ISO / IEC 27001 Compliance Statement

Created On: September 15, 2025
Last Reviewed On: September 15, 2025

1. Introduction and Scope

Wytmode Cloud Private Limited ("Wytmode", "we", "our", or "us") maintains an information security management system ("ISMS") that is designed and operated in alignment with ISO/IEC 27001:2022. While Wytmode is not yet certified, our practices, processes, and procedures are structured to meet the requirements of the standard and to protect information across our organization. This statement applies to all Wytmode business lines and technology stacks, including Wytmode Workforce, PlanInsta, and Wytmode Passwords Manager, as well as corporate websites, internal systems, and back-office operations. It summarizes our governance, risk management, control environment, and continual improvement approach intended to preserve the confidentiality, integrity, and availability of information assets entrusted to us.

2. ISMS Overview and Objectives

Our ISMS establishes a systematic, risk-based framework for identifying, assessing, treating, and monitoring information security risks throughout the information lifecycle. Security objectives are set by leadership, cascaded through measurable key results, and reviewed at least annually to ensure they remain aligned to our strategic goals, legal and contractual obligations, and stakeholder expectations. The ISMS integrates with enterprise risk management so that security risk decisions are made in business context and are supported by appropriate resources, ownership, and timelines.

3. Governance, Leadership, and Roles

Information security is governed by senior management and overseen by designated ISMS leadership who are responsible for policy approval, risk acceptance, corrective actions, and continual improvement. Roles and responsibilities are defined and communicated through documented policies, charters, and operating procedures that bind employees, contractors, and third parties. Security decision-making is supported by cross-functional forums that include engineering, product, legal, HR, and operations to ensure that controls are embedded into day-to-day work.

4. ISMS Scope and Boundaries

The ISMS scope encompasses people, processes, and technologies used to design, host, deliver, and support Wytmode Workforce, PlanInsta, and Wytmode Passwords Manager, along with supporting corporate functions such as HR, finance, legal, procurement, and customer support. Scope boundaries include cloud platforms, development pipelines, production and staging environments, corporate endpoints, identity systems, and data repositories under Wytmode's control. Supplier-managed infrastructure is included through contractual and technical controls, while purely customer-owned environments are governed by customer contracts and are out of operational scope.

5. Risk Assessment and Treatment

Wytmode operates a documented methodology for risk assessment that identifies assets, threats, vulnerabilities, and business impacts, and evaluates inherent and residual risks using calibrated likelihood and impact scales. Risk treatment plans select controls consistent with ISO/IEC 27001 and its Annex A control set, supplemented by other frameworks where beneficial. Risks are tracked to closure with defined owners, milestones, and acceptance criteria, and results are reported to management for oversight and re-prioritization as conditions change.

6. Statement of Applicability and Control Selection

We maintain a Statement of Applicability ("SoA") that maps our controls to the ISO/IEC 27001:2022 Annex A control themes—organizational, people, physical, and technological—and documents whether each control is implemented, excluded with justification, or addressed through compensating measures. The SoA is reviewed on material change and at least annually to reflect new risks, technologies, and legal or contractual requirements, ensuring transparency in our control environment.

7. Organizational Controls and Policies

Wytmode's policy framework establishes mandatory requirements for information security, acceptable use, access control, cryptography, secure development, vulnerability management, incident response, business continuity, asset management, classification and handling, supplier security, and data protection. Policies are approved by leadership, versioned, communicated to personnel, and supported by detailed standards and procedures. Exceptions are formally recorded, risk-assessed, time-bound, and subject to management approval.

8. Human Resources Security and Awareness

Personnel security begins with lawful and proportionate background screening where permitted, reinforced by confidentiality agreements and role-specific access provisioning at onboarding. Employees and contractors receive security and privacy training at induction and at regular intervals, including secure coding for engineers and data

handling for staff with access to regulated data. Disciplinary processes address violations, and termination or role change triggers prompt access revocation and return or secure wiping of assets.

9. Asset Management and Data Classification

Information assets, including data sets, source code, configurations, devices, and cloud resources, are inventoried with assigned owners and classification labels reflecting sensitivity and regulatory obligations. Handling requirements, retention rules, and secure disposal methods correspond to classification levels to ensure that sensitive information receives appropriate protection throughout its lifecycle and that records are not retained longer than necessary.

10. Access Control and Identity Management

Access follows least-privilege and need-to-know principles enforced through role-based access control, strong authentication, and segregation of duties. Administrative access to production systems requires multi-factor authentication and is limited to a small group of trained personnel using hardened, monitored pathways. Access reviews occur at scheduled intervals and upon personnel changes, and privileged activity is logged and subject to heightened monitoring and investigation.

11. Cryptography and Key Management

Data in transit is protected with TLS configured to current industry standards, and data at rest is encrypted using proven algorithms and managed keys. Key management follows documented procedures for creation, rotation, storage, usage, and revocation, leveraging cloud key management services with access controls and audit trails. Cryptographic implementations are reviewed periodically to ensure alignment with evolving best practices and regulatory expectations.

12. Operational Security, Change, and Configuration Management

Operational controls include secure configuration baselines, hardening guides, vulnerability scanning, patch management, and separation of development, staging, and production environments. Changes are peer-reviewed, tested, and approved through automated pipelines with artifact integrity checks, reproducible builds, and roll-back plans. Infrastructure as code is scanned for misconfigurations, and production deployments are logged for traceability and audit.

