OnePlaceSafe

OnePlaceSafe Security Doc

1. Executive Summary

In a world where life's unpredictability can strike at any moment, OnePlaceSafe empowers you to take control of your personal data with confidence. Designed as a secure, trusted companion, OnePlaceSafe ensures that critical information remains safeguarded and accessible, ready for you or your loved ones in times of need—whether facing loss, incapacity, or health challenges.

With OnePlaceSafe's secure vault, you can store and protect essential files, bank details, financial information, and asset records, along with passwords and other critical data. This platform not only provides robust security but also simplifies inheritance planning and handovers. In the event of your passing, it enables seamless, secure information sharing with a nominated person, ensuring nothing vital is lost.

As digital threats intensify, safeguarding personal information has never been more crucial. OnePlaceSafe addresses these concerns by combining high-grade encryption, stringent access controls, and a seamless user experience to make data security effortless and effective.

2. Problem statement

In an increasingly digital world, managing and securing personal data for unforeseen events like death, incapacity, or mental health decline is a complex and often neglected task. Traditional storage methods—physical files or unsecured digital notes—leave sensitive data vulnerable to loss, unauthorized access, or cyber threats, complicating inheritance and critical information handover.

OnePlaceSafe addresses this need by providing a secure, centralized platform where users can store essential data, including passwords, bank details, and asset records. This ensures vital information remains protected and easily accessible to trusted individuals when it matters most, reducing risks and offering peace of mind in managing life's unpredictabilities.

OnePlaceSafe prioritizes user data security and confidentiality. This document outlines the key measures in place to protect personal information stored on the platform, ensuring it meets the highest standards for data protection and privacy.

3. Our Security Principles

OnePlaceSafe is more than a platform—it's a sanctuary. It's where security is absolute, privacy is unquestioned, and peace of mind is woven into every interaction. We've dismantled the complexity of traditional security to create a seamless experience, free of extra steps or confusing settings. Here, your data is protected by top-tier protocols and the expertise of dedicated minds. With OnePlaceSafe, you're in control, reclaiming your digital life with simplicity and confidence, one effortless step at a time.

3.1. Data Encryption

At OnePlaceSafe, we prioritize the protection of user data through robust encryption mechanisms, ensuring data confidentiality at every stage of interaction.

3.1.1 Encryption in Transit

All communications between users' browsers and our servers are encrypted using SSL/TLS protocols. This ensures secure data transmission, protecting against potential interception or eavesdropping while data is in transit. We use HTTPS, the industry-standard protocol, to establish a secure, encrypted tunnel for all data exchanged between the OnePlaceSafe application and our servers, making it impenetrable while traveling across the internet.

3.1.2 Encryption at Rest

While not all data is encrypted at rest, we ensure that **sensitive data** stored in **AWS RDS (Relational Database Service)** is encrypted using **AWS's built-in encryption**. AWS RDS employs **AES-256 encryption** and leverages **AWS Key Management Service (KMS)** to manage and control encryption keys. This encryption applies to the database storage, backups, snapshots, and replicas, ensuring that sensitive data remains protected from unauthorized access.

While not all data in the database may be encrypted, **sensitive user data** is explicitly secured, and AWS RDS provides multiple layers of security such as **network isolation, access control policies**, and **monitoring** to further safeguard the stored information.

Our system guarantees **end-to-end encryption**, safeguarding your data at all stages—whether it's being transmitted or stored—so you can trust that your personal information is always protected.

3.2 Authentication and Authorization

OnePlaceSafe is committed to robust security measures for authentication and authorization, ensuring that only verified users access the platform's resources securely. Key components of our security framework include:

3.2.1 Multi-Factor Authentication (MFA)

MFA is implemented for all privileged accounts, requiring users to complete two or more verification methods (e.g., password and authenticator app or SMS code) before accessing sensitive data.

3.2.2 Role-Based Access Control (RBAC)

Access permissions are based on user roles, ensuring that users only access resources essential to their roles, minimizing exposure to sensitive information.

