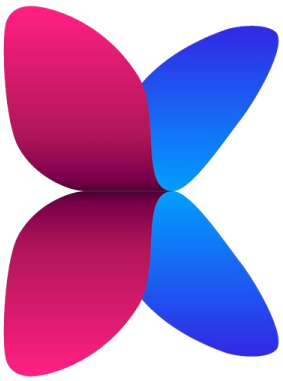
A-LIGN

A-LIGN.com

Type 1 SOC 2

Prepared for:
ASTERISM (Kirha)

Year:
2026



REPORT ON ASTERISM (KIRHA)'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN OF ITS CONTROLS RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY

Pursuant to Reporting on System and Organization Controls 2 (SOC 2)
Type 1 examination performed under AT-C 105 and AT-C 205

July 15, 2026

Table of Contents

SECTION 1 ASSERTION OF ASTERISM (KIRHA) MANAGEMENT 1

SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT 3

SECTION 3 ASTERISM (KIRHA)'S DESCRIPTION OF ITS KIRHA CONTEXT-AS-A-SERVICE SYSTEM AS OF JULY 15, 2026 7

OVERVIEW OF OPERATIONS 8
Company Background 8
Description of Services Provided 8
Principal Service Commitments and System Requirements 9
Components of the System 10
Boundaries of the System 16
RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING 16
Control Environment 16
Risk Assessment Process 18
Information and Communications Systems 19
Monitoring Controls 19
Changes to the System in the Last 3 Months 21
Incidents in the Last 3 Months 21
Criteria Not Applicable to the System 21
Subservice Organizations 21
COMPLEMENTARY USER ENTITY CONTROLS 22
TRUST SERVICES CATEGORIES 23
CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION 25
TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY 25
ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY 53
ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY 55

SECTION 4 INFORMATION PROVIDED BY THE SERVICE AUDITOR 56

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR 57

SECTION 1

ASSERTION OF ASTERISM (KIRHA) MANAGEMENT

ASSERTION OF ASTERISM (KIRHA) MANAGEMENT

August 30, 2026

We have prepared the accompanying description of ASTERISM (Kirha)'s ('Kirha' or 'the Company') Kirha Context-as-a-Service System titled "ASTERISM (Kirha)'s Description of Its Kirha Context-as-a-Service System as of July 15, 2026" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the Kirha Context-as-a-Service System that may be useful when assessing the risks arising from interactions with Kirha's system, particularly information about system controls that Kirha has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Kirha uses Google Cloud Platform ('GCP' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Kirha, to achieve Kirha's service commitments and system requirements based on the applicable trust services criteria. The description presents Kirha's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Kirha's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed are necessary, along with controls at Kirha, to achieve Kirha's service commitments and system requirements based on the applicable trust services criteria. The description presents Kirha's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Kirha's controls.

We confirm, to the best of our knowledge and belief, that:

a. the description presents Kirha's Kirha Context-as-a-Service System that was designed and implemented as of July 15, 2026, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of July 15, 2026, to provide reasonable assurance that Kirha's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organization and user entities applied the complementary controls assumed in the design of Kirha's controls as of that date.

Pierre Hay
Founder
ASTERISM (Kirha)

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: ASTERISM (Kirha)

Scope

We have examined Kirha's accompanying description of its Kirha Context-as-a-Service System titled "ASTERISM (Kirha)'s Description of Its Kirha Context-as-a-Service System as of July 15, 2026" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design of controls stated in the description as of July 15, 2026, to provide reasonable assurance that Kirha's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Kirha uses GCP to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Kirha, to achieve Kirha's service commitments and system requirements based on the applicable trust services criteria. The description presents Kirha's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Kirha's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Kirha, to achieve Kirha's service commitments and system requirements based on the applicable trust services criteria. The description presents Kirha's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Kirha's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Kirha is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Kirha's service commitments and system requirements were achieved. Kirha has provided the accompanying assertion titled "Assertion of ASTERISM (Kirha) Management" (assertion) about the description and the suitability of the design of controls stated therein. Kirha is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

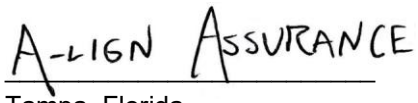
a. the description presents Kirha's Kirha Context-as-a-Service System that was designed and implemented as of July 15, 2026, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of July 15, 2026, to provide reasonable assurance that Kirha's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of Kirha's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Kirha, user entities of Kirha's Kirha Context-as-a-Service System as of July 15, 2026, business partners of Kirha subject to risks arising from interactions with the Kirha Context-as-a-Service System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.



Tampa, Florida
August 30, 2026

SECTION 3

ASTERISM (KIRHA)'S DESCRIPTION OF ITS KIRHA CONTEXT-AS-A-SERVICE SYSTEM AS OF JULY 15, 2026

OVERVIEW OF OPERATIONS

Company Background

Kirha (legal entity: ASTERISM, SAS, SIREN 942 905 670) was founded on 3 April 2025 with the objective of providing a Context-as-a-Service platform for autonomous AI agents. Kirha delivers unified, governed access to external data sources and tools through Model Context Protocol (MCP) integrations, enabling Artificial Intelligence (AI) agents to retrieve trusted, real-time context on demand. The platform is built and designed for reliability, security, and regulatory compliance, including data residency and hosting within the European Union.

ASTERISM is a French société par actions simplifiée (SAS) registered at 23 rue d'Anjou, 75008 Paris, France, with a distributed team operating across Paris, France and Barcelona, Spain. Production infrastructure is hosted in the European Union to support General Data Protection Regulation (GDPR) and Hébergement de Données de Santé (HDS) requirements.

Kirha serves organizations building autonomous AI agents and agentic applications that require secure, governed access to external context and data sources.

Description of Services Provided

Kirha provides a Context-as-a-Service platform delivered to customers as a cloud-hosted service. The company was founded in 2025 to provide governed, real-time access to external data and tools for any organization or application that needs to consume such data, across a range of verticals including finance, healthcare, and advertising.

Kirha's core value is the intelligent aggregation of data across many third-party data providers, a significant portion of which are private, licensed, or paywalled sources rather than publicly available web data. Rather than requiring customers to hold and manage separate accounts and credentials with each individual data provider, Kirha exposes this aggregated access through a single Application Programming Interface (API) key. Kirha intelligently combines and synthesizes data across these providers to deliver relevant, consolidated responses to customer queries.

Customers consume the service in two primary ways: programmatically via a Representational State Transfer (REST) API, and interactively via a web dashboard. Internally, connected data sources and tools are integrated through the MCP. The platform enables the following:

- Aggregating and providing unified access to numerous third-party data providers, including private and licensed data sources, through a single set of Kirha credentials
- Intelligently combining and synthesizing data across providers to produce consolidated responses
- Authenticating and authorizing customer access to the platform and connected data sources
- Governing and controlling which data and tools a customer or agent may access
- Retrieving and delivering real-time context and data on demand
- Providing prebuilt agents that perform multi-step tasks using Kirha's connected data providers (for example, deep research across data verticals, disease evidence review, and regulatory/Standard Operating Procedures (SOP) document preparation)
- Providing customers with access to data-access logs for the requests they make
- Tracking and reporting per-call usage and cost for each MCP tool invoked

A defining characteristic of the platform's architecture is that Kirha does not store the underlying third-party data payloads it retrieves. Data from connected providers is consumed and delivered in real time and does not persist, which limits Kirha's handling of sensitive third-party data to transient processing only. Kirha does store operational metadata required to run the service, including customer account information, API keys, data-access logs, and per-tool usage and cost records.

