Security Measures / Technical and Organisational Measures

HarmonyATS

Provider	HarmonyHR LTD, incorporated and operating under the laws of Kyrgiz Republic, Register № 309328-3301-OOO, having its registered office at Imeni Baltagulova st., 27, Bishkek, Kyrgiz Republic.
Product	HarmonyATS — cloud SaaS applicant tracking system.
Effective Date	05.12.2025
Contact	info@harmonyats.org

This document describes the baseline technical and organisational measures that HarmonyHR LTD applies, or intends to apply, in connection with the delivery and operation of HarmonyATS. It is designed to support customer security, privacy, procurement, and diligence reviews. Unless otherwise agreed in writing, this document is informational in nature and should be read together with the applicable Master Subscription Agreement, Data Processing Addendum, and other contractual documentation governing the service.

1. Scope and interpretation

These measures apply to HarmonyATS as a hosted multi-tenant cloud software-as-a-service applicant tracking system. They address the security controls and operating practices that are relevant to the processing of customer data within the service environment, related support operations, and associated vendor and subprocessor oversight.

References in this document to “customer data” mean data submitted to, stored in, or otherwise processed through HarmonyATS on behalf of a customer. References to “personal data” have the meaning given under applicable data-protection law.

Security controls and implementation details may vary depending on the nature of the service component, system architecture, product evolution, and risk profile. HarmonyHR LTD may update or replace individual security practices over time, provided that the overall level of protection for HarmonyATS is not materially degraded.

2. Security governance and internal access control

HarmonyHR LTD maintains internal security governance appropriate to the size, nature, and risk profile of its business and the HarmonyATS service. Security responsibilities are allocated to relevant personnel and are supported by internal policies, procedures, and operational oversight.

- Access to systems and environments used to operate or support HarmonyATS is granted on a need-to-know and least-privilege basis, taking into account job role, support function, and operational necessity.
- Administrative and privileged access is restricted to authorised personnel and is subject to approval, provisioning, modification, and removal processes.

- Access rights are reviewed periodically and are updated or revoked when roles change, access is no longer required, or personnel separate from the organisation.
- Internal access to customer data is limited to what is reasonably necessary to provide, secure, maintain, or support HarmonyATS, or as otherwise required by law.

3. Authentication and account security

HarmonyHR LTD implements authentication and account-security measures intended to reduce the risk of unauthorised access to HarmonyATS administrative interfaces and internal support tools.

- Administrative accounts are expected to use strong authentication controls, including multifactor authentication or other equivalent access safeguards where supported and implemented for the relevant systems.
- Passwords and secrets are managed using reasonable security practices, including secure storage, controlled access, and change procedures where appropriate.
- Customer-facing account-security capabilities may include configurable user credentials, session controls, password reset processes, and role-based access settings, and may also include single sign-on integrations or multifactor authentication features where made available as part of the service.
- Customers remain responsible for managing their own authorised users, role assignments, credential hygiene, and account use within HarmonyATS.

4. Encryption and data protection safeguards

HarmonyHR LTD applies reasonable safeguards to protect customer data in transit and at rest, taking into account the sensitivity of the data, the functionality of HarmonyATS, and the technical capabilities of the relevant environment.

- Data transmitted over public networks is protected using industry-standard transport security measures appropriate to production web services.
- Stored customer data is protected using at-rest encryption controls provided by relevant infrastructure, databases, storage systems, managed services, and backups, where implemented and appropriate for the relevant environment.
- Cryptographic keys, secrets, tokens, and credentials are managed through controlled processes and are not intentionally exposed to unauthorised personnel.

Where encryption is provided by underlying hosting, platform, database, storage, communications, or other service providers, HarmonyHR LTD relies on those technical controls in combination with its own access, configuration, and governance measures.

5. Logging, monitoring, and operational visibility

HarmonyHR LTD maintains logging and monitoring practices designed to support service reliability, troubleshooting, security review, and incident response.

- Relevant systems may generate logs relating to authentication events, administrative actions, service operations, errors, and other security-relevant or operationally relevant events.
- Logs and alerts are used to support detection, investigation, and remediation of suspected misuse, service disruption, and security events.
- Access to operational logs is restricted to authorised personnel with a business need to review them.
- Log retention periods, monitoring thresholds, and alerting workflows may vary by system and are managed pursuant to internal operational, security, and incident-management requirements.

6. Vulnerability management and change control

HarmonyHR LTD maintains processes intended to identify, evaluate, prioritise, and address security vulnerabilities and software changes affecting HarmonyATS.

- Security issues identified through internal review, third-party notifications, vendor advisories, dependency monitoring, or customer-reported concerns are assessed and addressed based on severity, exploitability, and service impact.
- Patches, updates, and configuration changes are applied through controlled change-management processes intended to reduce the risk of introducing instability or unauthorised change.
- Development, testing, and production environments are separated to a reasonable extent appropriate for the relevant systems and workflows.
- Where appropriate, code changes and infrastructure changes are subject to review and approval prior to deployment.

HarmonyHR LTD does not, by this document, commit to any specific vulnerability remediation timeframes, penetration-testing programme, disclosure schedule, or reporting cadence, except to the extent expressly agreed in writing in the applicable customer contract.

