Security Assurance Report for Alterland's Virtual Office

1. Executive Summary

Alterland's Virtual Office Environment represents a cutting-edge solution designed to meet the evolving needs of remote work, providing an immersive and secure virtual workspace for global corporations and smaller firms alike. In an era where data security and privacy are paramount, Alterland has committed to implementing robust security measures to protect the integrity and confidentiality of client data. This Security Assurance Report (SAR) outlines the comprehensive security framework that underpins Alterland's virtual office product, demonstrating our unwavering commitment to safeguarding our clients' information.

The core objective of this document is to provide a detailed overview of the security architecture, policies, and procedures that Alterland has established to ensure the highest levels of data protection. This includes an in-depth analysis of our data workflows, encryption methodologies and authentication mechanisms. By adhering to international security standards and best practices, Alterland aims to foster trust and confidence among our prospective clients, particularly those operating in highly regulated industries such as banking and finance.

Key Highlights:

1. Advanced Encryption: Utilization of state-of-the-art encryption technologies for data at rest and in transit, ensuring that all client data is securely encrypted using industry-standard protocols.
2. Robust Authentication: Implementation of multifactor and adaptive authentication mechanisms to enhance user access security and prevent unauthorized access.
3. Comprehensive Data Workflow Management: Detailed documentation of data ingestion, processing, storage, and sharing practices, emphasizing transparency and control over data handling processes.
4. Third-Party Security Partnerships: Collaboration with leading security vendors and OAuth providers to bolster our security infrastructure and compliance capabilities.

Alterland's dedication to security is not just about implementing technical measures; it's about creating a culture of security awareness and continuous improvement. This document serves as a testament to our proactive approach to security and our commitment to maintaining the trust of our clients by protecting their most valuable assets.

In conclusion, Alterland's Virtual Office Environment is designed with security at its core, offering a reliable and secure platform for remote work. Through our comprehensive security measures and adherence to regulatory standards, we are confident in our ability to meet the stringent security requirements of top-tier global corporations, ensuring that their data remains protected at all times.

2. Introduction

2.1. Overview of Alterland's Virtual Office Product

Alterland's Virtual Office Environment is a revolutionary platform designed to redefine the concept of remote work by providing an immersive, interactive, and highly secure virtual workspace. Our product leverages cutting-edge virtual reality (VR) technology to create a collaborative and engaging office experience for teams distributed across the globe. By simulating a physical office environment in a virtual space, Alterland enables seamless communication, collaboration, and social interaction among remote employees, fostering a sense of community and belonging.

The virtual office environment includes features such as customisable virtual workspaces, interactive meeting rooms, private and group communication channels, and integration with popular productivity tools. These features are designed to enhance productivity, facilitate collaboration, and improve the overall remote work experience while ensuring the highest levels of data security and privacy.

2.2. Purpose of the Data Security Audit Document

The purpose of this Security Assurance Report (SAR) document is to provide a comprehensive overview of the security measures and protocols that Alterland has implemented to protect the data and privacy of our clients. This document is intended for the corporate compliance and security divisions of large international firms, including banks and other regulated entities, that require assurance of the security and confidentiality of their data when engaging with external partners.

This document outlines the technical and procedural safeguards in place to secure client data throughout its lifecycle within the Alterland Virtual Office Environment. It covers aspects such as data encryption, authentication and compliance with international data protection regulations. By providing this detailed security overview, Alterland aims to demonstrate our commitment to upholding the highest standards of data security and to build trust with our prospective clients, ensuring they can confidently choose Alterland as their remote work solution provider.

3. Technical Overview

3.1 Software Components

3.1.1 Alterland App

The Alterland application is designed to operate seamlessly across both VR and PC platforms, providing users with a versatile and immersive experience regardless of their preferred device. As a stateless front-end interface, the application ensures that no user information or sensitive data is stored within the application itself, whether accessed via VR or PC. This design approach significantly minimizes the risk of data exposure or leakage directly from the application.

For the purposes of data collection, transfer, and storage, Alterland App leverages an internal browser built into the Unreal Engine 5 (UE5), known as UWebBrowser/SWebBrowser. This internal browser facilitates access to the Web component, referred to as Alterland Hub, which is the central node for processing all sensitive and confidential data.

Security Aspects of Using UE5 Built-in Browsers:

The use of UE5's built-in browsers (UWebBrowser/SWebBrowser) for accessing the Alterland Hub introduces several security considerations. From a security standpoint, these browsers are designed to

provide a seamless integration between the VR environment and web-based services, enabling a rich user experience without leaving the VR interface. However, this integration also presents unique security challenges and strengths.

Strengths:

- **Isolation**: The UE5 browser operates within a controlled environment, isolated from the user's main operating system and web browsers. This isolation can help mitigate the risk of cross-site scripting (XSS) attacks and other web-based threats.
- **Controlled Updates**: Being part of the UE5 ecosystem, the built-in browser benefits from regular updates and security patches directly from Unreal Engine developers, ensuring that known vulnerabilities are addressed promptly.