Customers access the API using API keys. Access to the web dashboard is authenticated via OAuth, using e-mail or social login. The dashboard provides visibility into data-access activity, usage, and per-tool cost.

The user entities of the service are Kirha's customers ("data consumers"), organizations and applications that need to consume external data through the platform, spanning verticals such as finance, healthcare, and advertising. These include software developers and AI-agent builders integrating Kirha into their products.

Principal Service Commitments and System Requirements

Kirha designs its processes and procedures related to its Context-as-a-Service platform to meet its objectives for the service. Those objectives are based on the service commitments that Kirha makes to user entities, the laws and regulations that govern the provision of the service, and the financial, operational, and compliance requirements that Kirha has established for the service. The services provided by Kirha are subject to applicable data protection and privacy requirements, including the European Union (EU) GDPR and, where health data is processed, the French HDS framework, as well as other laws and regulations in the jurisdictions in which Kirha operates.

Security commitments to user entities are documented and communicated in customer agreements and terms of service, and in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

Security principles within the fundamental design of the platform are designed to permit users to access only the information and functionality appropriate to their role, through role-based access controls (RBACs), while restricting access to data and functions not needed for their role.

Use of encryption technologies to protect customer data both in transit and at rest. Data in transit is protected using Transport Layer Security (TLS). Sensitive data at rest, including personal information, credentials, and API keys, is stored in encrypted form, and secrets are managed through encrypted secret management. Where personnel access in-scope systems, connections are established securely using encryption.

By design, Kirha does not persist the third-party data payloads it retrieves on behalf of customers; such data is processed transiently and delivered in real time, reducing the storage of sensitive third-party data.

Kirha establishes operational requirements that support the achievement of its security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Kirha's policies and procedures, system design documentation, and agreements with customers, vendors, and third-parties. Changes to commitments, requirements, and responsibilities are communicated to affected parties.

Organizational and information security policies are formally documented to support the functioning of internal controls and to define an organization-wide approach to how systems and data are protected. These include policies governing how the service is designed and developed (Software Development Lifecycle (SDLC)), how the system is operated and changes are managed (Configuration Management, Change Management), how incidents are handled (Incident Response Plan), how availability is maintained (Redundancy and Availability, Business Continuity and Disaster Recovery (BCDR)), and how personnel are onboarded, trained, and offboarded. Standard operating procedures document how specific manual and automated processes are carried out. These policies and procedures are made available to Kirha personnel.

Components of the System

Infrastructure

Primary infrastructure used to provide Kirha's Kirha Context-as-a-Service System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Google Kubernetes Engine (GKE), GCP	Container orchestration	Runs the Go microservices that make up the Kirha platform
GKE-managed node pools (GCP Compute Engine)	Compute nodes	Provide the compute capacity for containerized workloads
Cloud Structured Query Language (GCP SQL)	Relational database	Stores operational metadata (customer accounts, API keys, access logs, usage/cost records)
NGINX Ingress Controller	Ingress / load balancing	Routes and load-balances inbound traffic to platform services
GCP Cloud Armor	Web application firewall (WAF)	Filters and protects inbound traffic against web-based attacks
GCP Pub/Sub	Messaging / async processing	Handles asynchronous messaging between platform components
Google Cloud Storage (GCS)	Object storage	Stores static/public assets
GCP Secret Manager / Secrets Operations (SOPS)	Secret management	Stores and manages encryption keys, API keys, and service credentials

Software

Primary software used to provide Kirha's Kirha Context-as-a-Service System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
GKE	N/A	Container orchestration for platform microservices
GCP	N/A	Underlying cloud infrastructure and managed services
GitHub	N/A	Source code management and Continuous Integration/Continuous Deployment (CI/CD) pipelines
GCP Cloud Logging / Logs and Trace Explorer	N/A	Logging, tracing, monitoring, and alerting
WireGuard	N/A	Secure Virtual Private Network (VPN) tunnel for administrative access to internal/production infrastructure

Primary Software		
Software	**Operating System**	**Purpose**
Drata	N/A	Continuous compliance monitoring and control evidence
Notion	N/A	Policy, procedure, and compliance documentation hub
Google Workspace	N/A	Business communication, e-mail, and identity (Multi-factor Authentication (MFA) managed)
Helm	N/A	Kubernetes application packaging and deployment
Jenkins	N/A (containerized on GKE)	Continuous delivery / deployment automation
Google Meet	N/A	Video conferencing and team communication
Google Docs	N/A	Document collaboration and authoring
Google Drive	N/A	File storage, sharing, and collaboration

People

Kirha is an early-stage startup with a small team. The organization consists of approximately four people, who collectively perform all functions supporting the in-scope service. Given the size of the organization, individuals hold multiple responsibilities across the following functional areas:

- Leadership / Corporate: The Chief Executive Officer (CEO) is responsible for overall company direction, business operations, legal and compliance oversight, finance, vendor relationships, and formal approval of security policies and procedures. Executive leadership holds ultimate accountability for the organization's security commitments and system requirements.
- Backend and Infrastructure / DevOps / Security: A founding engineer is responsible for backend development, infrastructure and cloud operations (GCP/GKE), CI/CD pipelines, deployment, monitoring, and information security. This includes managing access controls, secrets management, security configuration, incident response, and the ongoing compliance program. Given the team size, the information security function is performed within the founding engineering staff rather than by a dedicated security department.
- Full stack and AI: A co-founder is responsible for full stack development, including the customer-facing dashboard, and for the AI and agent capabilities of the platform.
- Interns: The organization may engage interns to support engineering and operational activities under the supervision of permanent staff. Interns are subject to onboarding and access-control procedures appropriate to their role.

Because of the organization's size, there is no separate help desk, dedicated Information Technology (IT) operations group, or standalone information security team. These responsibilities are distributed among the founding team, and segregation-of-duties limitations inherent to a small organization are addressed through compensating controls documented in the company's policies (for example, code review requirements, change management, and least-privilege access).

Data

Data, as maintained and processed by Kirha, constitutes the following:

- Customer account data: customer identity, account records, and dashboard user profiles (including data obtained via OAuth login, such as e-mail address).
- Authentication and credential data: API keys, OAuth tokens, and service credentials used to authenticate customers and connect to third-party data providers.

- Data-access logs: records of the data-access requests made by customers, available to customers for their own activity.
- Usage and cost records: per-call usage and cost metering for each MCP tool / data provider invoked.
- Third-party provider data (transient): data retrieved from connected third-party data providers in response to customer requests. This data is processed transiently and delivered in real time. It does not persist by Kirha.
- System and operational logs: application, infrastructure, and audit logs generated by the platform (via GCP Cloud Logging).
- Configuration and secrets: platform configuration and secrets, managed encrypted via SOPS with a GCP Key Management Service (KMS) key.

A defining characteristic of the Kirha platform is that it does not store the underlying third-party data payloads it retrieves. Such data is consumed and delivered in real time, which limits Kirha's handling of potentially sensitive third-party data to transient processing only. The data Kirha does persist is limited to the operational metadata required to run and secure the service (customer accounts, credentials, access logs, and usage/cost records).

Data classification and handling are addressed through the company's information security policies, which define how data is classified, who may access it, how it is protected, and how long it is retained. Access to confidential and customer data is restricted to authorized personnel based on role and responsibility, following the principle of least privilege.

