APPSPACE

Security Whitepaper

July 2023

Table of Contents

Introduction

The purpose of this document is to provide external parties with an understanding of the security controls at Appspace. Technical and non-technical controls are implemented to safeguard the Confidentiality, Integrity, and Availability (CIA) of customer data. Appspace's ISMS security program is based on ISO, NIST, and SOC-2 Type 2 standards. To learn more about our product portfolio, please visit Appspace.

For a deeper understanding of how our products work, please visit our Knowledge Center.

Human Resource Security

The Appspace People/HR Team leverages the processes below during the hiring and onboarding of new hires:

- Background Checks (Criminal, Employment, and Academic) are completed before hiring by following the laws and regulations in which the candidate resides.
- All employees are required to sign the information security policy, acceptable use policy, employee handbook, and a non-disclosure/confidentiality agreement upon hire and annually thereafter. Disciplinary and sanction policies are included within acknowledgment documents.
- All employees are required to complete information security and privacy awareness training upon hire and annually thereafter. Industry-standard training content is utilized.
- Engineering team members are required to complete OWASP Security training upon hire and annually thereafter to ensure they follow secure coding practices.

User Access Provisioning

As a component of the onboarding process, the HR team opens a ticket that notifies the IT team and the Security team of a new user. Onboarding tickets contain a pre-populated checklist of required tasks and approvals. Baseline configurations for the corporate environment are automatically provisioned. Additional access specific to users' job functions requires additional approvals. All users are required to use a company-owned device

User Access Revocation

As a component of the offboarding process, the HR team opens a ticket that notifies the IT team and Security team of a terminated employee. Offboarding tickets include a pre-populated list of systems to terminate access. Access is revoked on the same day as termination. The return of employer assets is also tracked within the offboarding ticket.

Information Security Policies and Procedures and Audits

All information security policies are reviewed on an annual basis and approved by the CISO. All policies and procedures are reviewed by third-party auditors as part of our SOC-2 Type 2 and ISO 27001 audits.

Appspace's ISMS program complies with ISO 27001, ISO 27017, and SOC 2 Type 2 security standards. These controls are tested by a third-party attestation firm on an annual basis. In addition, an internal audit is completed on an annual basis to test the operating effectiveness of our internal controls environment. Appspace ISO 27001 and 27017 certificates can be downloaded on our Trust Site. Appspace SOC 3 Type 2 report is available on our Trust Site. A copy of the SOC 2 Type 2 report can be shared with external third parties upon request and under NDA. Appspace is registered with the Cloud Security Alliance (CSA) and has completed a Level 1 Security Assessment. Our CAIQ v4.0.2 self-assessment can be found on our STAR Registry Listing. Additionally, Appspace is a Microsoft 365 Certified Partner. This includes an annual audit of Appspace security controls for the Microsoft partner security requirements.

Customer Data - Retention and Disposal

Appspace has defined data retention policies and data disposal policies that are defined within the Appspace Privacy Policy and Data Processing Addendum. Customer data is retained for the duration of the contract. Data will be securely destroyed upon termination of the contract or a written request. Data can be made available to customers upon request via secure file transfer before being purged from Appspace systems. Appspace in coordination with Google follows the NIST SP 800-88 guidelines related to media sanitization. More information on Google's data deletion process can be found on Google Cloud's Media Sanitization page.

Role-Based Access Controls

Appspace employs a role-based access control service within the platform. This ensures users are assigned to individual user accounts and do not utilize shared accounts. Users are assigned least-privilege roles and permissions based on the functions they undertake with the Appspace Cloud application.

Internally, Appspace Production Support and Security teams perform quarterly access reviews to ensure access and assigned permissions remain appropriate. All privileged access requires management approval before provisioning. The principle of least privilege is applied to all users based on a need-to-know basis.

Authentication

All Appspace users are required to enter a username, password, and MFA token to access the internal Appspace infrastructure. Privileged user accounts must also authenticate using a physical token. Internally, SSO is utilized to centrally manage authentication.

Password Requirements

Appspace Cloud supports Single Sign-On capabilities for customers using SAML v2.0. Logical credentials will not be stored within the Appspace database if SSO is utilized. Customers should consider employing MFA controls prior to users being granted SSO access to Appspace Cloud.

Audit Logging and Monitoring

Specific system (security, application, and system events) and user activity in the Appspace environment is logged in the SIEM. Logs are retained for a minimum of 12 months, with 90 days of log data immediately recoverable. Default logging configurations by GCP Cloud Logging services are utilized along with alerts based on the Mitre Att&CK framework and Intel Threat feeds. Logs are encrypted and cannot be tampered with.

Appspace does not support sending syslog data to Customer SIEMs.

Encryption and Tokens

All customer data stored within databases and backup snapshots are encrypted at rest using AES 256 encryption standards. Appspace Cloud utilizes HTTPS over TLS 1.2+ encryption in transit. Appspace has ceased supporting TLS 1.0/1.1 encryption on all legacy display devices. Data Encryption Keys are owned and managed by GCP through Google's KMS service for all encryption at rest. Google uses AES-256 as the key strength.

Appspace's platform has an A+ rating on SSL Labs. In addition to a strong cipher policy, Appsace has ensured our top-level domain is on the HSTS Preload List.

