Howspace Security Whitepaper

***Trust is the foundation of every meaningful collaboration**. At Howspace, we've built our platform with a security-first mindset to protect your data and privacy. We believe that security shouldn't be a "black box," which is why we provide full transparency into our security posture and certifications. This overview is designed to provide the transparency and assurance you need to focus on driving impact within your organization. For additional information and detailed security resources, visit our Trust Center at trust.howspace.com.*

Howspace is a Collaborative Learning & Enablement Platform that helps organizations move from one-way training to active, collaborative learning. In one shared digital space, teams can design learning journeys, spark dialogue and co-creation, and turn participation into insight and action.

Howspace helps L&D and HR teams to:

- ***Enable collaborative learning:** Turn passive training into shared learning through dialogue, reflection, and co-creation.*
- ***Guide learning at scale:** Build structured yet flexible journeys that keep people engaged across teams and geographies.*
- ***Turn input into insight:** Use AI-powered sense-making to surface themes, track progress, and identify next steps.*

With a global presence, Howspace helps organizations build continuous, collaborative learning strategies where people drive real change together.

2. Security Certification & Compliance

*Howspace maintains a certified Information Security Management System (ISMS) in accordance with the **ISO/IEC 27001:2022** standard. This certification covers the development, provision, and management of the Howspace platform.*

- ***GDPR Compliance:** We strictly adhere to the General Data Protection Regulation (GDPR) and other applicable data protection laws to protect user privacy.*

- ***Transparency:*** *We provide real-time visibility into our system health and security status via our public status page at https://status.howspace.com/. For detailed security documentation, please visit trust.howspace.com.*
- ***Infrastructure Standards:*** *All hosting infrastructure is provided by AWS, which is ISO 27001 and SOC 2 Type II compliant.*

3. The Howspace Control Framework (HCF)

We don't just meet security standards; we harmonize them.
To maintain absolute transparency and protection, we developed the ***Howspace Control Framework (HCF)****—our organization's single source of truth for all security controls.*

The HCF is a unified security model built on the foundation of ***ISO 27001:2022*** *and rigorously tested against the safeguards of* ***NIST 800-171*** *and* ***SOC 2 Type II****. By synthesizing these global standards into one adaptable framework, we ensure that your data is protected by a consistent, high-impact taxonomy across 10 strategic domains.*

3.1. Governance, Risk & Policy

Our security organization is governed by a Security Steering Committee (SSC) that includes senior leadership. This ensures that security remains a business priority.

- ***ISMS Management:*** *We maintain a comprehensive ISMS reviewed annually for alignment with business and regulatory objectives.*
- ***Security Objectives:*** *The primary goal of our ISMS is to protect the confidentiality, integrity, and availability of information for our organization, employees, partners, and customers.*
- ***Risk Management:*** *Continual risk assessments are performed to identify and mitigate potential threats to the confidentiality, integrity, and availability of our services.*

3.2 Personnel Security & Training

Security is a collective responsibility at Howspace. We ensure our team is equipped to protect your data.

- ***Screening:*** *All personnel undergo mandatory background and identity checks prior to joining.*
- ***Training:*** *Employees participate in ongoing security awareness training, including specialized modules on AI usage and phishing defense.*
- ***Engagement:*** *Training and security updates are shared through a dedicated security workspace, ensuring all staff stay informed about evolving threats and internal best practices.*
- ***Confidentiality:*** *Strict non-disclosure and confidentiality agreements are a condition of every contract.*

3.3 Identity & Access Management

*We enforce the principles of **Need to Know** and **Least Privilege** across all systems.*

- ***Role-Based Access Control (RBAC):*** *We promote the use of RBAC to ensure that permissions are aligned with job functions.*
- ***Dual Control:*** *For sensitive actions or access to highly critical information, we implement the "four-eyes principle" to ensure oversight.*
- ***Authentication:*** *Multi-Factor Authentication (MFA) is mandatory for all production and administrative access.*
- ***Access Lifecycle:*** *We utilize automated provisioning and revocation, ensuring access is terminated within 24 business hours of a role change or departure.*
- ***Risk-Based Access Reviews:*** *We apply a risk-based approach to access governance. Access to critical systems is reviewed quarterly, while other systems are reviewed on a bi-annual to annual basis to ensure permissions remain strictly aligned with current job functions and roles.*

3.4 Configuration & Change Management

To maintain system integrity, we ensure all technical changes are controlled and documented.

- ***Change Control:*** *All infrastructure and application changes undergo change process, testing, and peer review before deployment.*
- ***Environment Isolation:*** *Development, testing, and production environments are strictly logically and physically isolated.*

- ***Vulnerability Management:*** *We maintain rigorous patching timelines, with critical vulnerabilities remediated within 72 hours.*

3.5 System & Network Protection

We implement active technical safeguards to protect our production environment from evolving threats.

- ***Network Segmentation:*** *Secure VPC architecture and firewalls prevent unauthorized lateral movement.*
- ***Monitoring:*** *24/7 security monitoring and logging provide real-time visibility into potential anomalies.*
- ***Hardening:*** *All systems follow industry-standard hardening baselines to minimize the attack surface.*

3.6 Asset & Media Protection

We inventory and protect organizational assets throughout their entire lifecycle.

- ***Data Classification:*** *Information is classified according to its sensitivity, with corresponding handling and protection requirements.*
- ***Secure Disposal:*** *We follow NIST-aligned procedures for the secure sanitization and disposal of media and data.*
- ***Encryption:*** *Customer data is encrypted at rest using AES-256 and in transit using TLS 1.2+.*

3.7 Physical Security

While our platform is cloud-hosted, we maintain strict security at our physical offices and processing facilities.

- ***Access Control:*** *Entry to Howspace facilities is restricted and monitored via electronic access control systems.*
- ***Clean Environment:*** *We enforce a "Clear Desk and Clear Screen" policy to ensure sensitive information is never left exposed.*

3.8 System Development & Operations

Security is integrated into every phase of our software development lifecycle (SDLC).

- ***Secure Coding:*** *Our developers follow secure coding guidelines based on industry best practices.*
- ***OWASP Alignment:*** *Our secure development practices are aligned with OWASP standards to mitigate common web application vulnerabilities.*
- ***Testing:*** *We conduct annual third-party penetration tests and maintain a continuous bug bounty program.*
- ***Operational Safety:*** *Production data is never used in non-production environments; synthetic data is used for all testing.*
- ***Quality Assurance:*** *All code changes undergo manual and automated security testing prior to deployment to production.*

3.9 Incident Response & Business Continuity

We maintain a robust capacity to respond to and recover from any disruption.

- ***Incident Management:*** *A formal Incident Response Plan (IRP) defines clear roles and reporting channels for rapid mitigation.*
- ***BCDR:*** *Automated, multi-region backups and high-availability architecture ensure a Recovery Point Objective (RPO) and Recovery Time Objective (RTO) that meet enterprise requirements.*
- ***Testing:*** *We conduct annual disaster recovery and incident response simulations to validate our readiness.*

3.10 Vendor & Third-Party Management

We ensure our partners adhere to the same high security standards that we set for ourselves.

- ***Vetting:*** *All sub-processors undergo a security assessment before being approved.*
- ***Monitoring:*** *We perform periodic reassessments of key vendors to ensure continued compliance with our HCF standards and GDPR requirements.*