3.2.3 JWT Tokens for API Protection

JSON Web Tokens (JWT) are used to secure API access, providing a secure, encrypted token-based authentication process. Tokens are generated on login, limited to a set duration, and protect against unauthorized access.

3.2.4 Email and Mobile Verification

During registration, users are required to verify their email addresses and mobile numbers by entering a one-time code. This step ensures authenticity and safeguards against unauthorized account creation.

3.2.5 Session Expiry

Sessions automatically expire after a set period of inactivity to prevent unauthorized access and reduce risks from unattended sessions.

3.2.6 Strong Password Policy

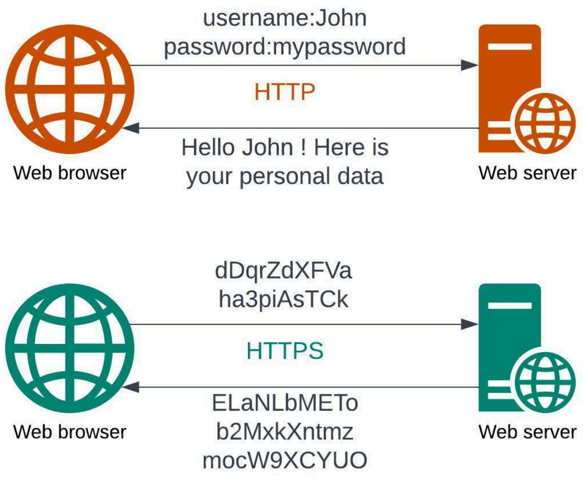
Users must follow a stringent password policy, requiring complex, unique passwords to enhance security.

3.2.7 Password Hashing

All passwords are securely hashed using the SHA256 algorithm, making them resistant to brute-force attacks. Passwords are stored in a hashed format, providing additional protection in case of unauthorized access to the data.

3.2.8 TLS/SSL Encryption

Transport Layer Security (TLS) and Secure Socket Layer (SSL) encryption protocols are implemented to ensure end-to-end encryption of all data transmissions, protecting data from interception and unauthorized access during transit.



3.2.9 Planned Identity Verification Enhancements

Next quarter, OnePlaceSafe plans to strengthen identity verification by implementing government ID and biometric verification:

3.2.9.1 Government ID Verification

Users will be required to upload a government-issued ID, verified automatically through Persona, an online identity verification tool. This step ensures that users create profiles using their legal names, preventing profile falsification.

3.2.9.2 Biometric Verification

For further security, biometric verification (such as facial recognition) will be integrated using a third-party service. This additional layer will enhance account security, ensuring verified users are who they claim to be.

Note: This comprehensive approach ensures that OnePlaceSafe maintains a secure and reliable environment for all users, aligned with industry standards and best practices.

3.3 Data Storage and Backup

OnePlaceSafe leverages Amazon Web Services (AWS) Relational Database Service (RDS) for secure and reliable data storage, benefiting from AWS's robust, multi-layered security features that safeguard our databases. AWS RDS offers a range of built-in security protections, including:

3.3.1 Automated Backups and Snapshots

AWS RDS provides automated daily backups, enabling point-in-time recovery for up to 35 days. Additionally, OnePlaceSafe conducts independent, scheduled backups (once a month) of user data to further enhance data redundancy and ensure rapid restoration if needed.

3.3.2 Database Instance Isolation

AWS RDS operates within a Virtual Private Cloud (VPC), which provides network isolation for databases, ensuring that only authorized resources within our infrastructure can access the data. We also use firewall rules to control access to specific IP addresses and ports, adding a layer of network security.

3.3.3 Automated Patching and Updates

AWS RDS automatically applies the latest security patches and updates to database instances, ensuring databases are protected against known vulnerabilities and reducing the need for manual intervention.

3.3.4 Fine-Grained Access Control

Access to AWS RDS is tightly controlled through AWS Identity and Access Management (IAM) roles, allowing OnePlaceSafe to assign and enforce permissions based on specific roles and responsibilities. This setup ensures that only authorized personnel can access and manage database resources.

