Security Whitepaper

April 2025

Table of Contents

Introduction

The purpose of this document is to provide external parties 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. Additional information on Appspace's security controls can be found on our Trust Page. To learn more about our product portfolio, please visit our website. For a deeper understanding of how our products work, please visit our Knowledge Center.

Appspace Organizational Security Controls

Human Resource Security

The Appspace People & Culture Team leverages the processes below during the hiring and onboarding of new employees:

- Background checks (criminal, employment, and academic) are completed before onboarding 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 the acknowledgement 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 understanding of secure coding practices.

User Access Provisioning

As a component of the onboarding process, the People & Culture Team opens a ticket to notify 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 the users' job function requires additional approvals. All users are required to use a company-owned device protected by an MDM policy.

User Access Revocation

As a component of the offboarding process, the People & Culture Team opens a ticket to notify the IT team and the Security team of a terminated user. Offboarding tickets include a pre-populated checklist of systems to terminate access. Access is revoked the same day as termination. All offboarded employees are required to return their company owned devices. The IT team wipes these devices upon receipt of the device.

Authentication

All Appspace users are required to enter a unique 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.

Information Security Policies and Procedures and Audits

All information security policies are reviewed annually and approved by our CISO. Policies and procedures align with ISO 27001 Clauses 4-10, Annex A controls, and SOC 2 Type 2 standards. Policies are reviewed by third-party auditors as a component of our annual external audits. See our ISO 27001 Certificate and SOC 2 Type 2 Report.

Appspace's ISMS program complies with ISO 27001, ISO 27017, and SOC 2 Type 2 security standards. A third-party attestation firm tests these controls on an annual basis. In addition, an internal audit is completed annually to test the operational effectiveness of our internal controls environment. Appspace ISO 27001 and 27017 certificates can be downloaded on our Trust Page. Appspace SOC 3 Type 2 report is available on our Trust Page. Appspace SOC 2 Type 2 report can be shared with external third parties upon request and under an MNDA. 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 CSA's STAR Registry Listing. Additionally, Appspace is a Microsoft 365 Certified Partner. This includes an annual audit conducted by Microsoft of Appspace's security controls against the Microsoft partner security requirements.

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.

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 a risk owner. 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 ISMS steering committee and the CISO reviews and approves the risk assessment results.

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's security requirements and contractual obligations. Third-party SOC 2 Type 2 and penetration test reports are reviewed as a component of this process.

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.

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.

Product Security

Appspace Artificial Intelligence

Appspace leverages Artificial Intelligence security controls defined by the EU AI Act & ISO 42001 as a baseline compliance benchmark for our Artificial Intelligence features. Appspace does not utilize customer data to train our models, nor does it store customer data. Personally Identifiable Information should not be submitted in our Artificial Intelligence platform. Appspace's offensive security team regularly tests Artificial Intelligence features against OWASP LLM standards. Our annual third party penetration test includes testing of our Artificial Intelligence features. Appspace leverages Azure AI and Google Vertex AI as our LLM models while using internal data sources to build maturity in the model. For additional information on our Artificial Intelligence features, please ask your Account Manager for our Artificial Intelligence Product Security Overview article.

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 upon 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 our cloud hosting service provider follows the NIST SP 800-88 guidelines related to media sanitization. More information on the data deletion process can be found on the cloud hosting service provider's Media Sanitization Page.

Public Cloud vs. Private Cloud

Appspace customers have the option to select either a public cloud or private cloud environment. Public cloud customers have a multi-tenant environment with unique cryptographic keys to logically segment customer data. Private cloud customers have a single tenant environment allowing for physical and logical segregation of customer data. Both environments comply with GDPR regulations. Private cloud tenants enforce cross-border transfer restrictions. As part of our compliance with the EU-US Data Privacy Framework, Appspace may transfer Public cloud data to the US.

Role-Based Access Controls

Appspace employs a role based access control service within the platform. This ensures users are assigned an individual user ID and do not utilize shared accounts. Users are assigned roles and permissions based upon least-privilege and 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 upon a need-to-know basis.

Password Requirements

Appspace 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 authentication controls before users access Appspace Cloud through SSO.

Audit Logging and Monitoring

Specific system (security, application, and system events) and user activity in the Appspace environment is logged in the Appspace SIEM. Logs are retained for a minimum of 12 months, with 90 days of log data immediately recoverable. Default logging configurations provided by the cloud hosting service provider's 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. Alternatively within the platform, the reports and analytics modules provide admin users with statistical data on their system and user's activity.

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. The cloud hosting service provider owns and manages all Data Encryption Keys through the cloud provider's KMS service for all encryption at rest. Appspace utilizes AES 256 as the key strength.

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

Appspace uses unique tokens that are generated when a session starts to grant access to Appspace Cloud. 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 Microsoft scopes can be found here.

Change Management

Appspace follows a Secure Software Development Lifecycle. The developer's code is peer-reviewed following OWASP code review guidelines before moving to QA. QA testing includes 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. 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 internal and external vulnerabilities. Scans are performed continuously and patched monthly according to criticality following CVSS.

On an annual basis, a third-party penetration test is conducted to identify any OWASP or CIS-related software vulnerabilities.

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

Incident Response Planning

Appspace has an incident response plan to address 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 notified of a confirmed security incident within 72 hours of discovery.

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 Operations team and Security 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 MNDA.

Backup and Recovery

Virtual snapshots of production instances are completed every 4 hours. All backups are virtual and no physical backup media is utilized. Backups are stored in encrypted format using AES 256 encryption. Backup restoration tests are performed in real-time and annually as a component of Business Continuity and Disaster Recovery Plan test. Backups are retained for 90 days. Appspace ensures platform availability across geographically

redundant cloud environments. Rollback capabilities are available through alternate processing regions and zones.

Data Privacy Program

Data Classification

Any content loaded 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 .

GDPR Requirements

Appspace complies with GDPR requirements as defined in our Data Processing Addendum. Appspace has appointed a Data Privacy Officer, who can be reached at privacy@appspace.com. In compliance with GDPR requirements, Appspace completes a data privacy impact assessment on an annual basis or in the event of a significant change to personal data of data subjects processed by Appspace.

Privacy Controls

Appspace's privacy program allows data subjects to exercise their privacy rights to access, update, modify, and delete their data while using the Appspace Cloud platform. Appspace has self-certified our compliance with the EU-US Data Privacy Framework (DPF) and partnered with PrivacyTrust to support third-party dispute resolutions. Appspace's Privacy Policy can be found on our Legal Page.

Sub-Processor Locations

A list of Appspace's sub-processors can be found in our Data Processing Addendum.

Conclusion

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