Replenit SECURITY, PRIVACY, AND ARCHITECTURE DATASHEET

(effective as of December 2024; subject to change without notice)

Introduction

The goal of this document is to provide high-level information to our customers regarding Replenit's commitment to security and data protection.

Replenit's Corporate Trust Commitment

Replenit is committed to achieving and maintaining the trust of our customers. Our goal is to be as transparent as possible with our customers in offering state-of-the-art security and protections to meet and exceed expectations in today's modern computing world.

1. Policy Ownership

Replenit has a documented information security policy that all employees must read and acknowledge. This policy is reviewed and updated annually. Security policy development, maintenance, and issuance is the responsibility of the Replenit Security Team.

2. Replenit Infrastructure

Replenit uses Microsoft Azure for European hosting.

For Europe-hosted customers, Replenit hosts the Replenit Services with Microsoft Azure (Microsoft Deutschland GmbH", registered with the District Court of Munich under the commercial register number HRB 70438, with the European Unique Identifier (EUID) DED2601V.HRB70438, is a company incorporated and having its registered office at Walter-Gropius-Str. 5, 80807 München, Germany).

3. Third-Party Architecture

Replenit may use one or more third-party content delivery networks to provide the Replenit Services and to optimize content delivery via the Replenit Services. Content items to be served to subscribers or end-users, such as images or attachments uploaded to the Replenit Services, may be cached with such content delivery networks to expedite transmission. Information transmitted across a content delivery network may be accessed by that content delivery network solely to enable these functions.

4. Audits, Certifications, and Regulatory Compliance

Replenit enters into the EU Standard Contractual Clauses with its Customers that require it, self-certifies to the EU-US and Swiss-US Data Privacy Frameworks and the UK Extension to the EU-US Data Privacy Framework.

Security Controls

5. Organization Security

Replenit's CPO is responsible for the overall security of the Replenit Services, including oversight and

accountability. Replenit's contracts with third-party hosting providers such as Microsoft Azure include industry-standard information protection requirements.

6. Asset Classification and Logical Access Control

Replenit maintains an inventory of essential information assets such as servers, databases, and information. All Customer Data is classified as Confidential by Replenit.

Replenit adopts the principle of least privilege for all accounts running application or database services, as well as with its own staff. Replenit maintains separate development, staging (or sandbox), user acceptance testing, and production environments access to each environment and within each environment is strictly controlled.

Access to Replenit's servers is controlled via revocable SSH keys managed via configuration management and rotated at least annually. All access to Replenit's servers or Customer Data is logged and can only be accessed through Replenit's VPN, which uses multi-factor authentication. Database access is controlled via 32 and 64-character passwords with IP whitelisting. Replenit's HR onboarding and off-boarding processes handle provisioning and de-provisioning of accounts and access.

7. Personnel Security and Training

All employees at Replenit sign a non-disclosure agreement when their employment begins. In addition, Replenit conducts appropriate background screenings of its employees, in compliance with legal requirements, as part of its onboarding process. All employees are informed of, and agree to comply with, Replenit's security policies and practices as a part of their initial onboarding. All Replenit employees undergo annual security and privacy training.

System administrators, developers and other users with privileged access receive special and ongoing training.

8. Physical and Environmental Security

Access to Replenit facilities under shared offices is controlled by 24-hour security. Additionally, all Replenit offices are protected by locked access and are under 24-hour video surveillance. All Replenit employee workstations are encrypted and password protected, and all Replenit employee user accounts require two-factor authentication.

Data centers and servers are managed and controlled by our Cloud hosting provider, Microsoft, Replenit employees have no access to any of these data centers.

Details regarding the security practices and controls applicable to these facilities can be found at their websites:

Microsoft: https://azure.microsoft.com/en-us/overview/security/

9. Policies and Logging

The Replenit Services are operated in accordance with the following procedures to enhance security:

- Dashboard User passwords are never transmitted or stored in clear text
- Replenit uses industry-standard methods to determine password validity
- API key information for third-party services provided by the customer are encrypted for storage
- Replenit keeps audit logs for all access to production servers
- Server access is controlled via public key access, instead of passwords, and only permitted while on VPN that requires multi-factor authentication
- Logs are stored in a secure centralized host to prevent tampering
- Replenit application and ssh audit logs are stored for one year
- Passwords are not logged under any circumstances
- Access to Replenit mail and document services is only allowed on approved mobile devices that have automated security policies enforced, such as encryption, autolock and passwords
- All access to customer dashboard accounts by Replenit Employees must be done through an internal service that is accessible via a 3-factor VPN only
- As part of Replenit's Employee Information Security Policy, employees may not store any Customer Data on removable media

10. Intrusion Detection

Replenit leverages CrowdStrike, an Endpoint Detection & Response solution (EDR). This solution is designed to review and conduct signature, heuristic, and behavioral analysis, granting the ability to detect advanced threats to both on our cloud infrastructure and corporate network. Logs from this system are centrally collected for further analysis and threat detection.

Additionally, Replenit may analyze data collected by Dashboard Users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the Replenit Services function properly.

Replenit's APIs and Dashboard use strict role-based access controls and user permissioning. Unauthorized web requests and API calls are logged and automatically alert Replenit's engineering team.

11. Security Logs

All Replenit systems used in the provision of the Replenit Services, including firewalls, routers, network switches, and operating systems log information to their respective system log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis. Replenit has automated alerts and searches on these logs.

