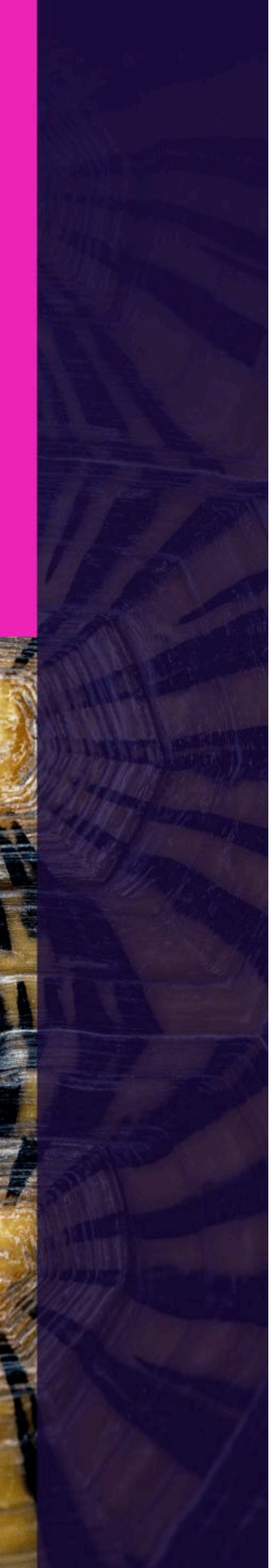
GoodData

# GoodData.CN
# Security Whitepaper

May 2025

# Table of contents

This whitepaper is organized into four sections, starting with the "Executive Overview" and ending with our final thoughts in the "Conclusion". After the overview, "GoodData.CN Security" explains the security measures that are applied to the GoodData.CN product and provides guidance on the security concepts and techniques that GoodData customers should use to ensure security. The third section, "GoodData Security Overview," provides an overview of GoodData's information security management system, built on the ISO 27001 standard.



# Executive Overview

GoodData offers a comprehensive API-first product suite comprising three distinct pillars — BI, AI, and the Analytics Lake. The end- to-end, composable platform enables businesses to design and deploy custom data applications and seamlessly integrate AI-assisted analytics wherever users need them. GoodData products offer developer-friendly features, such as declarative metadata and open API- and SDK-based integration, enabling the use of software development best practices in analytics development.

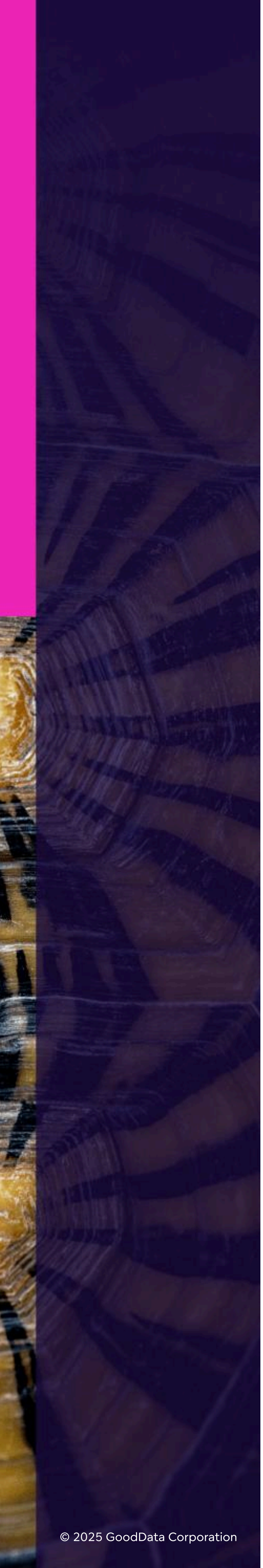
The GoodData product suite is available in two distinct deployment options — a fully-managed (GoodData Cloud) or self-managed on-premise deployment (GoodData.CN). GoodData.CN follows the same development procedures as GoodData Cloud, including secure development policies and practices, requirements on access controls, segregation of duties, code review, static and dynamic code analysis, etc. The scope of this whitepaper is limited to a description of the security practices applicable to GoodData.CN. For more comprehensive information on GoodData operations, including its organizational security, please refer to our standalone GoodData Cloud whitepaper.

