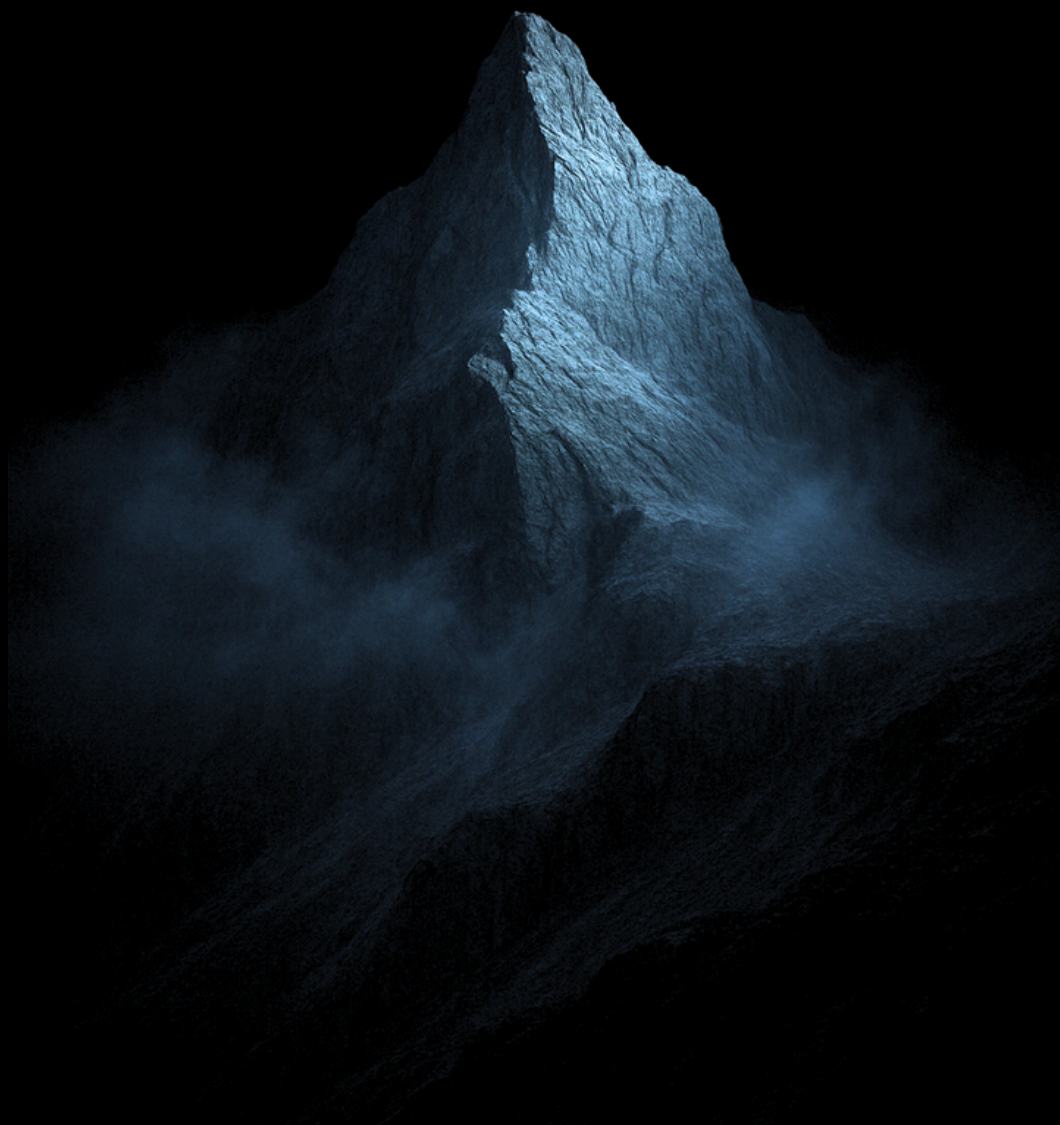
RuleWise



RuleWise INFORMATION SECURITY

RuleWise InfoSec

Detailed Response

[Version 2025-04-27]

Introduction

RuleWise is designed to deliver robust governance, risk, and compliance (GRC) solutions within a secure, high-performance environment.