12. System Patching and Configuration Management

Replenit patches its servers and rebuilds its entire cloud infrastructure from configuration management systems on a regular basis, which ensures that the latest patches are applied and that we "reset" back to a known, clean state. Replenit's configuration management system regularly applies patches via Linux repositories. Replenit uses the Chef configuration management tool and Kubernetes to automate this entire process, and our entire infrastructure.

Replenit maintains multiple environments and tests changes in containerized development environments and in live staging environments before making changes to production environments.

13. Vulnerability Management

Replenit's infrastructure and applications are continuously scanned by a Vulnerability Management System provided by Microsoft Azure. Alerts are monitored by our Security Team and addressed at least monthly by the Replenit Vulnerability Management Team.

14. Third-Party Penetration Testing

Replenit undergoes a third-party penetration test of the Replenit Services on adhoc basis.

15. Monitoring

For technical monitoring, maintenance and support processes, Replenit uses a combination of tools to ensure that processes and servers are running properly, including but not limited to:

- Process monitoring
- CPU, disk, and memory monitoring
- Uptime monitoring
- Functional monitoring
- Database monitoring
- APM performance monitoring
- Error monitoring
- Office monitoring

16. Customer Access Control

The Replenit Services employ a variety of security controls. These include, but are not limited to:

- API IP Whitelisting - Defines the range of IP addresses from which a customer's Dashboard Users can access the Replenit API to prevent unauthorized third parties from accessing the Replenit Services.
- Single-sign on with a Google Account - Replenit customers can access the Replenit Services by means of a Google Account, which allows customers to configure such access to require two-factor authentication.
- Mobile Authenticator - Replenit customers can enable two factor authentication via Authy which allows a mobile authenticator to be required for access to the Replenit Dashboard.
- Customer-Configurable Roles and Permissions - Replenit customers have the option to manage their Dashboard Users through selective and granular permissioning.
- All requests on the Replenit Dashboard have cross-site request forgery (CSRF) protection. All web services use encrypted HTTPS for all traffic and disallow all HTTP traffic via HTTP Strict Transport Security ("HSTS").
- Replenit does not use cookies for session storage to avoid replay attacks. Sessions expire after a few hours of inactivity.

- Dashboard User passwords on the Replenit Dashboard must meet minimum password length requirements. At the customer's request, Replenit can add password complexity requirements, such as lowercase, uppercase, numeral, and special characters.
- Replenit's REST APIs are accessed with separate API keys, which can only be provisioned by Replenit Dashboard User accounts with administrative access. API keys are granted access to specific API endpoints when created.

17. Development and Maintenance

Replenit uses tools such as GitHub and Jenkins to effectively manage the development lifecycle. During testing, Replenit generates sandbox accounts and fake data for testing. Replenit does not use production data in sandbox accounts.

Application source control is accomplished through private GitHub repositories. Replenit has controls in place to ensure that all code must be approved before being merged to Replenit's main code branch; only the CTO and approved employees are granted access to promote code to production.

Replenit developers receive additional security training as part of their onboarding, and undergo regular and periodic security training during the term of their employment. Replenit maintains a list of core security principles for engineering and high-level guidelines on security topics for secure software development.

18. Malware Prevention

As a mitigating factor against malware, all Replenit servers run LTS editions of Operation Systems, as well as the endpoint detection and response (EDR) service, Crowdstrike.

Replenit adopts the principle of least privilege for all accounts running application or database services. Proper change management ensures that only authorized packages are installed via a package management system containing only trusted software, and that software is never installed manually.

All Replenit employee computers have virus scanners installed and updated definitions sent out from a central device management platform.

19. ***Information Security Incident Management*** Replenit maintains written and regularly-audited security incident management policies and procedures, including an Incident Response Plan to be enacted in the event of an incident.

Replenit has 24x7x365 on-call incident management staff.

20. Data Encryption

The Replenit Services use industry-accepted encryption practices to protect Customer Data and communications during transmissions between a customer's network and the Replenit Services, including 256-bit TLS Certificates and 4096-bit RSA public keys at a minimum.

Data shipped to Microsoft Azure is encrypted in transit and at-rest using AES-256 encryption via Microsoft's managed encryption key process.

Where use of the Replenit Services requires a customer to provide access to third party services (for example, AWS S3 credentials for data exports), Replenit performs additional encryption of that information.

21. Return and Deletion of Customer Data

The Replenit Services allow import, export, and deletion of Customer Data by authorized Dashboard Users at all times during the term of a customer's subscription. Following termination or expiration of the Replenit Services, Replenit shall securely overwrite or delete Customer Data within 60 days following any such termination in Replenit's production instance, and in accordance with the Agreement, applicable laws and the Documentation.

22. Reliability and Backup

All networking components, SSL accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Replenit Services is stored on a primary database server with multiple active clusters for higher availability. All database servers replicate in near real-time and are backed up on a regular basis. Backups are encrypted using AES-256 encryption and verified for integrity.

23. Business Continuity Management and Disaster Recovery

Replenit has a written Business Continuity and Disaster Recovery Plan, which is tested annually. Replenit tests database backups and failovers as part of our Business Continuity Plan. Backups are encrypted and stored in Microsoft Azure provided backup services.

24. Blocking Third Party Access

The Replenit Services have not been designed to include any backdoors or similar functionality that would allow the government or any third parties to access Customer Data. We do not voluntarily provide any government or other third party with encryption keys, or any other way to break our encryption.

25. Contacts

Replenit's Security Team can be reached by emailing security@replenit.com.