GoodData.CN is purpose-built to scale with microservices. Customers can deploy it in containers next to their data, whether it is in a public or private cloud or on-premises. GoodData connects to customer data sources and can be integrated with the user authentication setup. Thanks to declarative APIs, everything customers do and build with GoodData can be easily stored in a version control system.

GoodData realizes that protecting customer data, mitigating any potential risks, and complying with relevant data protection laws, regulations, and standards are essential to building trust and delivering high-quality products. GoodData takes a risk-based approach to security, and this paper details the measures and technologies in place to protect our customers. It also outlines our internal security compliance standards to assure our customers about the diligence and robustness of our information security management system.

GoodData products and its operations adhere to the following certifications, frameworks, and best practices, demonstrating our commitment to data security and privacy (where relevant to the on-premise deployment):

- SOC 2 - SOC for service organizations: Trust Services Criteria for Security, Availability, and Confidentiality. We have maintained the SOC 2 certification since 2013 with a semiannual audit by an independent reputable assessor (KPMG, EY, currently Schellman).



- Compliance with the ISO 27001:2013 international standard for information security management systems, and adherence to best practices documented in ISO 27002.
- Compliance with all relevant privacy regulations, including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).
- Registered participant in the EU-U.S (incl. The UK extension) and Swiss-U.S. Data Privacy Frameworks.
- HIPAA compliance.

## Defense in Depth

Like any other reputable SaaS platform provider, GoodData does not rely solely on the protection of its perimeter to safeguard customer data. Rather, it is a well-designed solution that considers every layer, from the physical security measures at the data center to the access privileges that determine what data an individual user can access. As a best-in-class analytics provider, GoodData uses this approach to protect customer data, and respects the secure-by-default principle. Leveraging our long-term experience in providing secure, reliable analytics platforms, GoodData.CN has been built to align with up-to-date best practices for both public and private cloud environments.

## Regional Deployments

Data sovereignty is a complex issue involving the technical, regulatory, and, at times, even the political arena. Understanding the complexities of this issue — and thanks to its standardized blueprint for a data center in a public cloud — GoodData.CN is ready to be deployed in any data center worldwide (according to the needs of its customers).

# GoodData.CN Security

## Application Security

GoodData not only allows customers to access their reports, dashboards, and data, but also enables direct integration with their other software so they can provide clients with a seamless experience. The GoodData application employs many security measures to enable the secure flow of data from the customers' data sources to the end users' workspaces.

### Integration and APIs

All integrations with the GoodData API leverage HTTPS/TLS encryption. The user security model is enforced at the API level, ensuring that data retrieved through the API is still subject to user authentication and access privileges. For more information on this topic, please see the User Security section below.

## Connecting to Customer Data Sources

A data source is a logical object that represents the database where your source data is stored. To integrate your database into GoodData, you connect it to a workspace. The connection is protected via the same encryption as any other integration with GoodData. To help securely connect your data source, you should create a separate set of credentials, IP whitelisting them (or using private VPC links) then ensures the database is accessible only from your GoodData.CN deployment.

## Multitenancy

GoodData allows customers to manage an environment with many clients. In this multi-tenant environment, each client can access only the entities and data that they are enabled to access. Without appropriate permissions, a client cannot access those entities or data. Each customer has its own Organization within a shared GoodData.CN instance and is fully separated from the other customers on the metadata level.