Data in transit is protected using TLS. Sensitive data at rest - including personal information, credentials, and API keys - is stored in encrypted form. Operational metadata is stored in Cloud SQL (GCP, europe-west9), and static, public assets are stored in GCS.

Management has defined the components of data critical to supporting the in-scope system, including what the data is, its source, and how it is stored and transmitted. Operational personnel monitor the system through logging and alerting them to detect and resolve processing errors in a timely manner.

Processes, Policies and Procedures

Formal information security policies and procedures exist that describe logical access, system operations, change management, software development, incident response, data protection, and business continuity. Logical access policies address system settings and configurations, authentication requirements, access management, least-privilege access, and audit logging requirements.

Kirha's documented policies and procedures include, among others: the SDLC, Configuration Management Plan, Incident Response Plan, Redundancy and Availability, BCDR Plan, Information Security in Project Management, and onboarding and offboarding procedures.

All team members are expected to adhere to Kirha's policies and procedures, which define how the service is designed, developed, operated, and secured. These policies are maintained in the company's central compliance documentation hub and are accessible to all Kirha personnel.

Physical Security

Kirha relies on GCP for cloud hosting services to support the infrastructure and systems. Refer to the “Subservice Organizations” section below for physical security controls implemented and operated by GCP.

Logical Access

Kirha uses an RBAC model and requires users to be identified and authenticated prior to accessing in-scope system resources. Access to resources is granted based on the principle of least privilege, according to each individual's role and responsibilities.

Identity and authentication: Internal identity and access to business systems (e-mail, documents, collaboration) are managed through Google Workspace, with MFA enforced. Access to cloud infrastructure is managed through GCP Identity and Access Management (IAM). Access to source code and CI is managed through GitHub. Customer access to the platform dashboard is authenticated via OAuth (E-mail/Password, Google or X social login); customer access to the API is authenticated via API keys.

Privileged access: Privileged access to the production environment (GCP/GKE, Cloud SQL, secrets) is restricted to authorized engineering personnel who require it for their role. Administrative access to internal infrastructure is performed over an encrypted VPN (WireGuard). Secrets and credentials are managed encrypted via SOPS with a GCP KMS key.

Segregation of duties: Due to the small size of the organization, complete segregation of duties is not always achievable. Where incompatible responsibilities cannot be fully separated, Kirha implements compensating controls, including code review requirements, change management, logging of privileged actions, and review of access by a second team member where feasible.

Logging and monitoring: User and system activity within the in-scope environment is logged via GCP Cloud Logging, and logs are retained and reviewed as needed to detect and investigate anomalous or unauthorized activity.

Access provisioning and de-provisioning: Access is granted as part of the personnel onboarding process, based on the individual's role, and is revoked as part of the offboarding process upon termination or role change. Access provisioning and removal are documented in the company's onboarding and offboarding procedures and tracked in the Access Requests record.

Access reviews: Access to in-scope systems, including privileged access, is reviewed on a quarterly basis. Reviews consider each individual's role, duties requiring segregation, and the risks associated with the access granted. Identified changes are actioned and documented.

Computer Operations - Backups

Kirha has established backup practices for the data required to operate the in-scope service. Because the platform does not persist third-party data payloads, backup scope is limited to the operational metadata stored by the service (customer accounts, credentials, access logs, and usage/cost records) and to system configuration.

Database backups: Operational metadata is stored in Google Cloud SQL. Cloud SQL provides automated backups, managed by GCP. Backups are retained according to the configured retention settings.

Configuration and infrastructure: Infrastructure is defined and version-controlled (infrastructure-as-code, Helm charts), and secrets are stored encrypted (SOPS with GCP KMS key) in version control, enabling the environment to be reconstructed. Application source code and configuration are maintained in GitHub.

Geographic redundancy: Production infrastructure and backups are hosted within the EU (GCP europe-west9) to meet data residency and HDS requirements.

Backup testing and recovery: Backup and recovery capability is validated as part of Kirha's BCDR Plan.

Computer Operations - Availability

Kirha has established incident response policies and procedures to guide personnel in reporting and responding to information security and operational incidents. Procedures exist to identify, document, report, and act upon security breaches and other incidents. Incidents are analyzed, classified, prioritized, documented, tracked, investigated, and resolved. The status, remediation, and resolution of incidents are communicated to affected parties as appropriate. Incident response is documented in Kirha's Incident Response Plan, and incidents are recorded in the Incident Log.

Kirha monitors the capacity, utilization, and performance of its cloud infrastructure to help ensure the availability of the in-scope service. Monitoring is performed using GCP Cloud Monitoring and Cloud Logging, with alerting policies configured to notify personnel when thresholds are exceeded (for example, database Central Processing Unit (CPU), memory, disk utilization and I/O, and message processing age). Alerts are investigated and resolved by engineering personnel.

Processing capacity and system performance are monitored on an ongoing basis. Because the platform runs on managed, elastic cloud infrastructure (GCP/GKE), capacity can be scaled in response to demand. Infrastructure capacity monitoring includes, but is not limited to:

- Compute and container workload utilization (GKE)
- Database performance and storage (Cloud SQL)
- Messaging/queue processing (Pub/Sub)

Patch and vulnerability management: Kirha relies on GCP-managed services for patching the underlying infrastructure. GKE nodes and managed services (Cloud SQL, etc.) are patched by GCP according to Google's maintenance and upgrade processes. Application dependencies and container images are updated by engineering personnel as part of the development and deployment lifecycle.

BCDR: Kirha has established a formal BCDR Plan, along with a Redundancy and Availability policy. The BCDR Plan is tested annually, with revisions made based on testing results.

Kirha relies on GCP for cloud hosting services to support the infrastructure and systems. Refer to the “Subservice Organizations” section below for environmental security controls implemented and operated by GCP.

Change Control

Kirha maintains documented change management policies and procedures to guide personnel in developing and implementing system changes (application, infrastructure, and configuration). These are defined in the SDLC and Configuration Management Plan. The SDLC explicitly addresses how change control and separation of duties are implemented in the context of a small founding team, using compensating controls in place of traditional per-change peer review where that is not practical.

Environments: Kirha operates two environments: local development (isolated developer workstations using containers and synthetic data) and production (hosted on GCP/GKE, europe-west9 and europe-west1). Production is the only environment containing customer data; all other environments use synthetic data only. A dedicated staging environment is not maintained; this is a documented, risk-accepted decision, with the associated risk treated through the compensating controls below and recorded in the Risk Register and Statement of Applicability.

Change workflow: All source code is hosted in GitHub. All changes to main are made via pull request (PR) on a feature branch; direct pushes and force-pushes to main are blocked by branch protection rules, which apply to all engineers. Branch protection enforces linear history, required status checks, and conversation resolution before merge.

Automated merge gate: In place of mandatory per-change peer review on single-engineer repositories, all changes must pass an automated merge gate enforced by branch protection before merge to main. This gate includes unit tests, static analysis and linters (e.g. staticcheck, vet, biome, eslint, tsc), Go vulnerability scanning (govulncheck), dependency vulnerability scanning (GitHub Dependabot), secret scanning (gitleaks plus GitHub native secret scanning and push protection), and container image vulnerability scanning (GCP Artifact Registry). A failing check blocks merge for everyone.