7. Backup, resilience, and business continuity

HarmonyHR LTD maintains backup and resilience measures intended to support the continued operation of HarmonyATS and the recovery of customer data in the event of certain outages, failures, or corruption scenarios.

- Backups may be performed for relevant production data and service components in accordance with HarmonyHR LTD's internal backup, retention, restoration, and environment-specific operational procedures.
- Business continuity and recovery processes are designed to support service restoration using available personnel, infrastructure, and vendor dependencies.
- Recovery approaches may differ by system component and deployment architecture.

This document does not create any commitment to specific recovery time objectives, recovery point objectives, uptime percentages, service credits, or disaster-recovery metrics unless expressly agreed in writing in the applicable customer contract.

8. Incident response and personal data breaches

HarmonyHR LTD maintains incident-response procedures for investigating, containing, remediating, and documenting suspected security incidents affecting HarmonyATS.

- Security events are escalated to appropriate personnel for triage and response based on severity and potential impact.
- Response activities may include containment, forensic review, root-cause analysis, remediation, service restoration, and communication with relevant stakeholders.
- Where required under the applicable contract or data-protection law, HarmonyHR LTD will notify affected customers without undue delay after becoming aware of a confirmed personal data breach involving customer data processed by HarmonyATS on the customer’s behalf.

Incident-response processes are coordinated with the applicable contractual framework, including the Master Subscription Agreement and Data Processing Addendum, and may take into account the need to protect system integrity, preserve evidence, and comply with legal obligations.

9. Personnel confidentiality and security awareness

Personnel who are authorised to operate, support, or otherwise access systems relevant to HarmonyATS are subject to confidentiality obligations and are expected to follow internal security and acceptable-use requirements.

- Confidentiality obligations are imposed by contract, policy, or other legally binding means.
- Personnel receive security awareness or role-appropriate guidance and training at onboarding and/or periodically thereafter, taking into account the individual's responsibilities.
- Access is removed or adjusted when personnel responsibilities change or engagement ends.
- HarmonyHR LTD seeks to limit the number of personnel with elevated or production-level access to those whose roles reasonably require it.

10. Vendor and subprocessor oversight

HarmonyHR LTD may use vendors and approved subprocessors to support the delivery, hosting, maintenance, communications, analytics, support, and security of HarmonyATS. Such vendors and subprocessors are selected and managed using reasonable due-diligence and oversight measures appropriate to the service provided and the related risk profile.

- Relevant vendors and subprocessors are expected to be subject to written confidentiality and data-protection obligations appropriate to the services they provide.
- Where a vendor or subprocessor may process customer personal data, HarmonyHR LTD seeks to ensure that the relationship is governed by contractual terms consistent with applicable legal and contractual requirements.
- Information regarding HarmonyHR LTD's use of vendors and subprocessors may be made available by reasonable means, including through contractual materials, customer communications, support channels, or upon reasonable written request, in each case subject to confidentiality, security, legal, and third-party restrictions. HarmonyHR LTD may add, replace, or remove vendors and subprocessors from time to time in the ordinary course of business.

HarmonyHR LTD may rely on infrastructure, communications, storage, hosting, and related technology providers whose technical and organisational measures form part of the overall security model for HarmonyATS.

11. Data return, deletion, and secure disposal principles

At the end of the applicable services, HarmonyHR LTD will address customer data return and deletion in accordance with the Master Subscription Agreement, Data Processing Addendum, applicable law, and the technical limitations and retention logic of the relevant systems.

- Customer export options, post-termination access windows, and deletion timing may be addressed in the applicable service agreement or support documentation.
- Where customer data is deleted from active systems, residual copies may remain in backups, archives, logs, or disaster-recovery media for a limited period until overwritten, deleted, or otherwise retired in the ordinary course.
- Internal disposal of media, credentials, devices, and access rights is managed using reasonable administrative and technical controls appropriate to the relevant environment and medium.

12. Customer shared-responsibility assumptions

The security of HarmonyATS also depends on customer actions. Customers are responsible for their own use of the service, including their internal access governance, user training, endpoint security, lawful

configuration choices, and the content of the data they choose to upload or make available through HarmonyATS.

- Customers should assign roles carefully, manage authorised users promptly, maintain strong account-security practices, and review data exports, integrations, and user access on an ongoing basis.
- Customers are responsible for the legality, quality, and accuracy of customer data they submit to HarmonyATS, as well as for configuring and using the service in accordance with their own regulatory and employment-law requirements.
- Where customers enable third-party integrations, import tools, APIs, or external communications workflows, customers remain responsible for assessing the resulting data flows and access implications unless otherwise agreed in writing.

13. Security requests and further information

Customer questions regarding these Security Measures / Technical and Organisational Measures may be directed to info@harmonyats.org. HarmonyHR LTD may provide additional information under appropriate confidentiality protections where reasonably necessary for customer diligence, legal compliance, or contractual performance, subject to security, confidentiality, privilege, and operational considerations.

Any customer review, inspection, or audit rights relating to HarmonyATS are governed by the applicable contract and are not expanded by this document unless expressly agreed in writing.

Document control

Version: 1.1

Effective Date: 05.12.2025

Applies to: HarmonyATS cloud SaaS applicant tracking system

Provider: HarmonyHR LTD

Contact: info@harmonyats.org