WorkBoard

Security & Privacy Best Practices

Overview

WorkBoardAI is an **enterprise strategy execution platform** designed to help organizations define, align, and achieve their strategic objectives through a robust framework that integrates long-term strategies with quarterly OKRs. With features like **AI-powered assistance, real-time performance scorecards, automated business reviews, and seamless integrations** with tools like Microsoft Teams, Jira, Slack, and Asana, WorkBoard enhances organizational focus and agility. It enables dynamic meeting management, provides actionable insights, and ensures alignment across teams, fostering a high-performance, goal-driven culture that drives measurable results.

WorkBoard is committed to safeguarding customer data through a robust security and privacy framework. This document outlines WorkBoard's best practices for ensuring data integrity, availability and confidentiality, as well as its adherence to best industry security and privacy standards.

Security Framework & Compliance

WorkBoard's approach to security is built upon industry-leading standards, including:

- **SOC 2 Type 2**: Comprehensive compliance with Trust Services Criteria for Security, Availability, and Confidentiality.
- **ISO27001:2022:** Implementation of an Information Security Management System (ISMS) ensuring ongoing risk assessment and mitigation.
- **Microsoft Supplier Security and Privacy Assurance (SSPA) DPR Compliance:** Ensuring data protection and privacy standards meet Microsoft's stringent Data Protection Requirements (DPR).
- **GDPR Compliance**: Ensuring data protection rights for EU residents, including the right to be forgotten.

Customer Data

All data inputted by WorkBoard users and customers is categorized as **Confidential**, and the appropriate data protection and retention mechanisms are implemented following WorkBoard Security Policies and Processes.

WorkBoard **does not process or store Protected Health Information (PHI) or Payment Card Industry (PCI) data.** The platform is designed for enterprise strategy execution and alignment, not for handling sensitive medical or financial information. However, WorkBoard's processes adhere to security and privacy practices required for these particular data types.

Data Field Categories & Security Methods

Data Field	Category
Full Name	**PII**
Business Email Address	**PII**
Login Details	**Personal Data**
WorkBoard Usage (OKRs, AIs, etc.)	**User Input**

All **data is encrypted both in transit, TLS 1.2** or higher, and at rest, using **AES-256** encryption. Customers have the option to manage their own encryption keys via **Bring Your Own Key (BYOK) solution.**

Risk Management & Governance

WorkBoard maintains a formal risk management and governance framework to identify, evaluate, and mitigate risks across its operations and infrastructure. The approach includes:

- **Risk Assessments:** Regular assessments conducted to evaluate security, privacy, and operational risks, including those related to third-party vendors and infrastructure changes.
- **Policy Oversight:** A centralized governance model ensures WorkBoard's policies align with leading standards and regulatory requirements. Policies are reviewed and updated annually.
- **Control Monitoring**: Implementation of technical and organizational controls is continuously monitored to validate effectiveness.

- **Executive Oversight:** Risk management responsibilities are assigned to senior leadership, who oversee compliance, audit readiness, and strategic risk mitigation initiatives.

Infrastructure & Cloud Security

WorkBoard is a **Software-as-a-Service (SaaS)** solution delivered via the cloud. It is not available as an on-premise solution. Customers can access WorkBoard through secure web interface.

Microsoft Azure is a cloud infrastructure provider for WorkBoard. Data centers are located in Netherlands, as a Primary, and Ireland , as a Secondary, for EU Customers.

Physical security measures are in place to protect both data centers and office environment:

- **Data Centers**: Hosted in Microsoft Azure, are ISO 27001 certified and equipped with multi-layered security including biometric access controls, video surveillance, on-site security staff, and environmental controls.
- **Office Security**: WorkBoard's corporate office enforces badge-based access control, visitor logging, and secure area for IT equipment.

Infrastructure key practices include:

- **Network & Perimeter Security**: Enhanced monitoring and protection through continuous threat detection.
- **Data Encryption**: AES-256 encryption for data at rest and in transit. Additionally, encryption protocols include TLS 1.2/1.3 for network transmission security.
- **Redundancy & Availability**: Multi-availability zone deployments for failover support and high availability. The established **Recovery Time Objective (RTO)** is **4 hours** with a **Recovery Point Objective (RPO)** of **4 hours**.
- **Regular Backups**: Automated backups performed every **12 hours** with retention of **35 days**. Point-in-Time Recovery (PITR) is available within this window.
- **Disaster Recovery Exercises and Business Continuity:** Full disaster recovery drills are conducted annually to test all aspects of backup, recovery, and failover procedures. These exercises are intended to ensure readiness and validate the defined RTOs and RPOs.

- **Failover Mechanisms:** WorkBoard utilizes multi-availability zone deployments to provide failover support, ensuring uninterrupted service during infrastructure outages or other critical failures.
- **Monitoring & Detection:** Continuous monitoring using tools like Datadog ensures immediate identification of potential threats or failures, enabling rapid failover activation.

Application Protection

Security is incorporated throughout WorkBoard's Software Development Lifecycle (SDLC):

- **Unique Account IDs:** Every WorkBoard user must have a unique account ID (email address) to access the platform. This identifier is used to track user activity and enforce appropriate permissions.
- **Credential Protection:** Sign-in credentials are stored using a multi-level approach. Passwords are hashed using industry-standard SHA-2 algorithms and salted with unique, random data for added protection.
- **Password Requirements:** Passwords must meet complexity standards including:
    - Minimum of 9 characters
    - At least one uppercase and one lowercase letter
    - At least one numeric digit
    - At least one special character (e.g., ~!@#$%^&*)
- **Single Sign-On (SSO):** Supported through SAML 2.0, enabling secure integration with enterprise identity providers.
- **Secure Coding Standards**: Following best practices to prevent vulnerabilities.
- **Static & Dynamic Analysis**: Regular vulnerability scans, manual code reviews, and automated scanning using SAST, DAST, and infrastructure scanning tools.
- **Penetration Testing**: Annual external penetration testing conducted using OWASP methodologies, including post-remediation verification.
- **Patch Management**: WorkBoard conducts routine patching as part of its infrastructure lifecycle. Detected vulnerabilities are resolved through quality-

assured patch deployment. Emergency patches are applied immediately, with rollback support via system snapshots.

