Rubiklab
AI powered research

Rubifilab Ltd. Data Security and Standard Data Recovery Protocol

Effective: 1st of April 2022

Rubiklab Ltd.

1A Falmer Court, London Road, Uckfield, TN22 1HN

This policy was last updated in January 2026.

1. Security measures and best practices

Rubiklab Ltd. implements a comprehensive information security framework designed to protect the confidentiality, integrity, and availability of its systems, applications, and data assets. Security controls are applied across the full lifecycle of system design, development, deployment, and operation. These controls include network protection mechanisms, secure development practices, access management controls, encryption safeguards, and continuous monitoring processes. Rubiklab regularly reviews and updates its security measures to align with evolving threats, regulatory requirements, and industry best practices.

Web Application Security:

Rubiklab implements multiple layers of security controls to protect its web applications and APIs from unauthorised access and emerging threats. Network and application access is protected through the use of firewalls and strict access control mechanisms, ensuring that only authorised systems and personnel are able to interact with internal services and APIs. Secure development practices follow recognised industry standards, including the OWASP Top 10 guidelines, to mitigate common application security risks. Data processed within the platform is protected through encryption both in transit and at rest using industry-standard cryptographic protocols. In addition, Rubiklab conducts regular security audits and engages independent security specialists to perform periodic security assessments and penetration testing of its infrastructure and applications. These activities are designed to identify potential vulnerabilities, validate the effectiveness of implemented controls, and maintain a strong overall security posture. Findings from these assessments are reviewed by the engineering and security teams and addressed through established vulnerability management and remediation processes.

Database security:

Database infrastructure is protected through a combination of encryption, access controls, monitoring, and ongoing security oversight. Databases are secured using industry-standard encryption mechanisms both at rest and in transit, and access is strictly restricted to authorised personnel through controlled authentication and role-based access permissions. Continuous monitoring and intrusion detection mechanisms are in place to identify and alert the technical team to potential threats or anomalous activity. Rubiklab conducts regular security reviews and audits of its database environment to identify and remediate vulnerabilities in a timely manner. Development and maintenance of database systems follow recognised industry security and quality standards, ensuring that data storage and processing environments remain secure, resilient, and aligned with established best practices.

2. Continuous monitoring and observations:

Rubiklab maintains continuous security monitoring across its infrastructure using a combination of automated monitoring tools and vulnerability intelligence services. These tools assist in identifying potential exposure of assets, misconfigurations, or emerging vulnerabilities. Security monitoring outputs are reviewed by the technical team and integrated into the organisation's vulnerability management and remediation processes.

The aforementioned security measures and detailed technical specifications represent Rubiklab Ltd.'s commitment to maintaining robust data security and ensuring the protection of sensitive information across its infrastructure.

Rubiklab operates its production infrastructure within a managed cloud environment. Critical data services are protected through controlled network architecture, secure configuration practices, and managed database services. Backup procedures are implemented to ensure that operational data can be restored in the event of system failure, operational errors, or security incidents. These procedures form part of the organisation's broader business continuity and disaster recovery framework.

Employee training and awareness

Rubiklab Ltd., as a proactive member of the DataExpert group, is committed to a culture of continuous learning and awareness in the realm of data security and incident response. Our internal ongoing training program ensures that all employees are regularly updated on the latest data security practices and incident response strategies. This program includes not only in-house training sessions but also external audits that provide an independent evaluation of our practices and procedures. These training initiatives are designed to empower our workforce with the knowledge and skills necessary to identify, prevent, and respond to potential security threats effectively. By maintaining a high standard of awareness and preparedness, we safeguard our information assets and reinforce our resilience against data breaches and cyber threats."

Data backup and retention

Rubiklab maintains a structured data backup and retention strategy designed to minimise the risk of data loss and support rapid recovery of services. Automated backups are performed regularly and stored securely within the organisation's cloud infrastructure. Backup processes are designed to support defined recovery objectives and are periodically reviewed to ensure they remain aligned with operational requirements and evolving infrastructure architecture.

Incident response and recovery

Rubiklab maintains a documented Incident Response and Recovery Plan designed to ensure timely detection, containment, and remediation of security incidents. In the event of data loss, system disruption, or suspected security breach, the response team assesses the incident, determines its scope and impact, and initiates appropriate remediation and recovery procedures. Restoration of services relies on validated backup systems and established recovery procedures to minimise operational disruption.

Personnel involved must be proficient in the procedures governing the initiation of restoration from these backups, and a detailed inventory of backup archives must be diligently upheld. Periodic drills are implemented to validate the efficacy of our recovery plan and ensure its alignment with evolving environmental conditions.

We integrate industry-leading standards into our disaster recovery planning. This approach encompasses not only technological disruptions but also natural disasters, major cyber-attacks, and other catastrophic events that could impact our operations. By aligning with best practices and benchmarks in the field, we ensure that our disaster recovery plan is comprehensive, resilient, and adaptable to a range of potential adversities. This plan is regularly reviewed and updated to

reflect emerging threats and changes in our operational environment, ensuring that we are always prepared to maintain business continuity under any circumstances.

Continuous oversight and enhancement

The process of data recovery requires constant attention and improvement. To ensure the integrity of our data, we have established a continuous monitoring system. This system is instrumental in identifying any irregularities, potential issues, or changes in the database environment that could impact data integrity. In addition, we have integrated automated tools and alerts into our operations, enhancing our ability to swiftly detect and respond to potential data loss scenarios. These combined measures actively reinforce the resilience of our data infrastructure.

Testing and validation of recovery procedures

We place a strong emphasis on the rigorous testing and validation of our data recovery procedures. We understand that the technological landscape is ever-evolving, and our response strategies must evolve accordingly. To this end, any new technological integration or update within our infrastructure undergoes thorough testing to assess its impact on our data recovery capabilities. These checks are comprehensive, covering various scenarios to ensure the robustness and effectiveness of our recovery plans.

Third-party vendor management

We understand the importance of extending our high data security standards to all third-party vendors we engage with. As such, each vendor undergoes a rigorous assessment process to ensure they meet our exacting standards for data protection and security. This includes evaluating their security practices, compliance with relevant regulations, and their ability to respond effectively to potential data breaches. Regular reviews and audits of our vendors are conducted to ensure ongoing compliance and to address any emerging risks. This vigilant approach to vendor management is a critical component of our overall data security strategy, ensuring that every aspect of our data handling, from internal processes to external partnerships, is secure and reliable."

Conclusion

Our formalized Data Recovery Protocol stands as an essential pillar for safeguarding the invaluable data assets of our organization. By prioritizing the development of a comprehensive backup and retention strategy, solidifying a robust incident response and recovery framework, and perpetually refining our recovery procedures, we fortify the foundation of our data infrastructure and uphold business continuity in the face of unforeseen adversities.

Please contact us

Please email support@rubiklab.ai with any questions, concerns, or comments regarding this protocol.