3.3.5 Planned Multi-AZ (Availability Zone) Deployment

For high availability and reliability, we can utilize AWS's Multi-AZ configuration, which maintains synchronous database replicas across multiple data centers. This setup helps ensure continuity and data protection in case of hardware failure or other incidents.

Note: Our approach to data security in AWS RDS, combined with our independent, scheduled backups and AWS's automated backups, provides multiple layers of data redundancy and protection. These security features, together with our own practices, ensure that OnePlaceSafe maintains a secure, resilient, and compliant data storage environment for all user information.

3.4 Secure File Management

OnePlaceSafe has implemented a comprehensive and secure approach to file management, ensuring proper file isolation, optimal performance, and robust protection for user-uploaded data:

3.4.1 Dedicated User Workspaces

All files and uploaded data are stored in separate user workspaces, ensuring complete data isolation and preventing any risk of data mix-up or cross-contamination.

3.4.2 Secure Storage with AWS S3

All media files are securely stored in Amazon S3, benefiting from AWS's scalable and highly secure infrastructure. AWS S3 offers **encryption at rest (AES-256)** and **in-transit encryption (TLS/SSL)**, ensuring the data is protected during both storage and transmission.

3.4.3 CloudFront CDN for Performance Optimization

To enhance the speed and reliability of file access, we use **AWS CloudFront** as our Content Delivery Network (CDN). CloudFront caches media files at multiple edge locations worldwide, delivering them quickly and efficiently to users, reducing latency and distributing the load for improved performance.

3.4.4 Access Control and Permissions

Access to AWS S3 buckets is strictly controlled using **AWS Identity and Access Management (IAM)** policies. These policies enforce role-based access controls, ensuring only authorized users or services can interact with or access sensitive files.

3.4.5 Object-Level Access Logging and Monitoring

AWS S3's **access logging** feature records every request to access files, providing detailed audit trails for enhanced monitoring. Continuous logging and regular audits help identify unauthorized or suspicious access attempts.

3.4.6 Versioning and File Recovery

AWS S3 versioning is enabled to store multiple versions of each file, allowing for easy recovery of files in case of accidental deletion or modification. This ensures that files can be restored to their previous, unaltered state.

3.4.7 Planned: Automated Security Scans

Uploaded files are automatically scanned for malware and security risks before they are stored in the system, ensuring that only clean, safe files are uploaded and distributed.

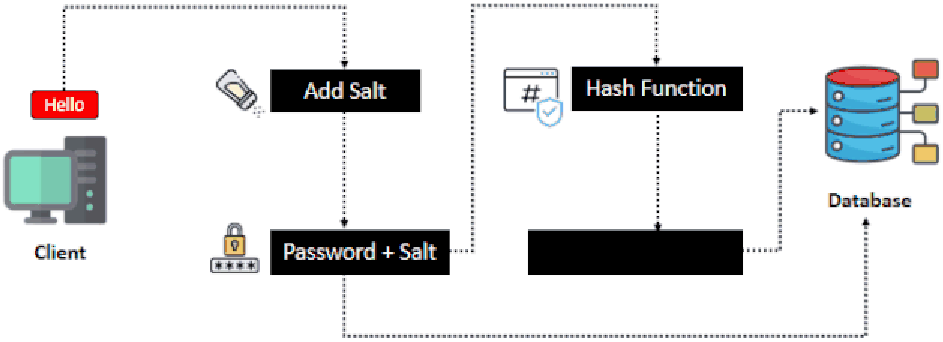
Note: By combining **AWS S3** with **CloudFront CDN**, **strong access controls**, **versioning**, and regular security scans, OnePlaceSafe delivers a secure, efficient, and high-performance file management system, ensuring both user data protection and a seamless experience.

