Rubiklab 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 November 2024.

1. Security measures and best practices

Rubiklab Ltd. prioritizes the security of both its web applications and databases by adhering to industry best practices:

Web Application Security:

- Firewalls and Access Control: Multiple firewalls and access control systems are in place to safeguard against unauthorized access. Access to APIs is strictly controlled and monitored.

- OWASP Top 10: Rubiklab follows the OWASP Top 10 guidelines to mitigate common security risks in web applications.

- Collaboration with Security Experts: Independent security experts collaborate to identify and track dependencies and potential security risks.

- Regular Security Audits: The company conducts routine security audits to proactively identify and address vulnerabilities.

- Encryption: Data in the web application is encrypted using industry-standard algorithms both at rest and in transit.

Database security:

- Encryption and Access Limitation: Databases are secured using industry-standard encryption algorithms both at rest and in transit. Access is strictly limited to authorized personnel only.

- Intrusion Detection Systems: Systems are in place to detect and alert the team about potential threats or breaches.

- Security Audits: Regular security audits are conducted to identify and resolve vulnerabilities promptly.

- Adherence to ISO Standards: Development and maintenance adhere to ISO standards for quality and security.

2. Continuous monitoring and observations:

Defender EASM Service: Completed an environment analysis with a reassuring result of 0 high-severity observations. Continuous monitoring services are in place to maintain a secure environment.

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.

In the context of our Google Cloud Platform (GCP) infrastructure, where we employ a meticulously managed demilitarized MySQL database instance featuring a 7-day data retention policy and a comprehensive backup system, it is paramount to establish a robust and formalized Data Recovery Protocol. This protocol serves as a foundational element in our data management strategy, ensuring the organization's ability to swiftly and effectively restore crucial data in the face of data loss, system disruptions, or inadvertent human errors.

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

At the heart of our Data Recovery Protocol lies an unwavering commitment to a comprehensive data backup and retention strategy. Our GCP-managed MySQL database instance is configured to perform automated daily backups, retaining data for a specified 7-day window. These backups constitute the primary line of defense against data loss incidents. Should the need arise to adhere to more stringent recovery point objectives (RPOs), we recommend the implementation of additional automated backup procedures. It is imperative to thoroughly document the protocols governing the initiation, validation, and access of these backups, enabling authorized personnel to expeditiously trigger the recovery process when the situation demands.

Incident response and recovery

In the unfortunate event of data loss or system malfunction, our operational readiness is underpinned by a meticulously defined Incident Response and Recovery Plan. A dedicated team is entrusted with the responsibility of overseeing data recovery efforts, encompassing the identification of the root cause of the incident and a comprehensive evaluation of the extent of data loss. Our primary recourse for data recovery is the judicious utilization of meticulously maintained backups.

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.

This policy was last updated in November 2023.

Please contact us

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