A.I. Storage

For every Enterprise

Security
Whitepaper

www.aispace.co

Table of Content

INTRODUCTION

This whitepaper covers the security of Alspace, an AI Storage platform. Except where noted, the information in this whitepaper applies to all Alspace products. In terms of security, we separate security into three distinct segments:

1) Data Security
2) Application Security
3) Platform Security

The structure of this whitepaper reflects the above three distinct security segments.

Alspace is a service fully owned by Babbobox (www.babbobox.com).

Babbobox developed the World's First true Unified Search Engine, where we combined numerous advanced technologies like Speech Recognition, Video OCR, Cognitive Services, Image Analysis, Artificial Intelligence and Enterprise Search into a single platform. Giving Alspace the unique ability to "Search Everything" - index and search inside every document, image, audio and video.

The most logical place to apply A.I. is where information is stored - Storage. Thus, making **Alspace** the next generation of Intelligent Enterprise Storage where we make A.I. easily available to all enterprises.

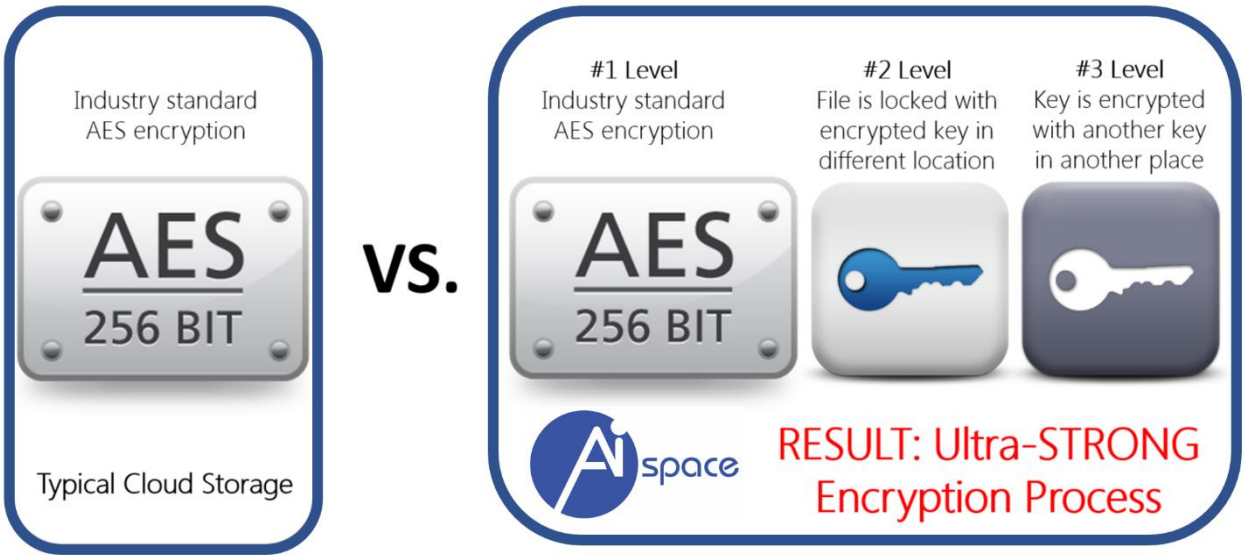
A.I. Storage for every Enterprise

DATA SECURITY

We employ multiple layers of military grade AES 256-bit encryption technology to ensure the security of your files and data.

Most other cloud providers typically use 2-way encryption to secure files. Nothing wrong with that, however, it also means that files can still be opened by using the "brute force" method. Alspace encrypts files in such a way that in the very unlikely event that your files are compromised, your files simply cannot be opened and are totally useless to the perpetrators.

Despite the complex nature of deploying multiple layers of encryption, we do feel that this methodology offers one of the best (if not the best) form of data security in the Cloud. In addition, all communications are done over SSL to complete the entire security loop.



As a result, our encryption process is ultra-strong and is more sophisticated than any typical cloud storage. Our single-minded objective is to ensure that data within Alspace is safe and secured.

APPLICATION SECURITY

3-Tier Security

On top our data security measures, we apply our proprietary application level 3-Tier Security for files are targeted at the following levels:

1. **User Account** – Users sharing their files with specific users only.
2. **Folder** – Users sharing their files inside a folder via a specific link
3. **File** – User sharing individual files using a specific link

The above file-sharing methodologies can be:

1. **Password protected** – users can set unique passwords to protect folder and files
2. **Set expiration (date)** – users can set expiration dates to automatically terminate sharing options.

Collaboration – User Type security

Collaboration with other users are set with 2 levels of permission:

1. **Editor** – has full permission of the shared folder
2. **Viewer** – only has permission to view contents of the shared folder

You can also un-share or delete folders and files based on schedule (known as document expiration feature), and even enforce greater security protection to your sensitive shared folders or files with hierarchy of passwords.

Audit Log – User Activity Security

In addition, Alspace provides a comprehensive audit log for both System Administrator and Users.

For “System Administrators”, you can track all actions users make in the system. These actions include:

- Uploads/Downloads
- Invite Collaborators
- Create/Delete Folders
- Create/Delete Files
- Share/Remove Folders
- Share/Remove Files
- Assign/Remove Password to Files/Folders, Etc

For “Users”, you can track all the following actions:

- All activities by yourself, AND
- All activities by OTHER USERS within the shared folder.

PLATFORM SECURITY

Our platform partner is MICROSOFT Azure (www.azure.com).

Azure has more certifications than any other cloud provider!

Microsoft leads the industry in establishing clear security and privacy requirements and then consistently meeting these requirements. Azure meets a broad set of international and industry-specific compliance standards, such as General Data Protection Regulation (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify Azure's adherence to the strict security controls these standards mandate.

In addition, Microsoft has developed an extensible compliance framework that enables it to design and build services using a single set of controls to speed up and simplify compliance across a diverse set of regulations and rapidly adapt to changes in the regulatory landscape. More information on specific compliance programs is available here:

- ISO 27001/27002
- SOC 1/SSAE 16/ISAE 3402 and SOC 2
- Cloud Security Alliance CCM
- FedRAMP
- FISMA
- FBI CJIS (Azure Government)
- PCI DSS Level 1
- United Kingdom G-Cloud
- Australian Government IRAP
- Singapore MTCS Standard
- HIPAA
- EU Model Clauses
- Food and Drug Administration 21 CFR Part 11
- FERPA
- FIPS 140-2
- CCCPPF
- MLPS

Read more about cloud security compliance HERE (https://www.microsoft.com/en-us/TrustCenter/Compliance/compliance-overview).

INCIDENT REPORTING

We have incident response procedures to address various AIspace security and integrity issues. As part of our incident response procedures, our team will:

- Promptly respond to alerts of incidents
- Determine the severity of the incident
- Execute mitigation measures (if necessary)
- Communicate with relevant stakeholders, including notification to affected customers
- Develop a permanent plan to upgrade system to prevent future incidents (if necessary)

To report any security incident, please write to support@aispace.com with the title “Security Incident”.

===== END OF DOCUMENT =====