RuleWise CORE - For organisations with user provisions under 100, RuleWise is deployed on OpenAI's "ChatGPT Team" environment, while for larger organisations with over 100 users, RuleWise is typically hosted on "ChatGPT Enterprise." In both instances, RuleWise functions as a Custom GPT, purpose-built to deliver specialised compliance and regulatory intelligence tailored to your operations.

RuleWise CLEUSO - Is a bespoke solution for each client with a proprietary user interface.

RuleWise CREW - Is a bespoke solution for each client with a proprietary user interface.

All RuleWise GRC modules are powered by proprietary intellectual property and exclusive frameworks, blueprints, and workflows guiding essential processes, methodologies, and strategies integral to each module. This approach ensures that clients benefit from a solution that is not only secure but specifically designed to meet the regulatory and compliance needs of today’s complex operational landscapes.

User Data Security and Control in the RuleWise Environment

A RuleWise user operates in a highly secure environment, interacting through a web browser and logging into a RuleWise Team account provisioned by OpenAI. All data transmitted during the session is protected by TLS 1.2 encryption, ensuring security in transit, and is stored on Microsoft Azure with AES-256 encryption at rest. Users have complete control over the data they upload for processing and can delete their data at any time—either within a specific chat or by deleting all user chats. No data is ever retained after deletion, ensuring permanent removal from the system. RuleWise enforces strict data confidentiality: no one, including RuleWise, OpenAI, Microsoft, or even other members of the user’s RuleWise Team, has sight of the user’s data, and it is not used for training large language models (LLMs).

1. Multi-Factor Authentication (MFA)

RuleWise users are requested to enable Multi-Factor Authentication (MFA) for their "RuleWise Team" account. This adds an extra layer of security. MFA in this context requires users to provide two forms of identification when logging in: something they know (their RuleWise User ID and RuleWise Password) and something they have (usually a one-time code from an authenticator app).

Key Points About MFA in RuleWise Team Accounts:

1. **Enabling MFA**:
    - Users can enable MFA by navigating to the "Settings" section after logging into their RuleWise Team account. Under the "Security" tab, they can select the option to enable MFA.
    - Once MFA is enabled, users will need to set up an authenticator app like Google Authenticator, Microsoft Authenticator, or Authy. This app will generate a time-based one-time password (TOTP) used alongside their regular login credentials.
2. **Recovery Options**:
    - During the setup process, users are provided with a recovery code, which should be stored securely. This code can be used if they lose access to their authenticator app.
3. **Impact on User Experience**:
    - Enabling MFA does not log users out of existing sessions, but it will require MFA verification for any new login attempts. This enhances security by making it significantly harder for unauthorised users to access the account.
4. **Customisability**:
    - MFA is optional and managed individually by each user. The organisation cannot enforce MFA across all accounts centrally in the RuleWise Team setup, which means each user needs to opt-in to use this feature.

This system of optional, user-managed MFA is a useful security measure but requires individual diligence to ensure all users are taking advantage of it.

2. Password Policy

The password policy for RuleWise Team accounts is determined by OpenAI, not by RuleWise or any other third party. When users create or change their passwords within the RuleWise Team, they must meet the security requirements set by OpenAI.

These requirements generally include:

- **Minimum Length**: OpenAI requires passwords to be at least twelve characters long. RuleWise supplies each new user with a password that is 32 characters long. The user can change this
- **Complexity**: It is advisable for passwords to include a mix of uppercase and lowercase letters, numbers, and special characters to enhance security.
- **Avoid Common Passwords**: Users are encouraged to avoid using easily guessable passwords, such as "password123" or common words and sequences.
- **Unique Passwords**: Users should use unique passwords that are not reused across different platforms to prevent security risks if one platform is compromised.
- **RuleWise Recommendation**: We recommend using a random password generator, such as the one provided by Avast. We suggest generating passwords with a minimum length of 32 characters, incorporating a mix of upper and lower case letters, numbers, and symbols (ABC, abc, 123, #$&).