Peer review and independent oversight: On repositories maintained by more than one engineer, at least one approving review by a non-author is required before merge. For single-engineer repositories, independent oversight is provided by a monthly post-merge independent review, conducted by a founder other than the repository owner, covering merges to main, production releases, emergency changes, and security-relevant findings during the period. Reviews are recorded in the Audit Findings and Remediations database and retained for at least two years. This substitution of automated gates plus monthly independent review for per-change peer review is documented as an exception in the Statement of Applicability against International Organization for Standardization (ISO) 27001 A.5.3 (Segregation of duties) and A.8.32 (Change management).

Separation of build and deploy: Continuous Integration (build, test, scan, publish artifact) runs on GitHub Actions and is separated from Continuous Deployment (promote artifact to production), which runs on a self-hosted Jenkins instance. A merge to main does not automatically deploy; production deployment requires an engineer to deliberately cut a GitHub Release, introducing an explicit checkpoint between "code merged" and "code in production." Jenkins runs under a dedicated service account with least-privilege IAM permissions scoped to reading from Artifact Registry and applying manifests to the GKE production namespace; it cannot modify infrastructure, IAM, or other GCP resources. This separates trust boundaries so that compromise of GitHub does not directly compromise production deployment.

Traceability and rollback: Every production deployment is traceable through commit → PR → merge → immutable image tag (commit Secure Hash Algorithm (SHA)) → GitHub Release → Jenkins build → Cloud Logging entry. Rollback is performed by cutting a new GitHub Release pointing at a prior tested commit; no production image is overwritten or deleted.

Emergency changes: Emergency changes (hotfixes) follow the same workflow with no relaxed checks: a PR with all automated gates passing, an explicitly cut GitHub Release (no bypass path), and a record in the Emergency Change Log within 24 hours capturing the change description, PR and commit SHA, release tag, checks passed, engineer, deployment timestamp, and justification of urgency.

Infrastructure as code: Production infrastructure (GKE cluster configuration, NGINX Ingress with ModSecurity WAF ruleset, GCP IAM policies, Cloud Monitoring alert policies, Domain Name System (DNS)) is defined declaratively in version control and follows the same PR and automated-gate process as application code. Manual changes via the GCP console are not the change-management path; drift, if discovered, is investigated and either re-applied via code or recorded as an exception.

Change communication: Changes that materially affect the service are communicated to affected internal and external parties.

Data Communications

Kirha's data communications and network security controls are implemented within GCP, consistent with its cloud-native architecture.

Network filtering and segmentation: Network traffic is controlled through GCP Virtual Private Cloud (VPC) firewall rules, which deny inbound connections that are not explicitly authorized. Default-permissive rules (for example, default Secure Shell (SSH) access) have been removed. Workloads are segmented within GCP, and administrative interfaces are not exposed publicly. Inbound application traffic passes through the NGINX Ingress Controller and a Web Application Firewall (GCP Cloud Armor, and NGINX with ModSecurity v3 / Open Worldwide Application Security Project (OWASP) Core Rule Set) that filters and blocks malicious web traffic.

Encryption in transit: All external communications with the platform occur over encrypted connections (Hypertext Transfer Protocol Secure (HTTPS)/ TLS). Communications with connected third-party data providers occurs over encrypted connections.

Administrative / remote access: Administrative access to internal and production infrastructure is performed over an encrypted WireGuard VPN. Access to the VPN and to production systems is restricted to authorized personnel based on role and responsibility, following least privilege. Access and activity are logged via GCP Cloud Logging and reviewed as needed.

Monitoring and alerting: Kirha monitors in-scope systems to identify potential security threats and unusual activity. GCP Cloud Logging captures audit logs, and Cloud Monitoring alert policies notify personnel of anomalous or suspicious activity (for example, WAF firings, IAM changes, and infrastructure anomalies). Alerts are investigated and resolved by engineering personnel.

Vulnerability management: Kirha performs vulnerability scanning as an integrated part of its development and deployment lifecycle, including dependency vulnerability scanning (GitHub Dependabot), Go vulnerability scanning (govulncheck), secret scanning (gitleaks and GitHub native secret scanning with push protection), and container image vulnerability scanning (Trivy and GCP Artifact Registry native scanning). Identified vulnerabilities are documented, prioritized, and remediated in accordance with defined remediation timelines: Critical within 7 days, High within 30 days, Medium within 90 days, and Low on a best-effort basis.

Boundaries of the System

The scope of this report includes the Kirha Context-as-a-Service System performed in the remote facilities.

This report does not include the cloud hosting services provided by GCP at multiple facilities.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Kirha's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Kirha's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts, and the communication of entity values and behavioral standards to personnel, primarily through the company's documented policies and through management's direct example within a small team.

Specific control activities that Kirha has implemented in this area include the following:

- Documented information security policies communicate the company's expectations and behavioral standards to personnel and are made available to all personnel through the company's central documentation hub.
- Confidentiality obligations are established through non-disclosure agreements, which are put in place with employees, contractors, or third-parties where required by the nature of the engagement or the information involved. Confidentiality and intellectual property obligations are also established through the company's founder and key-person agreements.
- Background checks are performed where required, based on the nature of the role and applicable legal or contractual requirements. Given the size and founding structure of the organization, background checks are applied on a risk-based basis rather than uniformly, and this position is treated as a documented, risk-based decision.
- Personnel are able to raise security concerns or report unethical behavior directly to management, consistent with the size and structure of the organization.

Commitment to Competence

Kirha's management defines competence as the knowledge and skills necessary to accomplish tasks that define personnel roles and responsibilities. Management's commitment to competence includes consideration of the competence levels required for particular roles and how those levels translate into the requisite skills and knowledge.

Specific control activities that Kirha has implemented in this area include the following:

- As part of the hiring process, management evaluates a candidate's competencies, skill sets, and prior experience for the role.
- Roles and responsibilities within the organization are assigned based on each individual's skills and experience, reflecting the founding team's areas of ownership (for example, backend and infrastructure, full stack and AI, and business leadership).
- Security awareness training is provided to personnel to maintain and reinforce security knowledge appropriate to their roles.

Management's Philosophy and Operating Style

Kirha's management philosophy and operating style encompass a broad range of characteristics. These include management's approach to identifying, taking, and monitoring business and security risks, and management's attitudes toward information processing, data protection, and the security and reliability of the service.

Specific control activities that Kirha has implemented in this area include the following:

- Management stays informed of regulatory, industry, and security developments affecting the service provided, including data protection requirements (such as GDPR and HDS) relevant to the company's operations.
- As a small founding team, management maintains close, direct involvement in day-to-day operations and meets at least monthly to discuss major initiatives, risks, and issues affecting the business as a whole.
- Management maintains an ongoing compliance and security program, including engagement with external specialists and use of a continuous control monitoring platform, reflecting its commitment to security and risk management.

Organizational Structure and Assignment of Authority and Responsibility

Kirha's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility. The organizational structure has been developed to suit the company's needs and is based, in part, on its size and the nature of its activities.

As a small founding team, Kirha assigns authority and responsibility primarily along clear areas of ownership. Each founder owns defined domains of the business and the associated systems and services end-to-end. Responsibilities are distributed as follows: the Chief Executive Officer holds responsibility for overall company direction, business operations, and legal and compliance oversight; one founding engineer holds responsibility for backend development, infrastructure, DevOps, and security; and a co-founder holds responsibility for full stack development and AI capabilities. Interns and other personnel operate under the supervision of the founding team.

Reporting relationships and accountability are direct and clear given the size of the organization. Because complete segregation of duties is not always achievable at this scale, compensating controls (documented in the SDLC, Configuration Management, and Risk Register) are used to maintain appropriate oversight and accountability.