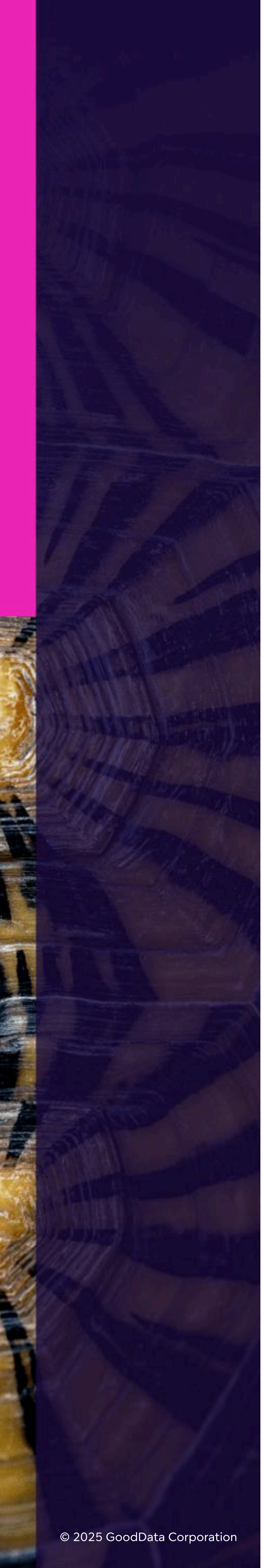
Customers may also choose a dedicated deployment hosting model, where a separate Kubernetes cluster is dedicated to each single customer. In this setup, additional custom technical security safeguards can be implemented. This option is suitable for customers with strict or non-standard security requirements, or those who expect that their solution will need to scale up/down dynamically.

Each object or data entity is tied to a specific Organization, thus ensuring strong segregation between individual customers or applications. Within the Organization, the objects and entities can be further assigned to one or more clients.

## Workspaces

A workspace hierarchy in a multi-tenant environment defines how entities of a particular tenant (parent workspace) can be shared with other tenants (child workspaces) in read-only mode within a single Organization. The child workspaces inherit the parent workspace’s logical data model (LDM), analytical model, connected data sources, and so on. When the parent workspace receives a new entity, it becomes available to its child workspaces.

Child workspaces inherit entities from their parent workspace as well as from that parent workspace’s own parent workspaces — all the way up to the root workspace. The root workspace is the top-level workspace in the hierarchy, which does not have a parent workspace. Customers may set up as many root workspaces as needed.



### User Access

End users may access the data only through the application layer. Whether this access is through the user interfaces or through the publicly available API, it enforces user access controls to permit access to customer data only to authorized users and personnel.

## User Security

User security is enforced through various security measures that allow authorized users to view only the strictly defined set of objects and data needed to perform their jobs.

### Authentication

GoodData's architecture relies on a centralized authentication and authorization security framework to control access to services. GoodData supports the OAuth standard so that our customers can use their own IAM to ensure seamless integration with their ecosystem. It also allows them to manage user access, including the authentication mechanism, session expiration, etc., according to their company standards. OIDC tokens are stored in secure HTTP Cookies. API tokens may be created to access GoodData from command line tools or for integration with other customer systems.

### User Groups, Permissions, and Data Filters

By default, only the administrator starts off with the permissions necessary to view and modify the objects. To make your project accessible to other users, you should group users into appropriate user groups and assign permissions to these groups according to the use case.

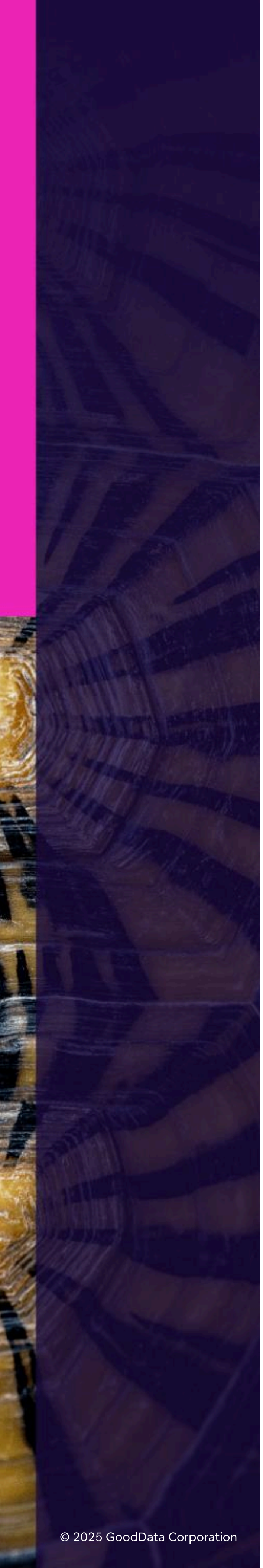
Permissions are organized into hierarchy and scope. The scope is determined by an object type's unique features which can be further restricted or enabled via permissions.