These practices align with standard cybersecurity protocols to ensure the security of user accounts. OpenAI may update these requirements periodically to enhance security further.

If a client’s requirements specify additional criteria, such as mandatory periodic password changes or more stringent complexity rules, these would need to be managed at the user or organisational level, as OpenAI's platform itself enforces its default password policy.

https://www.avast.com/random-password-generator

3. Role-Based Access Control (RBAC)

RuleWise utilises Role-Based Access Control (RBAC) to enforce the segregation of duties. In a "RuleWise Team" account, users can be assigned one of three roles: Owner, Admin, or Member. Each role has distinct permissions and responsibilities:

1. **Owner**:
    - **Highest level of control**: The Owner has the most extensive permissions, including the ability to manage all aspects of the workspace.
    - **Invite and manage Admins/Owners**: Only the Owner can invite or promote users to Admin or Owner roles, and modify these roles.
    - **Billing and settings access**: The Owner can view and manage billing information, and toggle features within the workspace's settings.
    - **Manage all users**: The Owner can remove users, cancel invitations, and has the authority to change any user's role within the workspace.
2. **Admin**:
    - **User management**: Admins can invite new Members and remove users from the workspace. However, they cannot invite or promote other users to Admin or Owner roles.
    - **Limited settings access**: Admins can view and manage certain settings within the workspace but do not have access to billing or the highest-level settings reserved for the Owner.
3. **Member**:
    - **Basic access**: Members have the ability to use the core chat functionality and can see other users in the workspace.
    - **Invite Members**: Members can invite new users to the workspace, but they cannot modify roles or remove users.
    - **No administrative privileges**: Members do not have access to workspace settings, billing, or user management beyond inviting new Members.

These roles help in structuring the team’s use of RuleWise, ensuring that administrative tasks are handled by those with the appropriate permissions while allowing general team members to focus on using the service.

RuleWise, despite being the Owner of the account, never has access to any user data. This access is used solely for managing the Team, adding new users, for configuring the specific RuleWise SaaS solution, or for updating the RuleWise core.

- The RuleWise team is always called “RuleWise.Client”, for example “RuleWise.ABC”
- RuleWise Support is the “Owner” of the team.
- Client users are “Members”.

4. Session TimeOut

The session timeout settings for OpenAI accounts, including those managed through a RuleWise Team, generally follow a standard approach where users are automatically logged out after a period of inactivity. Specifically, OpenAI has configured RuleWise Teams so that users are logged out if they are inactive for a certain amount of time to help protect their security. However, recent updates have relaxed the session management somewhat, allowing users to stay logged in longer without being forced to re-authenticate as frequently as before. For instance, users will no longer be logged out every two weeks, which was a previous practice.

While the exact timeout period can vary depending on the specific implementation and configuration by the administrators, typically, these settings are aimed at balancing security and user convenience.

RuleWise has no direct control over any RuleWise Team session timeout.

5. Data Handling

Here is a comprehensive understanding of the data handling and security practices within the RuleWise Team environment:

1. **Data Handling and Visibility**:
    - **Client-Provided Data**: Data is only ever uploaded by the client user during an interaction or chat session. This data is securely transmitted to the RuleWise Team environment and is never visible to any member of RuleWise Ltd., including the RuleWise Client Team owner account.
    - **Confidentiality**: All client data is strictly confidential and is never shared with, or used by, OpenAI or Microsoft Azure for any purpose, including training their LLMs. This ensures that client data remains fully private and is not utilised outside the specific interaction it was intended for.
2. **Data Availability and Sharing**:
    - **Internal Data Sharing**: Within the RuleWise Client Team, data can be shared by "freezing" a chat, similar to taking a screenshot. This allows other team members, if invited by a user, to see the prompts and responses, but any uploaded files or data themselves remain inaccessible.
    - **Data Deletion**: Uploaded data is deleted whenever a chat is deleted. Furthermore, all data related to a specific user or the entire team can be instantly deleted upon request, ensuring that no remnants of the data are retained. To delete a user's chats, the user must go to Settings, General, Delete All. To delete all data for all team members, the client must instruct the RuleWise Team Owner to do so.
    - For users requiring access to documents stored in cloud environments, RuleWise offers optional integration with Google Drive and Microsoft OneDrive (including SharePoint). This integration enables users to select files directly from these storage platforms for use within the RuleWise environment. However, the integration is limited to file selection only and does not support saving or storing data back to these external platforms, thereby ensuring that document management and storage remain within the client's existing security boundaries.
3. **Data Segregation and Security**:
    - **Physical and Logical Segregation**: While the infrastructure is shared across multiple clients within Microsoft Azure's global data centres, data is logically segregated to ensure integrity and confidentiality. Azure's security measures, including encryption and compliance with certifications like ISO 27001 and SOC II, reinforce these protections.

- **Environment Segregation**: Client data is not used in staging environments. It is confined strictly to the production environment, ensuring that it is not exposed to unnecessary risks.

These practices collectively ensure that RuleWise maintains a high standard of data security, privacy, and confidentiality, aligning with industry best practices and client expectations.

6. Key Management

RuleWise Key Management and Encryption Policy

1. **Purpose and Use of Encryption Keys**: RuleWise Teams do not directly use or manage encryption keys for encrypting user data. The encryption of user data in transit is handled by the user's browser through the TLS 1.2 protocol. This ensures that data is securely transmitted between the user's device and the RuleWise Team servers. Once the data reaches the servers, it is stored on Microsoft Azure, where it is encrypted at rest using the AES-256 encryption standard. The management of the encryption keys used for data at rest is handled by Microsoft Azure, which follows stringent security practices to protect these keys.

2. **Encryption in Transit**: User data is protected during transmission using TLS 1.2, which ensures that the data cannot be intercepted or tampered with during its journey between the user's browser and the servers used by the RuleWise Team. This level of encryption is standard for securing communications on the internet and is managed by the user's browser and the server-side infrastructure.

3. **Encryption at Rest**: Once user data is stored, it is protected using AES-256 encryption, a robust encryption standard that is widely recognised for its security. The encryption and key management for data at rest are handled by Microsoft Azure, which is responsible for securely storing the encryption keys in its infrastructure.

4. **Key Management**: Since RuleWise does not manage the encryption keys directly, there is no internal key management lifecycle or access control policy within RuleWise related to these keys. The security and management of the encryption keys used for data at rest are fully handled by Microsoft Azure under their security protocols and standards.

This explanation underscores that RuleWise relies on proven, industry-standard security practices provided by the user's browser and Microsoft Azure to ensure the secure transmission and storage of user data, without directly handling or managing the encryption keys themselves.

7. Architecture

This is a generalised representation. RuleWise uses a service provided by OpenAI. There are many architectural variables in the OpenAI and Microsoft Azure environment, and RuleWise, as a client of OpenAI, has no say over the fine detail.

For creating a technical architecture diagram that demonstrates the connections of the RuleWise solution with all its components, including databases and API connections, here is an overview of the necessary components and their interactions:

1. **Core Components:**
    - **Azure OpenAI Service:** This is the central component where the RuleWise solution interfaces with the OpenAI models hosted on Microsoft Azure. The service processes inputs (prompts) from users and returns generated responses. The service may include API connections that allow RuleWise to send and receive data between the application and the OpenAI service.
    - **API Gateway:** An optional component that acts as a reverse proxy to manage traffic between the RuleWise application and the Azure OpenAI service. The gateway can handle tasks such as federated authentication, rate limiting, and routing requests to the appropriate model instances, ensuring that requests are handled efficiently and securely.
    - **Azure App Service:** This service hosts the application logic and the chat UI that interacts with users. It is connected to the API Gateway and the Azure OpenAI service to process user inputs and display outputs.
2. **Database Connections:**
    - **Azure Storage Solutions (Blob Storage, Data Lake Gen2):** These are used to store data that may be referenced by the OpenAI models, such as training data or configuration files. Connections to these data stores are managed securely, with the data either referenced directly or accessed via API calls.
    - **Key Vault:** Although RuleWise does not directly manage keys, Azure Key Vault is used by the underlying infrastructure to store secrets securely. This includes API keys and other sensitive information needed for connecting to various services.
3. **Network Configuration:**
    - **Virtual Networks (VNet):** The architecture includes separate subnets for different purposes, such as handling API requests, managing private endpoints, and controlling traffic to and from Azure services. Network security groups (NSGs) are applied to manage traffic flow and ensure that only authorised connections are allowed.

- **Private Endpoints:** These are used to securely connect to Azure services such as Storage, Key Vault, and OpenAI. This ensures that data does not traverse the public internet, reducing the risk of exposure.

4. **Security Measures:**
    - **Role-Based Access Control (RBAC):** RBAC is implemented to control access to resources based on user roles, ensuring that only authorised users can interact with sensitive components like the Azure OpenAI service or storage accounts.
    - **Content Filtering and Abuse Monitoring:** These features are integrated within the Azure OpenAI service to prevent misuse and ensure that all content generated complies with organisational policies and regulations.

This architecture ensures a secure, compliant, and efficient environment where the RuleWise solution can operate effectively while leveraging the capabilities of Azure and OpenAI.

8. Data Flow

As RuleWise, it is important to clarify that while our platform operates on the robust infrastructure provided by OpenAI and hosted on Microsoft Azure, we do not directly manage or control certain aspects of the underlying technology. Specifically:

1. **Azure Key Vault Access:**
    - RuleWise, as a client of OpenAI, does not have direct access to Azure Key Vault. This means we do not manage encryption keys at the Azure level. Instead, data encryption and key management are handled by OpenAI as part of their infrastructure responsibilities.
2. **Data Residency Choices:**
    - Microsoft Azure, as the hosting provider, does not offer RuleWise the ability to choose specific data residency locations within their global data centres. Our only options relate to data processing agreements (DPAs) tailored to the jurisdictional needs of our clients. Specifically:
        - **UK/USA Requirements:** When processing data under UK or USA regulations, we enter into a DPA with OpenAI LLC.
        - **EU Requirements:** For clients requiring GDPR compliance within the EU, we engage in a DPA with OpenAI Ireland, which ensures that data processing aligns with EU regulations.

This setup ensures that RuleWise can deliver a secure and compliant service, tailored to the legal requirements of our clients, without directly handling certain infrastructural components such as encryption key management or data residency selection.

9. Backup and Disaster Recovery

Backup Period and Content:

RuleWise Ltd does not handle or store customer data directly. All data related to customer accounts, including backups, is managed by Microsoft Azure and OpenAI. Therefore, RuleWise does not perform any direct backups or manage backup retention periods for customer data.

Backup Retention:

As RuleWise does not manage customer data directly, the responsibility for data backups, including retention periods, lies with Microsoft Azure and OpenAI. You may need to refer to the data retention policies provided by Microsoft Azure and OpenAI for specific details regarding how long data is kept.

Backup Storage and Access:

Backups of any data associated with RuleWise services are managed and stored by Microsoft Azure and OpenAI. The storage locations and access controls for these backups are governed by the policies and practices of these providers. RuleWise Ltd does not have direct access to customer backups or storage locations.

Disaster Recovery Plan:

RuleWise relies on the robust disaster recovery and fault tolerance mechanisms provided by Microsoft Azure and OpenAI. RuleWise itself does not maintain a separate Disaster Recovery (DR) plan specific to customer data. However, Microsoft Azure and OpenAI implement extensive disaster recovery and redundancy measures to ensure data availability and resilience.