Appspace uses unique tokens generated when a session starts to grant access to Appspace Cloud. The session tokens expire after 20 minutes of idle time.

In addition, Appspace has implemented OAuth 2.0 to enable integration with third-party applications using a unique set of refresh and access tokens. Additional information regarding our integration capabilities can be found here.

Additional information regarding the required MS scopes can be found here.

Change Management

Appspace uses an Agile change management framework and follows a Secure Development Lifecycle. All changes are tracked in change tickets. Developer's code is peer-reviewed using OWASP code review guidelines prior to moving to QA. QA testing includes a combination of manual and automated tests. SAST scans, DAST scans, and penetration tests are completed prior to each release. Separation of duties is adopted between the developers, approver, and a merge to production. Rollback plans and post-change reviews are completed for each change. Separate environments are used for development, staging and production. Production data is never used in staging or development environments. Test scripts are utilized to generate test data. Changes are communicated to customers through the Appspace Release Calendar on our public website,

which includes Release Notes. Customers can submit feature requests through our Product Roadmap site or submit a ticket via the Appspace Cloud platform.

Vulnerability Management and Penetration Testing

Appspace's vulnerability management process includes scanning for internal and external vulnerabilities. Scans are performed continuously. Reports are run monthly for our monthly patch cycle. Vulnerabilities are rated by their criticality following CVSS.

On an annual basis, a third-party penetration test is conducted to identify any OWASP and CIS-related software vulnerabilities The pen testers leverage both manual and automated tests.

Open-source software scans are carried out in real-time and patched quarterly.

Appspace does not allow customers to carry out penetration tests or vulnerability scans in the Appspace Cloud environment. The Appspace penetration test report will be shared with customers upon request and under an NDA.

Malware and Antivirus Software

Appspace installs antimalware and antivirus software on all endpoints, including workstations and production servers. Scans are performed in real-time. Software updates are performed in real-time for new virus signatures and definitions. Assets and files are quarantined upon identification of a virus signature. In addition, the OS is hardened to further secure the platform by disabling unnecessary services from running.

Mobile Device Management

Appspace utilizes a centralized mobile device management policy to control, secure, and enforce policies on all mobile devices. Appspace requires all employees to sign the acceptable use policy upon hire and annually thereafter which defines the policy regarding using mobile devices. Customer information is not stored on mobile devices or PCs/Laptops.

Asset Inventory

All production servers and internal company-owned endpoints are tracked in a centralized inventory system. Assets are labeled per the data classification policy.

Risk Assessment and Risk Treatment Plans

Appspace performs an internal risk assessment on an annual basis. Appspace first defines a risk acceptance criteria. Risks are then identified and ranked based on the likelihood and impact of the risk occurring. All identified risks are assigned to owners. Risk treatment plans are applied to reduce the overall risk to an acceptable risk tolerance level. Risk treatment plans include implementing automation tools, detection tools, or corrective controls. The risk assessment results are reviewed and approved by the ISMS steering committee and the CISO.

Vendor Management

Appspace performs a third-party risk assessment for all third-party vendors upon onboarding and annually thereafter. The third-party risk assessment process aims to ensure that all third-party security controls align with Appspace security requirements and contractual obligations. Third-party SOC 2 and penetration test reports are reviewed as a component of this process.

Incident Response Planning

Appspace has an incident response plan in place to respond to potential security incidents. Incidents are classified by severity per the Risk Assessment results. The incident response plan is tested on an annual basis using red team/blue team testing scenarios. Customers are informed in the event of an impacting security event within 72 hours of discovering the event.

Business Continuity / Disaster Recovery Plan

Appspace has a documented Business Continuity and Disaster Recovery Plan that is reviewed and approved by management on an annual basis. The primary objective of the plan is to ensure continued operations of critical systems to meet customer contractual requirements and SLAs in the event of a disaster. The plan is tested annually by the Cloud Ops team to ensure RTO and RPO objectives are met. Upon request, a summary of the Business Continuity and Disaster Recovery plan can be shared with external third parties under a fully executed MNDA.

Backup and Recovery

Virtual snapshots of production instances are completed on an hourly basis. All backups are virtual and no physical backup media is utilized. Backups are stored in an encrypted format using AES 256 encryption. Backup restoration tests are performed in real-time in GCP and annually as a component of the DR test. Backups are retained for 90 days. Appspace ensures the availability of the platform through geographically redundant cloud environments. Rollback capabilities are available through alternative GCP processing regions and zones.

Data Classification

Any content uploaded or stored in our platform falls under the customer's ownership and is considered confidential information by Appspace, subject to our Acceptable Use Policy and Privacy Policy. Which can be viewed here: https://www.appspace.com/legal.

GDPR Requirements

Appspace complies with GDPR requirements as defined in our DPA. Appspace has appointed a Data Privacy Officer, who can be reached at privacy@appspace.com. In compliance with GDPR requirements, Appspace completed a data privacy impact assessment on an annual basis or in the event of a major release where data subject data fields may change.

Conclusion

Any additional questions regarding Appspace ISMS security control and policies and procedures can be clarified with your designated Account Manager. Appspace does not share our policies, procedures, or similar confidential security documents as these controls are audited by third-party auditors.