3.5 Password and Key Management

At OnePlaceSafe, we prioritize the security of user credentials and access keys by employing best practices for hashing, storage, and password strength:

3.5.1 Password Hashing

All user passwords are securely hashed using the **SHA-256** algorithm, a cryptographic hash function that ensures strong security for protecting stored passwords. To further enhance security, we use **salting**, which adds a unique, random value to each password before hashing. This makes it significantly harder for attackers to crack or reverse the hashed passwords, even if intercepted during data transmission or storage.



3.5.2 Strong Password Policy

We enforce a **strong password policy** to ensure that user passwords are sufficiently secure. Passwords must meet minimum complexity requirements, such as a combination of uppercase and lowercase letters, numbers, and special characters. We also require a minimum password length to help protect against common attack vectors like dictionary or brute-force attacks.

3.5.3 Access Key Management

Third-party access keys, including those for APIs and services, are stored securely in **separate configuration files** outside of version control systems. This reduces the risk of accidental exposure, such as when source code is shared publicly or mismanaged in development environments. By maintaining this separation, we ensure that critical access keys are not inadvertently leaked or exposed to unauthorized parties.

Note: These best practices—combined with our strong password policy—help safeguard user credentials and system access keys, ensuring protection against unauthorized access and potential exploitation.

3.6 Regular Security Audits

We plan to conduct **regular security audits** and **vulnerability assessments** to proactively identify and address potential security risks. These audits involve thorough reviews of our system architecture, access controls, and data handling procedures to ensure compliance with best practices. The vulnerability assessments are designed to test our defenses against emerging threats, including malware, unauthorized access attempts, and potential exploits. This **proactive approach** helps us maintain the **integrity and resilience** of our systems, ensuring that security gaps are swiftly identified and mitigated before they can be exploited.

Note: This will be developed before the commencement of operations.

3.7 Compliance and Regulatory Standards

OnePlaceSafe is committed to upholding the highest standards of data protection and privacy, ensuring full compliance with global data protection regulations, including **GDPR**. We don’t just meet regulatory requirements; we actively implement measures that go above and beyond these standards to protect user data and ensure complete transparency and control for our users.

3.7.1 Compliance and Best Practices:

- **Data Collection, Storage, and Processing**:
  - **Data Minimization**: We collect only the minimum amount of data necessary for our platform to function effectively. This ensures that we are not over-collecting sensitive information that could increase the risk of misuse.
  - **Data Encryption**: All sensitive data, including personal information, is encrypted both at rest and in transit, using industry-standard encryption protocols like **AES-256** for data storage and **SSL/TLS** for data transmission. This ensures that data is always secure, whether it is being sent or stored.
  - **Data Anonymization & Pseudonymization**: We use techniques such as anonymization and pseudonymization to reduce the exposure of personally identifiable information (PII) during processing, ensuring that even if data is accessed or compromised, it cannot be easily attributed to specific individuals.
  - **Data Retention & Deletion**: We retain personal data only for as long as necessary for legal, operational, or contractual purposes. We also implement clear **data deletion policies** that comply with GDPR's right to erasure, allowing users to request the removal of their personal information from our systems.
- **User Control and Transparency**:
  - **Consent Management**: We provide users with clear and transparent consent mechanisms, ensuring that they are fully informed of the data we collect and how it will be used. This allows users to provide or withdraw consent as needed, in accordance with GDPR's requirements.
  - **User Access and Data Portability**: Users can easily access and manage their data through their **OnePlaceSafe** account. We also support **data portability** by allowing users to download their personal data in a structured, commonly used format, enabling them to transfer it to other services or platforms if desired.
  - **Privacy Settings**: We offer customizable privacy settings so users can control what data they share and with whom, ensuring full transparency and giving users autonomy over their personal information.
- **Access Control and Authorization**:
  - **Role-Based Access Control (RBAC)**: We strictly enforce **role-based access control (RBAC)** to ensure that only authorized individuals have access to specific data. This includes ensuring that only **OnePlaceSafe clients** have access to their