10. Logging

RuleWise Team Accounts

Regarding the logging and auditing features of a "RuleWise Team" standard account, here are the accurate details:

1. **Types of Logs**:
    - OpenAI does maintain certain logs, such as access and activity logs, which record system access, usage patterns, and errors. However, these logs are primarily used for maintaining and improving the system's stability and security.

2. **Accessibility of Logs**:
    - For "RuleWise Team" accounts, the logs are not accessible to the team owner, administrators, or any other members. This includes chat logs and other detailed activity records. The privacy of individual user conversations is strictly maintained, meaning that even administrators or team owners cannot view or audit individual user chats. This privacy policy is part of OpenAI's commitment to safeguarding user data and ensuring that conversations remain private.

3. **Log Retention**:
    - While specific details about the retention period of logs are managed by OpenAI, these logs are typically kept for a limited duration to support system operations and are not accessible externally. Any data retained follows OpenAI's privacy and data management policies, which are designed to comply with relevant regulations.

11. Application Patching

RuleWise Application Patching Procedure

1. **Customised Client Solutions:** RuleWise creates a bespoke version of its solution for each client, ensuring that all interactions or chats generated by a specific version will always utilise that version's logic and features.

2. **Patch and Update Process:**

    - **Patching an Existing Version:** When a minor update or patch is required, the existing version (e.g., version 1.10) is cloned. The clone undergoes the patching process where necessary fixes or enhancements are applied. This patched version is rigorously tested in a controlled environment. Upon successful testing, the patched version is released, replacing the previous version. For example, version 1.10 would become 1.11. From this point, version 1.11 would replace 1.10 entirely—no new chats can be initiated using version 1.10, although ongoing chats will continue to operate under the logic of version 1.10. All new chats will use the logic within version 1.11.

    - **Creating a New Major Version:** When a new major version is developed (e.g., version 2.00 or 3.00), it is created from scratch and provisioned as a completely new version. This new version is released alongside the existing version. For example, if the current version is 1.11, and a new major version 2.00 is released, both versions would be available simultaneously for at least a month. Users have the option to choose which version they wish to use, allowing them to transition at their own pace.

3. **Notification and Rollout:**

    - **User Notification:** When a new production version, either a minor update or a major release, is available, users are informed through a clear message displayed at the bottom of their screen. This ensures users are aware of updates without interrupting their workflow.

    - **Parallel Version Support:** In the case of a major version release, the original and new versions are available side by side for a minimum of one month. This flexibility ensures that users can complete ongoing tasks without being forced into an immediate update.

4. **Communication and Issue Reporting:**

    - **Reporting Issues:** Clients are encouraged to report any issues through our dedicated communication channels, including our fully ticketed Help Desk (support@rulewise.net), or directly via our designated Client Relations Officer (Mort Mirghavameddin, mort@rulewise.net), or Chief Product Officer (Simon Kirkpatrick, simon@rulewise.net). This ensures all concerns are logged, tracked, and addressed promptly.

- **Patch Approval Process:** Upon receiving an issue report, our team assesses the severity and impact, categorising the issue based on predefined severity levels. This categorisation guides the prioritisation of the patching process, with critical security vulnerabilities being expedited.

5. **Remediation Timeline:**
    - **Categorisation and Timeline:** RuleWise employs a categorisation system with specific remediation timelines:
        - **Critical Issues:** Addressed and remediated within 24 to 48 hours.
        - **High-Priority Issues:** Resolved within 3 to 5 business days.
        - **Medium and Low-Priority Issues:** Addressed within 7 to 14 business days, depending on complexity and client impact.
    - **Client Communication:** Clients are kept informed throughout the process, with updates provided at key stages, including issue identification, patch application, and deployment of the new version.
6. **Continuous Improvement:**
    - **Post-Patch Review:** After deploying a patch, a post-implementation review is conducted to assess the effectiveness of the remediation. Feedback from this review is used to continuously refine our patching and update procedures.
7. **Compliance and Documentation:**
    - **Audit Trails:** Detailed logs of all patching activities are maintained to ensure transparency and compliance with industry standards.