Specific control activities that Kirha has implemented in this area include the following:

- Key areas of authority and responsibility are defined along founder ownership of specific services and business domains and are understood across the team.
- Assignment of ownership reflects each individual's skills and experience and is communicated and updated as the organization and its services evolve.
- Access and privileges within systems are aligned to each individual's role and responsibilities, following the principle of least privilege.

Human Resources Policies and Practices

Kirha's human resources practices are designed to support the hiring, onboarding, and offboarding of personnel in a manner appropriate to the size and nature of the organization. These practices relate to personnel hiring, orientation, access management, and separation.

Specific control activities that Kirha has implemented in this area include the following:

- New personnel complete a documented onboarding process that includes provisioning of access based on role (least privilege), introduction to the company's security policies, and completion of security awareness training.
- Non-disclosure and confidentiality agreements are put in place with personnel, contractors, or third-parties where required by the nature of the engagement or the information involved. Confidentiality and intellectual property obligations are also established through founder and key-person agreements.
- A documented offboarding process guides the separation of personnel, including the timely removal of access to systems and data upon termination or role change.

Risk Assessment Process

Kirha's risk assessment process identifies and manages risks that could affect the company's ability to provide reliable and secure services to its user entities. This ongoing process requires management to identify significant risks inherent in its products, services, and operations, assess the potential impact and likelihood of those risks, establish acceptable risk tolerance levels, and implement appropriate measures to monitor and manage the risks.

Through this process, management has identified risks resulting from the nature of the services provided and the size of the organization. Risks considered include, among others:

- Operational risk: Changes in the environment, personnel, or systems, and the limitations inherent in a small team (including segregation-of-duties constraints).
- Strategic risk New technologies, changing business models, and shifts within the industry.
- Compliance risk: Legal and regulatory changes, including data protection (GDPR) and HDS requirements.
- Security risk: Threats to the confidentiality, integrity, and availability of the platform and the data it processes.
- Third-party/ vendor risk: Risks arising from sub processors and third-party data providers.

Given the size of the organization, risk assessment is performed by management (the founding team) rather than by a separate, independent risk function. Management maintains close, direct involvement in operations and addresses significant risks through the company's documented controls and its ongoing compliance program.

Identified risks are documented in the company's Risk Register, along with their assessment and the corresponding treatment or mitigating controls. Certain risk-based decisions including the acceptance of specific limitations inherent to a small team, together with their compensating controls are documented in the Risk Register and reflected in the Statement of Applicability.

Kirha performs due diligence on its vendors and third-parties. Where control gaps are identified, Kirha works to address and remediate them, and maintains an inventory of sub processors and associated data protection agreements.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Kirha's Context-as-a-Service platform; and the nature of the components of the system result in risks that the applicable trust services criteria will not be met. Kirha addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met.

Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address those risks is likewise unique to Kirha. As part of the design and operation of the system, Kirha's management identifies the specific risks that the criteria may not be met and the controls necessary to address those risks. This integration of risk assessment with the design and operation of controls is reflected in the company's Risk Register and Statement of Applicability, which link identified risks to their corresponding mitigating controls.

Information and Communications Systems

Information and communication are an integral component of Kirha's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization and the dependence on, and complexity of, information technology. At Kirha, information is identified, captured, processed, and reported through various information systems, as well as through direct communication with customers, vendors, and personnel.

Given the size and distributed nature of the team, Kirha relies on frequent, direct communication to disseminate policies, procedures, controls, and other strategic initiatives. At least monthly team communication (including recurring calls and ongoing collaboration through shared tools such as Notion, Google Workspace, and messaging) is used to discuss operational matters, coordinate work across services, and share information affecting the organization. Updates to entity-wide security policies and procedures are communicated to the appropriate personnel through the company's documentation hub and direct channels. Management leads communication of key issues, drawing on information from automated systems (such as monitoring, logging, and continuous control monitoring) as well as day-to-day collaboration.

Specific information systems used to support Kirha’s Context-as-a-Service system are described in the Description of Services section above.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Kirha's management performs monitoring activities to assess the quality of internal control over time. Necessary corrective actions are taken to correct deviations from company policies and procedures. This process is accomplished through a combination of ongoing monitoring activities and separate evaluations.

Kirha's monitoring activities include the following:

- Continuous control monitoring is performed through the Drata platform, which automatically and continuously tests the state of technical controls across the company's infrastructure, codebase, and pipeline, and surfaces failing controls for remediation.
- System activity is monitored through GCP Cloud Logging and Cloud Monitoring, with alert policies configured to notify personnel of anomalous or security-relevant activity for investigation and resolution.

- A monthly post-merge independent review is conducted by a founder other than the repository owner, providing independent oversight of changes, releases, and security-relevant findings. Results are recorded in the Audit Findings and Remediations database and tracked to closure.
- Vendor and third-party assessments are performed annually to identify and remediate control gaps.

Because of the size of the organization, complete independence between those who operate key controls and those who monitor them is not achievable. Kirha addresses this limitation through compensating controls, including automated and continuous control monitoring (Drata), independent tooling that enforces controls regardless of operator (for example, branch protection and automated merge gates that apply to all engineers including administrators), and the monthly independent review described above. These compensating controls are documented in the company's SDLC, Risk Register, and Statement of Applicability.

On-Going Monitoring

Kirha's management conducts ongoing monitoring of its controls and operations. Monitoring activities are used to identify deviations and to initiate corrective action through team communication, reviews, and automated notifications. Kirha has assigned responsibility for coordinating and monitoring the company's compliance and control activities to ensure the internal control environment is maintained and reviewed on an ongoing basis.

Ongoing monitoring at Kirha is accomplished through a combination of automated and manual activities, including:

- Continuous, automated control monitoring through the Drata platform, which surfaces control failures as conditions change so they can be remediated.
- Real-time system monitoring and alerting through GCP Cloud Logging and Cloud Monitoring, with alerts investigated and resolved by engineering personnel.
- The monthly post-merge independent review of changes, releases, and security-relevant findings, with results recorded and tracked to closure.

Management's close, direct involvement in Kirha's day-to-day operations helps to identify significant variances from expectations regarding internal controls. When a potential control weakness or deviation is identified, management evaluates the facts and circumstances to determine whether the incident was isolated or requires a change to the company's procedures, controls, or personnel. Corrective actions and any resulting changes are tracked to resolution. The goal of this process is to maintain the security and reliability of the service, ensure compliance with applicable requirements, and continuously improve the control environment.

Reporting Deficiencies

Kirha documents and tracks the results of its ongoing monitoring activities and any identified control deficiencies. Deficiencies and control failures are captured through the company's monitoring tools and recorded for tracking and remediation. In particular:

- The Drata platform continuously identifies failing or deficient technical controls, which are surfaced for review and remediation.
- Findings from the monthly independent review are documented in the Audit Findings and Remediations database and tracked to closure.
- Security and operational alerts from GCP Cloud Logging and Cloud Monitoring are investigated, and any resulting incidents are recorded and managed through the Incident Response process and Incident Log.

Escalation is handled directly given the size of the team: identified deficiencies and risks are communicated to management, and higher-severity issues are prioritized and addressed on an expedited basis. Corrective actions are documented and tracked to resolution, and significant or recurring deficiencies are considered by management for changes to the company's controls, procedures, or configuration.

Changes to the System in the Last 3 Months

No significant changes have occurred to the services provided to user entities in the 3 months preceding the review date.