In addition, Workspace Data Filters and User Data Filters allow you to limit what data from a parent workspace is available to their child workspaces and users (additionally, we provide Dashboard Filters, but please note these are not considered a data security feature).

# GoodData Security Overview

## Information Security Policies

GoodData has established a comprehensive set of information security policies, processes, and standards. Our Information Security Management System (ISMS) is based on the international standard ISO 27001:2013. We are building our security procedures and standards upon the National Institute of Standards and Technology's (NIST's) Special Publication (SP) 800 series (incl. NIST SP 800-53). Our security controls are mapped against a wide range of standards, such as SOC 2, ISO 27001:2013, HIPAA, etc.



Our policies are owned and approved by appropriate management representatives and communicated to affected internal and external personnel. Policies are reviewed on an annual or ad hoc basis in case of a significant business change to ensure ongoing suitability, adequacy, and effectiveness.

## Organization of Information Security

GoodData has appointed a dedicated information security organization. The Head of Security & Compliance has the executive responsibility for information security across the corporation and leads the Security & Compliance department.

The Head of Security & Compliance also chairs the GoodData Security Council, a cross-functional group of senior stakeholders established for the ongoing oversight of GoodData's information security program, both from a design and an effectiveness point of view.

The council's senior roles bring together a wide range of perspectives, ensure the efficiency of the security program, and reinforce that information security is a business issue requiring involvement across the corporation. The council meets monthly to review security events and issues, discuss open and emerging security risks, and ensure ongoing alignment between security and business objectives.

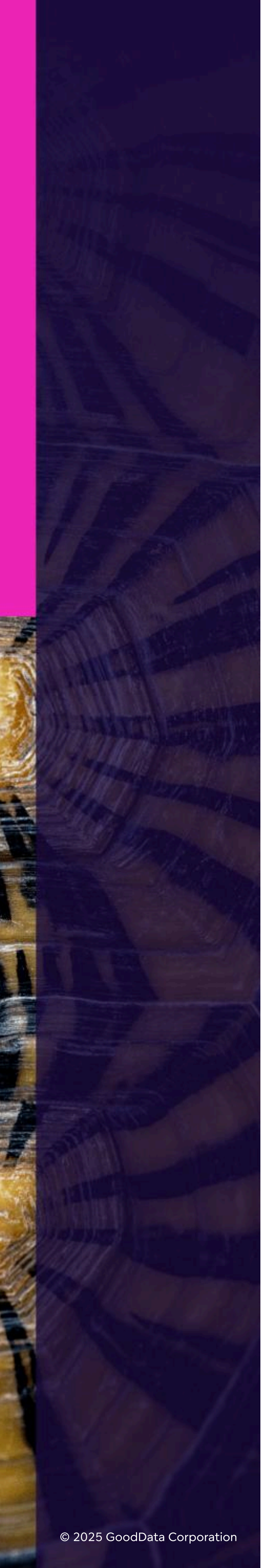
GoodData has implemented risk management practices into its day-to-day operations and decisions. This includes proactively evaluating risks, prioritizing critical areas, and implementing measures to mitigate vulnerabilities. In addition, we perform an annual formal risk assessment based on NIST and OWASP methodologies, including the identification of critical assets, threats, and vulnerabilities, and the evaluation of the impact and probability of individual risks.

GoodData's Security & Compliance department, together with the internal legal team, monitor the global regulatory landscape to identify emerging data security and privacy-related laws, standards, and regulations, and ensure that customer data is protected accordingly.