- **Vulnerability Management**: WorkBoard uses continuous vulnerability scanning and analysis tools to identify and address security risks across the application and infrastructure. Issues are prioritized based on severity and resolved within defined SLAs, with critical vulnerabilities remediated immediately.

Privileged User Accounts

WorkBoard enforces stringent controls over privileged user accounts to mitigate potential risks:

- **Access Restriction**: Privileged accounts are granted on a need-to-know basis, with strict adherence to the principle of least privilege.
- **Audit & Monitoring**: Continuous monitoring of privileged user actions, with audit logs retained for 90 days.
- **Separation of Duties**: Administrative roles are segregated from standard user roles to reduce risk of abuse or misuse.
- **MFA Enforcement**: All privileged user accounts require multi-factor authentication for access.

Organizational Security

WorkBoard maintains comprehensive security protocols for personnel and processes:

- **Adherence to Policies:** All employees are required to adhere to WorkBoard's security policies, including data protection, acceptable use, incident response, and access management policies.
- **Background Checks:** Background checks are performed as part of the hiring process.
- **Employee Screening & Training:** Security education and awareness training for all staff annually and based on need.
- **Logical Security:** Ensuring strict adherence to least privilege principles and role-based access controls (RBAC.

- **Access Control & Management:** Regular user permission reviews, automated monitoring, and stringent authentication processes.
- **End-User Device Management & Monitoring:** WorkBoard enforces endpoint security measures to protect devices accessing its systems. This includes antivirus software, encryption, patch management, and monitoring to detect and respond to suspicious activity.
- **Incident Response:** Continuous monitoring and rapid remediation procedures.

Enhanced GDPR Compliance Practices

The platform implements privacy-by-design principles and upholds transparency, accountability, and control over personal data processing.

Legal Basis for Data Processing

WorkBoard processes personal data under the following lawful bases as defined in Article 6 of the GDPR:

- **Contractual necessity** – to fulfill obligations related to the delivery of services to customers (e.g., managing user accounts, enabling platform functionality).
- **Legitimate interests** – to improve and secure the platform, provided such interests are not overridden by individual rights and freedoms.
- **Consent –** where applicable, for optional product features (e.g., marketing communications or beta programs).
- **Legal obligations** – where processing is necessary for compliance with applicable legal requirements.

Customers may reach out WorkBoard privacy team if there are any questions or concerns.

Data Protection Officer (DPO)

WorkBoard has appointed a Data Protection Officer (DPO) responsible for overseeing GDPR compliance and acting as a contact point for supervisory authorities and individuals.

Cross-Border Data Transfers & SCCs

- All data transfers are governed by Standard Contractual Clauses (SCCs) approved by the European Commission.
- Sub-processors and affiliates involved in processing EU personal data are contractually bound to adhere to equivalent data protection standards.
- WorkBoard regularly assesses the legal and regulatory environment of third countries and updates transfer impact assessments accordingly.

Data Subject Rights: Compliance with GDPR, including the right to be forgotten.

- **Data Collection & Minimization:** Only necessary data is collected in alignment with product functionality.
- **Transparency & Consent:** Clear communication and consent mechanisms are in place where applicable.
- **Access & Control:** Supports user rights to access, correct, or delete their data.
- **Data Sharing & Transfers:** Strict controls govern third-party data sharing and cross-border data transfers.
- **Retention & Disposal:** Data is retained per legal and contractual requirements, then securely disposed.
- **Accountability & Governance:** Oversight through policies, training, and audits ensures compliance across the organization.

For more details, refer to our Privacy Policy.

Data Deletion Practices

WorkBoard adheres to industry-standard data deletion protocols to maintain data privacy and compliance:

- **Customer-Initiated Deletion**: Users can request deletion of their data under GDPR's Right to Be Forgotten. Upon a valid request, data is permanently deleted from primary systems within **30 days**.
- **Backup Data Handling**: Backup data, which is retained for **35 days**, will naturally age out and be permanently deleted from the backup environment within that period.
- **Logging & Auditing**: Deletion requests are logged and auditable to ensure proper compliance and traceability.

Third-Party Risk Management

WorkBoard maintains a structured third-party risk management program to ensure that all vendors and partners meet strict security, privacy, and operational standards. The process includes:

- **Vendor Evaluation & Due Diligence**: All third-party services undergo security, compliance, and risk assessments prior to onboarding.
- **Contractual Safeguards**: Agreements include data protection clauses, audit rights, and breach notification requirements.
- **Ongoing Monitoring**: Vendors are reviewed periodically based on risk tier, including assessments of compliance documentation (e.g., SOC 2 reports, ISO certifications).
- **Sub-Processor Transparency**: A public list of sub-processors is maintained and regularly updated at WorkBoard Subprocessors. Customers are notified in advance of any new sub-processors.
- **Termination & Offboarding**: At contract termination, vendors are required to return or securely destroy all customer data, with confirmation provided to WorkBoard.

Responsible AI

WorkBoard is committed to responsible AI use, ensuring transparency and privacy by design. AI technologies are used to enhance team productivity, not to replace human decision-making.

For more information, visit: WorkBoard AI Trust.

Our Commitment

WorkBoard's commitment to security and privacy is foundational to its platform. Continuous improvement and adherence to industry standards ensure a secure and reliable experience for all users.