Incidents in the Last 3 Months

No significant incidents have occurred to the services provided to user entities in the 3 months preceding the review date.

Criteria Not Applicable to the System

All Common/Security, Availability, and Confidentiality criteria were applicable to the Kirha's Kirha Context-as-a-Service System.

Subservice Organizations

This report does not include the cloud hosting services provided by GCP at multiple facilities.

Subservice Description of Services

Kirha relies on GCP for cloud hosting services to support the in-scope infrastructure and systems.

Complementary Subservice Organization Controls

Kirha's services are designed with the assumption that certain controls will be implemented by subservice organization. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Kirha's services to be solely achieved by Kirha control procedures. Accordingly, subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of Kirha.

The following subservice organization controls should be implemented by GCP to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - GCP		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Data center server floors network rooms and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval form authorized personnel and is controlled via badge access readers, biometric identification mechanism, and/or physical locks.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit.
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.

Subservice Organization - GCP		
Category	**Criteria**	**Control**
		Data centers are continuously staffed and monitored by security personnel through the use of real time video surveillance and/or alerts generated by security systems.
Availability	A1.2	Critical power and telecommunications equipment in data centers is physically protected from disruption and damage.
		Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).
		Data centers are equipped with fire detection alarms and protection equipment.
		The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.
		The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.

Kirha management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Kirha performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and the subservice organization
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Kirha's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Kirha's services to be solely achieved by Kirha control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Kirha's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Kirha.
2. User entities are responsible for notifying Kirha of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Kirha services by their personnel.

5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Kirha services.
6. User entities are responsible for providing Kirha with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Kirha of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
8. User entities are responsible for restricting access to system resources to appropriate user entity personnel.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security, Availability, and Confidentiality Categories)
Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage and ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability
Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality
Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Control Activities Specified by the Service Organization