## Human Resources Security

All new employees are subject to an industry-standard background check. GoodData has established three levels of security clearance. The highest level, which has the most demanding background check requirements and must be regularly renewed every three years, is mandatory for all key security-related roles and for personnel with the highest level of administrative access to the GoodData Cloud and critical internal systems.

Contractual agreements include confidentiality clauses and information security responsibilities, ensuring the relevant employee



responsibilities (including the non-disclosure clauses) remain valid after job termination. To mitigate the risks, we also rotate all relevant technical shared credentials as part of the employee termination process.

During onboarding and annually, employees familiarize themselves with the company's Code of Conduct. This includes ethical behavior standards, employee compliance requirements, guidance for safeguarding intellectual property and maintaining confidentiality, and reporting of violations and whistleblowing.

GoodData has established a disciplinary process. Management reviews all compliance violations, and sanctions are taken in the event of high-risk violations. All employees have to sign an acknowledgment of the possible consequences of policy violations, which include loss of access, employment termination, and/or criminal prosecution.

Management is responsible for security compliance in their areas of business. Documented job descriptions further outline specific security-related rights and responsibilities for all roles.
All internal and external employees must complete security awareness training as part of their onboarding and on an annual basis, including familiarizing themselves with information security policies. Additional role-specific training is required for privileged access and for work with highly regulated or sensitive data.

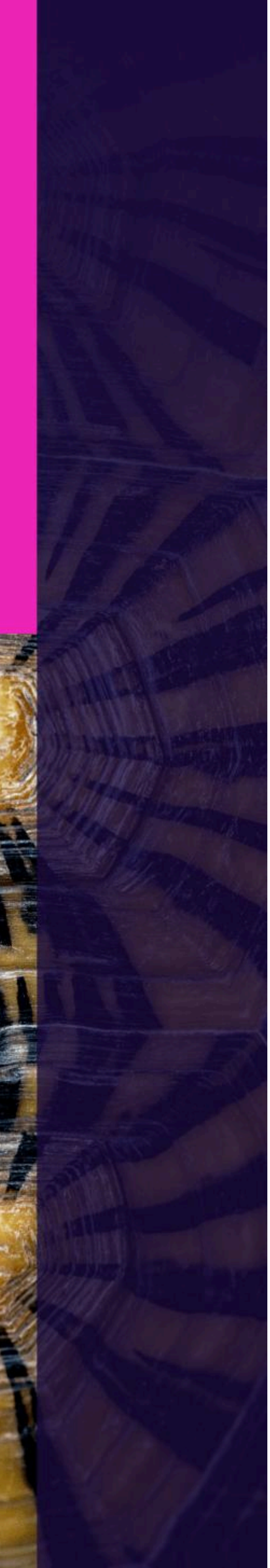
## Data Classification and Asset Management

GoodData maintains inventories of relevant IT assets and has established responsibilities and assigned ownership. Our internal data classification policy defines five levels of data classification as well as mandatory data protection requirements on systems that process particularly classified data.

All internal systems are labeled in line with data classification rules to ensure the enforcement of adequate data protection.

GoodData employee laptops and BYODs follow defined security rules, and centralized monitoring is established to ensure ongoing compliance. We use only MacOS- and Linux-based laptops. All MacOS-based laptops are equipped with centrally managed antivirus protection. All laptops are protected by a firewall, hard drives are fully encrypted, user accounts are protected by strong passwords, and session timeout with screen lock is activated. Additionally, endpoints of non-technical personnel have an MDM solution installed and are fully managed by the internal IT department. Acceptable use rules are documented and communicated to all employees.

Upon termination of employment, laptops are collected and wiped, and BYODs are deauthorized from company systems. Whenever possible, a remote wipe is enabled and triggered upon the report of a lost or stolen device.



## Access Control

GoodData has implemented an access control policy and enforcing mechanisms that comply with industry best practices. These rules are applied across all internal systems to ensure that only authorized users with proper business justification have access. We honor the principle of least privilege.