Conclusion: RuleWise is committed to delivering secure, reliable, and client-centric solutions. Our patching procedure is designed to ensure that issues are resolved promptly while maintaining the highest standards of security and functionality. By keeping clients informed and involved throughout the process, we ensure that our solutions continue to meet their evolving needs.

12. Penetration Testing

RuleWise itself does not conduct independent penetration testing of its platform. The RuleWise solution is built upon the OpenAI infrastructure, and as such, the responsibility for penetration testing and other security assessments lies with OpenAI and Microsoft Azure, which hosts the underlying infrastructure.

Both OpenAI and Microsoft Azure undertake extensive and regular penetration testing to ensure the security and integrity of their services. These tests are carried out by dedicated security teams using industry-standard practices to identify and address any potential vulnerabilities.

Regarding the availability of penetration testing reports, these documents are highly sensitive and confidential. While RuleWise does not directly hold or distribute these reports, OpenAI provides a mechanism through which interested and vetted parties can request access to such reports. You may register on the OpenAI Trust website, where, after a review of your credentials, OpenAI may grant you access to the most recent penetration testing reports and other security documentation.

This process ensures that all parties involved in utilising the RuleWise solution are operating within a secure and robust environment, protected by the stringent security measures employed by OpenAI and Microsoft Azure.

https://trust.openai.com/

13. Certifications

RuleWise does not maintain its own internal systems for coding, testing, addressing issues, or training personnel. Instead, all of our operational activities are carried out using external platforms, ensuring a high level of security through the established measures of our service providers.

Our SaaS solution is built directly on the infrastructure provided by OpenAI. OpenAI is responsible for the security, coding, testing, and issue resolution related to the RuleWise platform. OpenAI's infrastructure is hosted on Microsoft Azure, which is certified against numerous security standards, including ISO/IEC 27001, and is regularly assessed through external audits, including SOC 2 Type II reports. OpenAI's ChatGPT Team and Enterprise environments, certified to SOC 2 Type II standards and trusted by leading global organisations—including Morgan Stanley, PwC, Square, Zendesk, and the University of Oxford—serve as the foundation for RuleWise's secure and compliant solutions.

Additionally, RuleWise's working environment is entirely cloud-based and facilitated through Google Workspace. Google Workspace is also certified against several security standards, including ISO/IEC 27001, SOC 2, and SOC 3, and adheres to stringent security practices.

Therefore, the certifications that are relevant to RuleWise come through our service providers—OpenAI, Microsoft Azure, and Google Workspace. RuleWise itself does not operate or manage internal systems, and as such, does not possess independent certifications like ISO or SOC reports. The robust security measures and certifications provided by our external platforms ensure that our operations meet high standards of security and compliance.

14. SOC 2 Compliance

Overview of SOC 2 Compliance
RuleWise operates within OpenAI's SOC 2 Type II certified environments, providing assurance to clients that our service meets high standards in data security, availability, processing integrity, confidentiality, and privacy. This certification signifies adherence to the American Institute of Certified Public Accountants (AICPA) Trust Services Criteria, which include rigorous controls and independent verification of secure data practices.

Deployment Configurations and Security
RuleWise is deployed on either OpenAI's ChatGPT Team or ChatGPT Enterprise environments, depending on user requirements:

- **ChatGPT Team**: For organisations with fewer than 100 users.
- **ChatGPT Enterprise**: For larger organisations with over 100 users.

Both configurations leverage Custom GPT functionality to provide bespoke governance, risk, and compliance (GRC) insights, driven by RuleWise's proprietary methodologies and blueprints, ensuring that users receive tailored compliance intelligence.