The applicable trust services criteria, risks, and related control activities are included below and not described in narrative format in this section to eliminate redundancy. The applicable trust services criteria and related control activities included below are an integral part of Kirha's description of the system. Any applicable trust services criteria that are not addressed by control activities at Kirha are described below and within the Subservice Organization.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Personnel responsibilities for information security, are communicated to and acknowledged by personnel. Management conducts annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures. Background checks are conducted on eligible personnel prior to hire as permitted by local laws. The company maintains a documented code of conduct. Eligible personnel are required to accept the company's code of conduct during onboarding and annually thereafter. The company has a defined disciplinary sanctions process to be enacted when a member of the workforce violates the company's policies or causes a security or privacy incident. Management retains documentation of instances when the disciplinary process was enacted. Internal communication channels are in place for employees to report failures, events, incidents, concerns, and other issues to company management.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The Company's board of directors has a documented charter that outlines its oversight responsibilities for internal control. The company's board of directors, owners, senior leadership, or equivalent body meets at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies. Meeting minutes, including decisions made and action items, are documented. The Company uses compliance automation software to identify, select, and continuously monitor internal controls. Management conducts annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures. The board of directors includes members independent from management who are not involved in control operations. Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	An organizational chart is in place to describe the organizational structure and reporting lines. The chart is available to all employees and is updated upon changes to the organizational structure. The Company's board of directors has a documented charter that outlines its oversight responsibilities for internal control. Personnel responsibilities for information security, are communicated to and acknowledged by personnel. The board of directors includes members independent from management who are not involved in control operations. The company has documented job descriptions for each position at the company, which include roles and responsibilities as well as required qualifications, skills, and experience for the role. The company performs due diligence activities prior to engaging with a vendor. Results of the due diligence activities including action items are documented. The company obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the company's requirements, and the results of the review and action items, if any, are documented.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company has established training programs to help personnel gain awareness of information security best practices. Personnel are required to complete the training during onboarding and annual refresher training is provided to personnel at least annually and as deemed necessary. Management conducts annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures. Background checks are conducted on eligible personnel prior to hire as permitted by local laws. Management evaluates candidates for employment through a formal screening process. The process may include verification of academic and professional qualifications, identity verifications, validation of personal or professional references, technical interviews, or other steps as deemed applicable by the organization.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
		The company performs due diligence activities prior to engaging with a vendor. Results of the due diligence activities including action items are documented. The company obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the company's requirements, and the results of the review and action items, if any, are documented. Policies and procedures are in place that outline the talent acquisition, performance evaluation and annual training processes.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	An organizational chart is in place to describe the organizational structure and reporting lines. The chart is available to all employees and is updated upon changes to the organizational structure. Personnel responsibilities for information security, are communicated to and acknowledged by personnel. Management conducts annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures. The company maintains a documented code of conduct. Eligible personnel are required to accept the company's code of conduct during onboarding and annually thereafter. The company has documented job descriptions for each position at the company, which include roles and responsibilities as well as required qualifications, skills, and experience for the role. The company has a defined disciplinary sanctions process to be enacted when a member of the workforce violates the company's policies or causes a security or privacy incident. Management retains documentation of instances when the disciplinary process was enacted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company has defined and documented an information security policy and other topic-specific policies to support the functioning of internal control. A documented network diagram is in place to document system boundaries and connections to external networks. The diagram is reviewed and approved by management at least annually and updated as necessary when there are changes to the environment. Company policies are accessible to all employees and, as applicable, third-parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter. Network security controls are in place to restrict public access to remote server administration ports to authorized Internet Protocol (IP) addresses or address ranges only. Cloud resources are configured to deny public access. Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied. An Intrusion Detection System (IDS) is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has defined and documented an information security policy and other topic-specific policies to support the functioning of internal control. The company's board of directors, owners, senior leadership, or equivalent body meets at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies. Meeting minutes, including decisions made and action items, are documented. Personnel responsibilities for information security, are communicated to and acknowledged by personnel.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Company policies are accessible to all employees and, as applicable, third-parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter. The company has established training programs to help personnel gain awareness of information security best practices. Personnel are required to complete the training during onboarding and annual refresher training is provided to personnel at least annually and as deemed necessary. Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs. The company maintains a documented code of conduct. Eligible personnel are required to accept the company's code of conduct during onboarding and annually thereafter. The company has documented job descriptions for each position at the company, which include roles and responsibilities as well as required qualifications, skills, and experience for the role. The company provides external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined Service-Level Agreement (SLAs). Internal communication channels are in place for employees to report failures, events, incidents, concerns, and other issues to company management.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company's board of directors, owners, senior leadership, or equivalent body meets at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies. Meeting minutes, including decisions made and action items, are documented. Personnel responsibilities for information security, are communicated to and acknowledged by personnel.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
		The company maintains a third-party register that includes a complete and accurate list of third-parties, relationship owners, description for each of the services provided, risk ratings, results of third-party risk management activities, etc. The Company executes agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outline the responsibilities of each vendor or service provider. The company maintains a publicly available terms of service for use of the system. All users must agree to the terms of service prior to using the system. The company communicates service commitments and system requirements to customers through company website. The company provides notification to relevant parties of any changes to service commitments and system requirements. The company provides user guides, help articles, system documentation or other mechanisms to users to share information about the design and operation of the system and its boundaries. The information provided includes functional and nonfunctional requirements related to system processing and information specifications required to support the use of the system. The company provides external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined SLAs. Internal communication channels are in place for employees to report failures, events, incidents, concerns, and other issues to company management.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company has defined and documented an information security policy and other topic-specific policies to support the functioning of internal control. An organizational chart is in place to describe the organizational structure and reporting lines. The chart is available to all employees and is updated upon changes to the organizational structure. The company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented. The Company uses compliance automation software to identify, select, and continuously monitor internal controls. Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities. Company policies are accessible to all employees and, as applicable, third-parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter. Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs. The company communicates service commitments and system requirements to customers through company website. The company provides notification to relevant parties of any changes to service commitments and system requirements.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Management has defined company objectives, including mission and vision statements, operational objectives at the entity and functional levels, financial performance goals, and other objectives as appropriate, to serve as the basis for risk assessment activities. Management communicates its objectives and any changes to those objectives to personnel.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented. Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities. The company performs due diligence activities prior to engaging with a vendor. Results of the due diligence activities including action items are documented. The company obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the company's requirements, and the results of the review and action items, if any, are documented.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented. Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities. The Company performs an evaluation of fraud risks at least annually, either as a separate evaluation or as part of the overall enterprise risk assessment. The evaluation of fraud risk is performed in accordance with the company's risk assessment methodology. The company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented. The Company uses compliance automation software to identify, select, and continuously monitor internal controls. Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities. The company performs due diligence activities prior to engaging with a vendor. Results of the due diligence activities including action items are documented. The company obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the company's requirements, and the results of the review and action items, if any, are documented.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Changes to the entity's systems, applications, technologies, tools, and leadership are considered and evaluated as part of the annual comprehensive risk assessment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Monitoring Activities		
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The Company tests the integrity and completeness of backed-up data at least annually. Management performs user access reviews quarterly to validate user accounts, including third-party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical access as necessary. Changes resulting from the review, if any, are documented and implemented. The company has defined and documented an information security policy and other topic-specific policies to support the functioning of internal control. The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented. The Company uses compliance automation software to identify, select, and continuously monitor internal controls. Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities. The company conducts annual vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel and vulnerabilities are tracked to resolution in accordance with company policies. The company has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts. An external penetration test of production environments is performed by an independent third-party annually or after any significant infrastructure or application changes. Results are reviewed by management, and vulnerabilities are tracked to resolution in accordance with company policies.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Monitoring Activities		
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Company policies are accessible to all employees and, as applicable, third-parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter. Management conducts annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures. Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs. The company performs due diligence activities prior to engaging with a vendor. Results of the due diligence activities including action items are documented. The company obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the company's requirements, and the results of the review and action items, if any, are documented. Production systems and resources are monitored and automated alerts are sent out to personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalated per policy if necessary.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company's board of directors, owners, senior leadership, or equivalent body meets at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies. Meeting minutes, including decisions made and action items, are documented. The Company uses compliance automation software to identify, select, and continuously monitor internal controls. Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities. Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The Company uses compliance automation software to identify, select, and continuously monitor internal controls. The Company has a defined business continuity plan that outlines strategies for maintaining operations during a disruption. Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities. The Company has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. The Company conducts tests of the business continuity and disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary. The board of directors includes members independent from management who are not involved in control operations. Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company has defined and documented an information security policy and other topic-specific policies to support the functioning of internal control. The Company uses compliance automation software to identify, select, and continuously monitor internal controls. Company policies are accessible to all employees and, as applicable, third-parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has defined and documented an information security policy and other topic-specific policies to support the functioning of internal control. The Company uses compliance automation software to identify, select, and continuously monitor internal controls.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Company policies are accessible to all employees and, as applicable, third-parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter. Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs. The company has documented job descriptions for each position at the company, which include roles and responsibilities as well as required qualifications, skills, and experience for the role.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company has developed and documented a policy that outlines requirements for access control. Management performs user access reviews quarterly to validate user accounts, including third-party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical access as necessary. Changes resulting from the review, if any, are documented and implemented. A centralized asset register is maintained for physical, cloud, and other assets that includes descriptive attributes for asset accountability such as owner, description, location, classification, and other information based on the type of asset. Processes are in place to maintain an updated inventory through automated mechanisms. Key-management policies and procedures are documented and implemented including: generation of strong cryptographic keys, secure distribution, and secure storage of cryptographic keys used to protect sensitive data. The company retires, replaces or destructs cryptographic keys that are no longer used or needed or when the key expires, the integrity of the key has been weakened, or the key is known or suspected to be compromised, in accordance with documented company policies and procedures. Retired or replaced keys are not used for encryption operations. The company restricts access to system components and data to only those individuals whose job requires such access. System users are authenticated via MFA prior to being granted access the system. Remote access to the entity's network and systems (including that of users, administrators, and external access from third-parties or vendors including access for maintenance sessions) requires MFA. The company has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Audit logs are enabled and active for system components and sensitive data in accordance with company policies. Data at rest is encrypted using strong cryptographic algorithms. Data in transit is encrypted using strong cryptographic algorithms. Group, shared, or generic account usage is prevented unless strictly necessary and supported by documented business justification and management approval. Mechanisms are in place to confirm individual user identity before access to the account is granted and to trace every action to an individual user. Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel. The company has implemented technical measures to protect stored user passwords for the system. The company has implemented segregation controls so that customers cannot impact or access data or resources of other customers. The company has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. Access requests to information resources, including access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. System access is revoked within one business day of effective termination date for terminated users. Authentication to systems requires the use of unique identities. Root password authentication to production resources is disabled and only allowed under exceptional circumstances for a limited time duration based on documented business justification and approval from management. The company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company. The company uses network segmentation to isolate portions of the environment and to control traffic between them based on security and business needs.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		The company assigns permissions through groups or roles based on the principle of least privilege and limits the use of wild-card permissions or broad-access patterns. The company uses a centralized system that collects and stores logs of system activity and sends alerts to personnel based on pre-configured rules. Access to logs is restricted to authorized personnel. Access to the root account in the cloud infrastructure provider is monitored. Login activity for the root account is investigated and validated for appropriateness.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company has developed and documented a policy that outlines requirements for access control. Management performs user access reviews quarterly to validate user accounts, including third-party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical access as necessary. Changes resulting from the review, if any, are documented and implemented. The company has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc. Access requests to information resources, including access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. System access is revoked within one business day of effective termination date for terminated users. The company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company has developed and documented a policy that outlines requirements for access control. Management performs user access reviews quarterly to validate user accounts, including third-party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical access as necessary. Changes resulting from the review, if any, are documented and implemented.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		The company has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc. Access requests to information resources, including access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. System access is revoked within one business day of effective termination date for terminated users. The company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The Company disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures. The Company has documented policies and procedures for erasure or destruction of information that has been identified for disposal.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The deployed anti-malware solution is kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware. The implemented anti-malware solutions are configured to perform real-time scans or to perform continuous behavioral analysis of systems or processes. The company restricts access to system components and data to only those individuals whose job requires such access. Remote access to the entity's network and systems (including that of users, administrators, and external access from third-parties or vendors including access for maintenance sessions) requires MFA. Anti-malware software is installed on company-managed devices.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Data at rest is encrypted using strong cryptographic algorithms. Data in transit is encrypted using strong cryptographic algorithms. Network security controls are in place to restrict public access to remote server administration ports to authorized IP addresses or address ranges only. Cloud resources are configured to deny public access. Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied. A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary. A web application firewall is in place to protect public-facing web applications from outside threats. An IDS is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected. Remote access to production systems is only available through an encrypted connection.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company restricts access to system components and data to only those individuals whose job requires such access. Remote access to the entity's network and systems (including that of users, administrators, and external access from third-parties or vendors including access for maintenance sessions) requires MFA. Data at rest is encrypted using strong cryptographic algorithms. Data in transit is encrypted using strong cryptographic algorithms. Network security controls are in place to restrict public access to remote server administration ports to authorized IP addresses or address ranges only. Cloud resources are configured to deny public access.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied. A web application firewall is in place to protect public-facing web applications from outside threats. An IDS is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected. Remote access to production systems is only available through an encrypted connection. The deployed anti-malware solution is kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware. The implemented anti-malware solutions are configured to perform real-time scans or to perform continuous behavioral analysis of systems or processes. Changes to system components in the production environment are made according to established procedures that include documentation and testing. The company has enabled a change-detection mechanism to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts. Anti-malware software is installed on company-managed devices. Access to make changes in production environments is restricted to authorized personnel in accordance with segregation of duties principles and the company's documented policies and procedures. Production systems and resources are monitored and automated alerts are sent out to personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalated per policy if necessary. A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company has identified and documented baseline security configuration standards for system components in accordance with industry-accepted hardening standards or vendor recommendations. These standards are reviewed at least annually and updated as needed and verified to be in place before or immediately after a production system component is installed or modified. The company conducts annual vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel and vulnerabilities are tracked to resolution in accordance with company policies. The company has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts. An external penetration test of production environments is performed by an independent third-party annually or after any significant infrastructure or application changes. Results are reviewed by management, and vulnerabilities are tracked to resolution in accordance with company policies. The company has enabled a change-detection mechanism to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts. Network security controls are in place to restrict public access to remote server administration ports to authorized IP addresses or address ranges only. The company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company. Cloud resources are configured to deny public access. Storage buckets that contain sensitive data have versioning enabled to preserve, retrieve, and restore versions of objects.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Management has defined company objectives, including mission and vision statements, operational objectives at the entity and functional levels, financial performance goals, and other objectives as appropriate, to serve as the basis for risk assessment activities. Management communicates its objectives and any changes to those objectives to personnel. Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied. Production systems and resources are monitored and automated alerts are sent out to personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalated per policy if necessary. A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary. A web application firewall is in place to protect public-facing web applications from outside threats. An IDS is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The deployed anti-malware solution is kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware. The implemented anti-malware solutions are configured to perform real-time scans or to perform continuous behavioral analysis of systems or processes. Audit logs are enabled and active for system components and sensitive data in accordance with company policies. The company has enabled a change-detection mechanism to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts. Anti-malware software is installed on company-managed devices.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Network security controls are in place to restrict public access to remote server administration ports to authorized IP addresses or address ranges only. The company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company. Cloud resources are configured to deny public access. The company uses a centralized system that collects and stores logs of system activity and sends alerts to personnel based on pre-configured rules. Access to logs is restricted to authorized personnel. The company provides external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined SLAs. Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied. Production systems and resources are monitored and automated alerts are sent out to personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalated per policy if necessary. A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary. A web application firewall is in place to protect public-facing web applications from outside threats. Internal communication channels are in place for employees to report failures, events, incidents, concerns, and other issues to company management. An IDS is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected. Part of this criterion is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The company has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan is reviewed at least annually and updated as needed according to lessons learned from previous incidents and industry developments. The company evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures. The company has identified and documented roles and responsibilities for incident management. The company provides external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined SLAs. Internal communication channels are in place for employees to report failures, events, incidents, concerns, and other issues to company management.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations. The company has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan is reviewed at least annually and updated as needed according to lessons learned from previous incidents and industry developments. The company evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures. The company has identified and documented roles and responsibilities for incident management.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company provides external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined SLAs. Internal communication channels are in place for employees to report failures, events, incidents, concerns, and other issues to company management. The Company tests the integrity and completeness of backed-up data at least annually. The company has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan is reviewed at least annually and updated as needed according to lessons learned from previous incidents and industry developments. The Company has a defined business continuity plan that outlines strategies for maintaining operations during a disruption. The Company has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. The Company conducts tests of the business continuity and disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary. The company has identified and documented roles and responsibilities for incident management.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Change Management		
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Changes to system components in the production environment are made according to established procedures that include documentation and testing. The company uses a version control system to manage source code, change documentation and tracking, release labeling, and other change management tasks. Access to the version control system is restricted to authorized personnel. The company has enabled a change-detection mechanism to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts. The company has a documented policy that describes the requirements for managing changes across the organization, including changes to infrastructure, systems, and applications. Access to make changes in production environments is restricted to authorized personnel in accordance with segregation of duties principles and the company's documented policies and procedures. Pre-production environments are separated from production environment and the separation is enforced with access controls. The company communicates system changes via e-mail communications. Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Mitigation		
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented. Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented. The company has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities. The company performs due diligence activities prior to engaging with a vendor. Results of the due diligence activities including action items are documented.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Mitigation		
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**
		The company maintains a third-party register that includes a complete and accurate list of third-parties, relationship owners, description for each of the services provided, risk ratings, results of third-party risk management activities, etc. The Company executes agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outline the responsibilities of each vendor or service provider. The company obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the company's requirements, and the results of the review and action items, if any, are documented.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY		
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Production systems and resources are monitored and automated alerts are sent out to personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalated per policy if necessary. The company monitors processing capacity and use of resources continuously to manage demand and to enable the implementation of additional resources as necessary. The company uses a load balancer to automatically distribute incoming traffic across multiple targets. The company has enabled auto-scaling configurations to provision new cloud resources when predefined capacity thresholds are met.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	The company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented. The Company has a defined backup policy that establishes the requirements for backup information, software and systems. Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities. Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs. The company has implemented redundancy strategies for equipment, systems, and processes as deemed necessary per the business continuity plan to meet availability requirements. Backups of production data are performed daily and are configured to be retained in accordance with the retention periods established in company policies and procedures. Automated notifications are sent to personnel in the event of a backup failure. Backup failures are investigated and resolved by engineering personnel following company policies and procedures.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY		
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Part of this criterion is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization. The Company tests the integrity and completeness of backed-up data at least annually. The Company has a defined business continuity plan that outlines strategies for maintaining operations during a disruption. The Company has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. The Company conducts tests of the business continuity and disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY		
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company has established a data classification policy in order to identify the types of information stored or processed by the organization and the protection measures that are required for each. Personnel, including employees and contractors, are required to sign an agreement that outlines confidentiality requirements prior to hire. Personnel responsibilities for information security, are communicated to and acknowledged by personnel. The company restricts access to system components and data to only those individuals whose job requires such access. Data at rest is encrypted using strong cryptographic algorithms. Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	The company has established a data classification policy in order to identify the types of information stored or processed by the organization and the protection measures that are required for each. The company disposes of customer data upon termination of services in accordance with contractual agreements. The Company disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures. The Company has documented policies and procedures for erasure or destruction of information that has been identified for disposal. A centralized asset register is maintained for physical, cloud, and other assets that includes descriptive attributes for asset accountability such as owner, description, location, classification, and other information based on the type of asset. Processes are in place to maintain an updated inventory through automated mechanisms. The company has documented a policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. The Company has implemented processes to change credentials based on a defined schedule.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN ASSURANCE's examination of the controls of Kirha was limited to the Trust Services Criteria, related criteria and control activities specified by the management of Kirha and did not encompass all aspects of Kirha's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria;
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization;
- Determine whether the criteria are relevant to the user entity's assertions; and
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.