We apply industry-standard password policies and, whenever possible, use single sign-on with MFA for access to internal company systems. We review access entitlements across all company systems at minimum on an annual basis.

## Encryption and Cryptography

GoodData uses state-of-the-art cryptography technology to protect data in transit and at rest, and has a documented cryptographic policy and standards.

All traffic outside of GoodData product deployments is encrypted in transit, and uses TLS 1.2 or higher and AES-256 by default.

## Network Security

GoodData.CN containers support running in a Kubernetes cluster with hardened and secured network configuration, including strict separation of networks and firewalls that ensure only designated externally facing microservices are reachable from external networks through dedicated load balancers.

## Security Operations

The GoodData security team evaluates, investigates, and tracks security-related events to resolution. They are also responsible for developing and maintaining a comprehensive security monitoring and security response program on the technical and organizational levels, as well as the corporate patch and vulnerability management program.

We have established industry-standard patch and vulnerability management procedures. Container images are scanned both at build time and in runtime. Our operations personnel monitor relevant security groups, upstream software providers, and hardware vendors for patch and vulnerability notices, and we have defined SLAs for remediation. Critical patches are handled via incident management procedures. Compliance with SLAs is monitored by the service delivery function and is reviewed by management on a monthly basis.

For details around monitoring of user access entitlement and usage, please refer to the Access Control section.

## Security Incident Management

GoodData has established an industry-standard security incident response plan. We train our staff to ensure that all potential security incidents are identified and reported in a timely manner. Our incident response team is on call 24x7x365, and we have defined protocols and escalation trees for the handling of security incidents and, when required by the nature of the incident and applicable contractual commitments and regulatory requirements, for the notification of the affected parties as well as the authorities. Procedures for collection of evidence ensure chain of custody.

Following the resolution of a security incident, GoodData conducts root cause analysis (RCA) and, as applicable, implements changes to its technology and procedures to prevent regressions or repetitions.

GoodData maintains industry-standard commercial insurance covering cybersecurity incidents and has engaged external breach services to assist in case of a major security incident.

## System Development, Maintenance, and Acquisition

We follow industry-standard secure development life cycle practices. A formal change control process minimizes the risks associated with system changes. The process enables tracking of changes made to the systems and verifies that risks have been assessed, interdependencies explored, and necessary policies and procedures considered and applied before any change is authorized. We have integrated static and dynamic security testing in our CI/CD infrastructure, and the enforced peer code review includes secure development considerations.

All new features and capabilities are managed as projects with the input of a Security Architect role to maintain the integrity of security measures across all components. To ensure that security is built into all aspects of GoodData.CN, the GoodData engineering team follows the DevSecOps methodology. Our software engineers and operations staff are trained in secure development practices and utilize a wide range of technical processes. These processes are built directly into the continuous integration infrastructure to address risks related to code flaws and vulnerabilities, as well as to prevent the promotion of changes without proper review and approval. Before rolling out to production, we review the implementation against the design and conduct penetration tests for new or significantly modified components.

## Machine Learning and AI

All GoodData features leveraging Machine Learning and AI, including intelligent (semantic) search, natural language processing, predictive analytics, and AI assistants are designed in a responsible way that acknowledges the potential security risks of these technologies. We have taken steps to ensure all AI models used by GoodData are secure, accurate, transparent, and compliant with both regulatory standards and individual customer commitments.

GoodData AI features also leverage state-of-the-art LLMs provided by external parties like OpenAI. No raw customer data is sent to these services, except for a semantically relevant subset of metadata (accessible to the user who is using the feature), keeping the customer data secure within it internal perimeter and minimizing exposure to external risks. GoodData allows users to audit all AI interactions, providing full visibility into the prompts and responses generated by the AI models. This transparency ensures that users can trace how AI-driven decisions are made, enhancing accountability and trust.

