDIT TRANSPARENCY & NON-DISCLOSURE

5.1. While WAWLYN commits to maintaining these standards, detailed internal audit reports, third-party penetration test results, source code repositories, and SOC 2 Type II attestation reports are strictly classified as proprietary trade secrets.

5.2. External review by enterprise partners or regulatory bodies is permissible only under a countersigned, legally binding Non-Disclosure Agreement (NDA). Requests for audit reviews may be submitted to admin@wawlyn.com.