Key Security Measures

1. **Data Hosting and Encryption**: All RuleWise data is hosted on Microsoft Azure. Azure provides industry-leading security measures, including:
    - **AES-256 encryption** for data at rest.
    - **TLS encryption** for data in transit, securing communication pathways.

2. **Privacy Protections and Data Ownership**: OpenAI's data handling policy ensures that:
    - Users maintain full ownership and control over their data.
    - Data used within ChatGPT Team or Enterprise environments is neither stored persistently nor utilised for AI model training, thus safeguarding confidentiality.

3. **Independent Audits and Trust Assurance**: OpenAI's SOC 2 Type II report demonstrates commitment to maintaining robust security protocols. Regular, independent audits validate the effectiveness of these controls, supported by additional certifications, including compliance with global data privacy regulations such as GDPR and CCPA.

Client Benefits
This SOC 2 Type II compliance enables RuleWise clients to confidently rely on our solutions, knowing that OpenAI's trusted security practices meet stringent regulatory and operational standards. Key clients of OpenAI's secure environments include major organisations such as PwC, Square, and the University of Oxford, evidencing the high trust in these systems.

With RuleWise's commitment to partnering with leading-edge SOC 2-certified infrastructure, our clients benefit from a robust, secure, and regulatory-compliant environment for all their GRC needs.

15. External Content

Regarding third-party components in RuleWise's solution, the concise response is as follows:

External Content and Third-Party Use:

- **Third-Party Utilisation**: RuleWise does not engage with any third parties directly, other than OpenAI. Our contractual and operational relationship is exclusively with OpenAI, who in turn manages all interactions with Microsoft Azure. This means that any technical vulnerabilities related to the infrastructure are managed by OpenAI, as they oversee the integration with Microsoft Azure.

RuleWise's Proprietary Enhancements:

- **Intellectual Property**: RuleWise adds significant intellectual property to the OpenAI Large Language Model (LLM). This includes advanced prompt engineering, a proprietary playbook that incorporates RuleWise Taxonomy, and bespoke implementations of qualitative and quantitative data analysis, and implementations of Bayesian theory.

- **Jurisdiction-Specific Content**: In addition to these technical enhancements, RuleWise integrates jurisdiction-specific governance, risk management, and compliance (GRC) information such as laws, regulations, rules, and guidance notes into the solution.

Responsibility for Remediation:

- **Responsibility**: Since OpenAI handles the infrastructure, including their relationship with Microsoft Azure, they are responsible for remediating any technical vulnerabilities in these components. RuleWise focuses on ensuring the integrity, confidentiality, and availability of the additional layers of proprietary enhancements and content it provides on top of the OpenAI infrastructure.

This summary outlines that RuleWise's involvement with third-party components is limited to its partnership with OpenAI, who manages all technical infrastructure matters, including vulnerability remediation.

16. Data Exporting

The RuleWise Team solution supports exporting data to a variety of file formats. Here is an list of the major file formats that can be exported directly from within a RuleWise Team:

1. **PDF**: Portable Document Format, ideal for creating read-only documents that preserve formatting.
2. **DOCX**: Microsoft Word format, allowing for further text editing in word processors.
3. **XLSX**: Microsoft Excel format, used for spreadsheets and data analysis.
4. **PPTX**: Microsoft PowerPoint format, suitable for creating presentations.
5. **CSV**: Comma-Separated Values format, often used for data exchange and import/export between different systems.
6. **TXT**: Plain text format, a simple file type for unformatted text.
7. **RTF**: Rich Text Format, which supports text formatting while remaining more universally accessible than DOCX.
8. **HTML**: Hypertext Markup Language, useful for web content and emails.
9. **Markdown (MD)**: A lightweight markup language with plain text formatting syntax, commonly used for creating formatted text for the web.
10. **PNG**: Portable Network Graphics, allows exporting the conversation as an image file.
11. **Markdown (MD)**: Often used for text with simple formatting, useful for web or documentation purposes.

These formats allow for flexible handling of the generated content, catering to a wide range of professional needs, from simple text files to fully formatted presentations and web content.