GoodData (or its suppliers) never trains models on customer data unless the customer explicitly requests it. A model trained on customer data is treated in the same way as the original customer data and is never reused for any other purposes except those agreed upon with the customer.

## Vendor Management

All vendors with access to GoodData are rigorously reviewed for security and compliance practices, and we have contractual arrangements in place to ensure their ongoing compliance with our security requirements. We review the contractual performance of these vendors and their adherence to security and compliance requirements annually.

## Business Continuity and Disaster Recovery

GoodData follows the international standard ISO 22301 for its business continuity and disaster recovery management. We have completed business impact assessments for all key corporate processes and have documented business continuity and disaster recovery plans.

## Compliance

GoodData complies with various data protection standards. Our fully-managed product undergoes an annual SOC 2 Type II audit review by an independent reputable third party. GoodData maintains compliance with the ISO 27000 standards family, and builds its security practices upon industry standards, including applicable NIST and OWASP standards and recommendations.

We have policies and procedures to ensure appropriate protection of PII and personal data. We comply with GDPR, CCPA, HIPAA, and similar privacy regulations globally.

We monitor the emerging legislation and standards to maintain compliance and achieve best-in-class security of our products.

We continuously monitor, review, and audit our security compliance. We do this on the policy and technical levels, both internally and using independent external assessors.

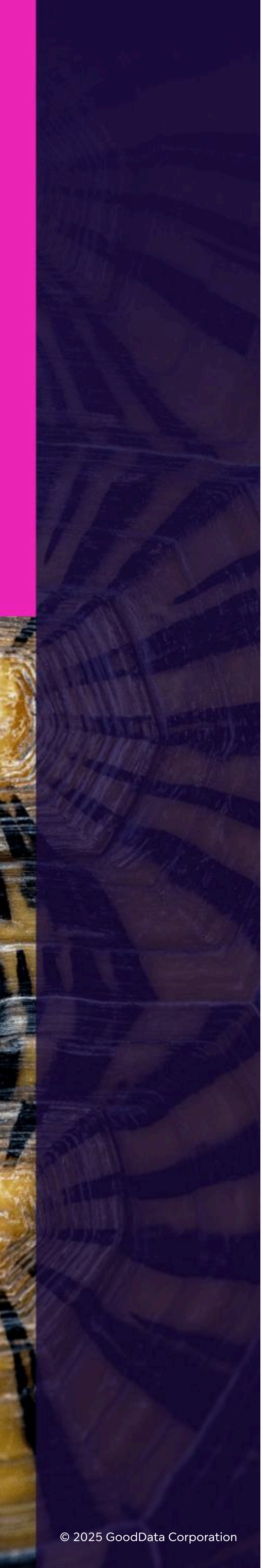
External reputable penetration testers conduct a comprehensive penetration test of the complete GoodData.CN API set on an annual basis. The entire GoodData infrastructure (including GoodData's office network) is subject to semiannual "weakest link" penetration tests and weekly vulnerability scans. We partner with two independent external penetration and vulnerability test providers who alternate on all test types to achieve above-standard coverage and depth of testing.

## Conclusion

At GoodData, we take pride in our vigilance in protecting our customers' data assets. We continually stress that a mature security organization requires coordinated dedication across technology, policy, procedures, and people. This dedication is underscored by the risk-based approach to implementing strength at every layer of security, minimizing any potential vulnerability or weakness.

We want our customers to know that this approach adequately protects their data, and we welcome the opportunity to discuss these practices and approaches further.

We also encourage our customers to consider the criticality and sensitivity of their usage of GoodData and, in line with the recommendations provided in this whitepaper, to implement adequate technical and administrative safeguards to achieve the desired level of security. The GoodData Security Team is looking forward to assisting with the implementation.



GoodData Corporation reserves the right to amend, modify, delete or remove this Security Whitepaper, at its sole and exclusive discretion, at any time. All information contained herein is provided "as-is", and GoodData disclaims all liability for itself and its affiliates, licensors and suppliers, with respect to the descriptions, statements and contents of this Security Whitepaper.