What are Legal Ready key security measures?

Privacy and Security · https://disclosureready.us.legalready.ai/knowledge/what-are-legal-ready-key-security-measures/

This article explains the key security measures that Legal Ready has implemented for its platform to deliver eBrief Ready and Disclosure Ready services.

Information to the Disclosure Ready User

1. Legal Ready is ISO 27001 accredited, which provides a framework organisations to manage the security of their data assets.
2. Legal Ready enforces the mandatory use of two-factor authentication (2FA) for all Disclosure Ready accounts. 2FA verifies that the person trying to gain access to the account is who they say they are – in addition to the login username and password. Even if someone else obtains your password, the two-factor authentication requires an additional step of SMS code or authenticator validation.
3. All client documents are held securely on Amazon AWS. The servers are located in Sydney (for those using the platform within Australia) and London (for those using the platform within the UK), so your data stays inside your sovereignty.
4. Disclosure Ready relies on third-party services, such as Amazon Web Services, Elastic Cloud, Elastic Email and others. All data from these services is encrypted in transit and, where possible, encrypted at rest.
5. In line with industry best practice, user account passwords are encrypted. The unencrypted password is not accessible to any member of the Legal Ready team.
6. The software libraries used by the Disclosure Ready platform are routinely checked for vulnerabilities as part of the application development and deployment process. A deployment of the platform is not able to proceed until any identified vulnerabilities have been rectified.
7. All Legal Ready team members sign confidentiality agreements, and their access to the client data is limited to what is required for development or troubleshooting purposes only.

8. Legal Ready has automated systems in place for error detection and reporting, as well as a robust system for the automated backup of critical user-provided data agreements.

Information to the Disclosure Ready Firm IT Department

Legal Ready has implemented several key security features to ensure the protection of information and systems, such as:

Access Control Policy and Procedure

1. Principle of Least Privilege
    - Accounts are granted the minimum access privileges necessary to perform the business processes. This includes user rights and resource permissions such as CPU limits, memory, network, and file system permissions.

2. Segregation of Duties
    - Duties and responsibilities are segregated to reduce human error and misuse of information processing assets. Where segregation is not possible, alternative controls like monitoring and independent audits are implemented.

3. Approval and Provisioning of Access Rights
    - Access to applications, databases, or documents is approved and provisioned by designated roles, ensuring that the role provisioning access is not the same as the one authorising it.

4. Review and Deprovisioning of Access
    - Regular reviews of user access rights are conducted, and access is deprovisioned as necessary to maintain security.

5. 2-Factor Authentication
    - Mandatory requirement to enhance security.

Information Security Policy

1. Commitment to Information Security
    - Legal Ready is committed to optimising information security performance in line with their risk appetite and ensuring that all staff and contractors understand their security obligations.

2. Industry Standards Compliance
    - Legal Ready adheres to industry standards for data integrity and incorporates information security into every phase of operations.
3. Information Security Management System (ISMS)
    - Implementation, maintenance, and continual improvement of ISMS, with compliance and certification to ISO 27001:2022.
4. Security Objectives
    - Confidentiality: Ensuring information is not disclosed to unauthorised individuals.
    - Integrity: Maintaining the consistency, accuracy, and trustworthiness of information.
    - Availability: Ensuring information is accessible and usable upon demand by authorised parties.
5. Staff Training and Development
    - Commitment to recruiting and skilling staff to deliver information security outcomes.

These features collectively ensure that Legal Ready maintains a robust security posture, protecting both the platform and clients' information.

For more details, please refer to:

- eBrief Ready End User Agreement
- Disclosure Ready End User Agreement