13. Logging, Monitoring, and Threat Management

Security-relevant events are collected from applications, infrastructure, identity providers, and endpoints into centralized logging. Alerts are triaged based on severity and business impact, with documented runbooks guiding response. We employ anomaly detection, integrity monitoring, and rate-limiting to reduce attack surface, and we periodically test detective controls through tabletop exercises and targeted simulations to validate effectiveness.

14. Vulnerability and Patch Management

We operate continuous vulnerability assessment across code, containers, dependencies, and cloud resources, complemented by security testing such as SAST, SCA, DAST, and dependency monitoring. Remediation timeframes are defined by severity and exposure, and exceptions require risk acceptance with compensating controls. Emergency patch processes address actively exploited vulnerabilities with accelerated change windows and post-implementation review.

15. Secure Development Lifecycle

Security is embedded into our software development lifecycle through threat modeling, secure design reviews, code review practices, and automated security gates in CI/CD. Dependencies are pinned and verified, secrets are excluded from code repositories and managed through secret stores, and production data is not used in development or testing unless irreversibly anonymized. Engineers receive ongoing training in secure coding patterns, common weakness classes, and privacy-by-design.

16. Physical and Environmental Security

Physical security controls protect offices and any hosted equipment with access restrictions, visitor management, and device protection proportional to sensitivity and local risk. Endpoints are encrypted, monitored, and configured with screen-lock, device firewall, and remote wipe capabilities. Equipment moves and disposals follow secure chain-of-custody and certified destruction standards to prevent data leakage.

17. Supplier Security and Cloud Due Diligence

Third-party providers, including cloud platforms, authentication, hosting, analytics, and HR/payroll systems, undergo risk-based due diligence that evaluates certifications, independent attestations, technical controls, data residency, subcontracting, and incident practices. Contracts impose confidentiality, security, audit cooperation, breach notification, and data protection obligations, with Standard Contractual Clauses or equivalent measures used where international transfers are implicated. Supplier performance is periodically reviewed, and material issues trigger corrective actions or replacement.

18. Product-Specific Security Posture

Wytmode Workforce processes candidate and employee data in controlled HR systems with access segregation, encryption, and audit logging aligned to legal requirements. PlanInsta protects user accounts, plan content, and financial assumptions using authenticated sessions, encrypted transport, server-side authorization, and retention that respects user choices. Wytmode Passwords Manager employs a zero-knowledge architecture in which vault contents are encrypted client-side and remain opaque to Wytmode; this design minimizes provider access while placing responsibility on users to safeguard master credentials and recovery methods.

19. Information Transfer, Privacy, and Regulatory Alignment

Security controls are integrated with our privacy program to ensure that transfers of personal data occur lawfully and with appropriate safeguards. Where required, we implement data processing agreements, standard contractual clauses, and supplementary measures consistent with regulatory guidance. Security risk assessments incorporate privacy impacts, and our Cookies and Privacy Policies describe transparency, rights handling, and choices available to users.

20. Business Continuity and Disaster Recovery

Business continuity and disaster recovery are addressed through documented plans, resilient architectures, backups with routine restore testing, and defined recovery time and point objectives commensurate with service tiers. Scenario planning covers loss of facilities, provider outages, cyber incidents, and key personnel unavailability. Lessons learned from tests and incidents drive updates to plans and architectures to strengthen resilience.

21. Incident Response and Non-Conformance Management

We maintain an incident response process that covers preparation, identification, containment, eradication, recovery, and post-incident review. Roles and escalation paths are defined, and communications procedures address stakeholder and regulatory notifications where required by law or contract. Non-conformities discovered through audits, testing, or incidents are recorded, analyzed for root cause, and remediated through corrective and preventive actions tracked to closure.

22. Internal Audit, Management Review, and Continual Improvement

The ISMS is subject to periodic internal audits that evaluate conformity to ISO/IEC 27001 requirements and the effectiveness of implemented controls. Findings are reported to management and followed by corrective actions with due dates and owners. Management reviews are held at planned intervals to assess audit results, risk status,

control performance, incidents, feedback, legal and regulatory changes, and opportunities for improvement. Continual improvement is a standing objective, and metrics are used to measure progress and drive investment.

23. Training, Culture, and Accountability

Security is a shared responsibility reinforced by regular awareness campaigns, simulated exercises, and role-specific training. Policies are acknowledged by personnel, and violations are addressed through proportionate disciplinary processes. Leadership sponsorship, open reporting channels, and recognition for proactive risk identification cultivate a culture where secure behaviors are expected and rewarded.

24. Certification Roadmap and Assurance

Wytmode's near-term objective is to complete readiness activities and an external pre-assessment against ISO/IEC 27001:2022, followed by a staged certification audit conducted by an accredited certification body. Interim assurance is provided through this statement, independent penetration testing, and customer-driven assessments under appropriate non-disclosure agreements. Upon certification, we will publish our certificate details and scope statement and will maintain surveillance audits as required.

25. Updates, Versioning, and Contact

This ISO/IEC 27001 Compliance Statement is reviewed periodically and updated to reflect changes in our organization, technologies, suppliers, and regulatory environment. The effective date above identifies the current version. Questions about this statement, requests for additional technical details, or security disclosures can be directed to legal@wytmode.com