  own data, and our staff members have restricted access to user data. Any access by staff is based on **the principle of least privilege**, meaning employees only have access to the minimum amount of data necessary to perform their job.
  - **Authentication and Authorization**: We implement strong **multi-factor authentication (MFA)** for privileged accounts and enforce robust password policies for all users, ensuring that only authenticated individuals can access sensitive data. Our systems also employ **token-based authentication** to secure APIs and provide an additional layer of protection against unauthorized access.
- **Audit Trails and Monitoring**:
  - **Continuous Monitoring**: We monitor all access to sensitive data in real-time and maintain detailed audit logs to track user actions, system access, and potential security threats. This allows us to detect and respond to any suspicious activity promptly.
  - **Regular Security Audits**: We conduct periodic internal and external security audits to assess the effectiveness of our security measures and ensure compliance with industry standards and regulatory requirements. These audits also help us identify potential vulnerabilities and address them proactively.
- **Data Transfer and International Compliance**:
  - **Cross-Border Data Transfers**: In compliance with GDPR and other global privacy regulations, we ensure that data transferred across borders is adequately protected. We rely on tools like **Standard Contractual Clauses (SCCs)** and **Privacy Shield frameworks** to ensure that data remains secure when stored or processed in different jurisdictions.
- **Staff Training and Awareness**:
  - **Employee Training**: We conduct regular training sessions for all staff to ensure they understand the importance of data protection and are aware of best practices for handling user information. This training covers topics such as data privacy laws, secure data handling, and threat detection.
  - **Access to Sensitive Data**: Staff members only have access to sensitive user data if absolutely necessary. We enforce strict guidelines to ensure that employees

are fully aware of their responsibilities when it comes to data privacy and security.

3.7.2 Handle Client Access to Data:

- **Authorized Individuals**: Access to sensitive user data is strictly limited to **authorized individuals**—specifically, the **OnePlaceSafe clients** themselves. Only clients have access to their own data, ensuring that their privacy is preserved. **OnePlaceSafe staff** are granted access only when absolutely required, for example, in cases of customer support or platform maintenance, and only with prior consent from the user.
- **Access Monitoring for OPS Staff**: Our systems actively monitor any staff access to client data. Even when access is required, we adhere to **role-based access control (RBAC)** to ensure that staff members can only access the minimum level of information necessary to perform their duties. We also regularly review and audit access logs to detect any unauthorized access.

By following these rigorous procedures and continuously reviewing and improving our security and privacy practices, OnePlaceSafe not only ensures compliance with GDPR and other global data protection regulations but also demonstrates a commitment to safeguarding user data and maintaining the trust of our clients.

3.8 Incident Response Plan

We have developed a comprehensive incident response plan that enables us to respond swiftly and effectively to any potential security breaches. This plan includes continuous real-time monitoring of our systems to detect anomalies, immediate alerts to notify our security team of any suspicious activity, and a well-defined escalation process to ensure rapid communication and action. Additionally, our mitigation efforts are designed to contain and remediate incidents promptly, minimizing potential damage and ensuring the continuity of our operations. Regular training and simulations are conducted to keep our team prepared for various scenarios, ensuring that we are ready to respond effectively when incidents occur.

Note: This will be developed before the commencement of operations.

3.9 Employee Training and Awareness

We conduct regular employee training programs to ensure our team is well-versed in the latest security best practices. These training sessions cover a range of topics, including threat recognition, data protection, and safe online behaviors, fostering a culture of security awareness throughout the organization. By empowering our employees with the knowledge and skills necessary to identify potential risks and respond appropriately, we create a proactive security-conscious environment that enhances our overall resilience against cyber threats.

Note: This will be developed before the commencement of operations.

4. Conclusion

OnePlaceSafe is committed to providing a secure, user-centric solution for safeguarding personal and financial data. Through advanced encryption, strong access controls, and rigorous security practices, we ensure that critical information remains protected and accessible when it matters most. Our platform brings peace of mind, enabling users to manage life’s uncertainties confidently and securely. With OnePlaceSafe, your data is not just stored—it’s safeguarded, entrusted, and ready for the moments that count.

This comprehensive security framework demonstrates **OnePlaceSafe**'s commitment to safeguarding user information and building trust with investors and users alike.