Risks:

- **Limited Security Features**: Compared to mainstream web browsers that offer extensive security features and plugins (e.g., advanced tracking protection, ad blockers), UE5's built-in browsers may have limited capabilities in this regard, potentially exposing users to certain web-based threats.
- **Dependency on Engine Updates**: Security of the built-in browser is directly tied to the update cycle of UE5. Any delay in applying engine updates could leave known vulnerabilities unpatched for longer periods.

Consequences of Using the Alterland Hub via UE Browser:

From a security perspective, accessing the Alterland Hub through the UE5 built-in browser requires careful consideration of the aforementioned strengths and risks. While the isolation and controlled update environment offer a layer of protection, the potential limitations in security features necessitate additional safeguards. To mitigate these risks, Alterland employs several strategies:

- **Regular Security Assessments**: Continuous security testing and vulnerability assessments of the Alterland Hub and its integration with the UE5 browser to identify and remediate potential security issues.
- **Secure Data Transmission**: Implementation of robust encryption protocols for all data transmitted between the Alterland App and Alterland Hub, ensuring that sensitive information is protected in transit.
- **Authentication and Authorization**: Strong authentication and authorization mechanisms to control access to the Alterland Hub, preventing unauthorized access to sensitive data.

In conclusion, while the use of UE5's built-in browsers for accessing the Alterland Hub introduces specific security considerations, Alterland's proactive approach to security, including regular updates, encryption, and access controls, aims to mitigate these risks and ensure a secure environment for all users.

3.1.2. Alterland Hub

AlterlandHub is a comprehensive user interface designed to facilitate all major workflows associated with Alterland, providing a centralized platform for users to manage their accounts effectively. Through AlterlandHub, users can handle a variety of essential tasks, such as managing user profiles, organizing and overseeing organizations, and handling payments securely. The platform also empowers users to rent and customize virtual office spaces, manage their calendars, and schedule meetings seamlessly.

As a web-based application, AlterlandHub is fully compatible with all modern web browsers, including Firefox, Safari, and Chrome, making it accessible across different devices.

Users can download the latest version of the Alterland Launcher directly through AlterlandHub. The Launcher is crucial for installing and updating the Alterland application, ensuring that users always have access to the most up-to-date features and improvements of the Alterland.

3.1.3. Launcher

The Alterland Launcher is an essential tool for users, designed to facilitate the download and installation of the latest version of the Alterland application. By using the Launcher, users ensure they have the most current features and updates, providing an optimal experience within the Alterland virtual environment.

In addition to its core function of managing software updates, the Launcher also includes capabilities for personalizing the user experience. Specifically, it enables users to create and customize their avatars through the integrated AvatarSDK. This feature allows users to design a unique virtual representation of themselves, enhancing their presence and interaction within the Alterland application.

3.2. Hardware and Network Infrastructure

All services within the Alterland ecosystem are hosted on Amazon Web Services (AWS), a leading cloud computing platform renowned for its high scalability, reliability, and security. AWS provides a resilient and highly available infrastructure, which is crucial for maintaining the continuous operation of Alterland services. With multiple data centers located globally, AWS offers geographic redundancy, reducing the risk of service disruption due to localized failures or outages. This ensures that users can access Alterland services reliably, regardless of their location.

3.3. Third party

Vivox

Vivox is integrated into our platform to provide high-quality voice communication services.

When using Vivox, Alterland only:

- transmits voice data for playback within our system, ensuring that voice communications remain secure and private. These data are not stored.

This approach helps to maintain the confidentiality of conversations by limiting data transmission to essential audio playback functions. You can review Vivox's privacy policy at this link https://vivox-ai.com/privacy-policy/.

AvatarSDK

AvatarSDK is used to create and manage user avatars within Alterland's virtual environment. This service enables the generation of realistic and customizable avatars based on user inputs.

AvatarSDK stores and processes:

- the photo that has been uploaded by the user, which is then used to generate the avatar.

You can review AvatarSDK's privacy policy at this link https://avatarsdk.com/privacy-policy/.

Auth0

Auth0 is integrated into our platform to provide secure and reliable authentication and authorization services.

It processes:

- user credentials and authentication data like email, nick and password to ensure that only authorized users can access our system.

Auth0 helps to maintain security by managing user sessions and enforcing strong authentication protocols. You can review Auth0 privacy policy at this link: https://auth0.com/docs/secure/data-privacy-and-compliance/.

AWS

AWS (Amazon Web Services) is utilized for hosting and managing our cloud infrastructure.

It stores:

- Account information: email addresses, passwords (encrypted), nicks, profile pictures, data related to organizations.
- Data related to subscriptions and payments - Users' transaction history.
- Files uploaded by users to Drive, such as photos, videos, documents (jpg, png, mp4, pdf).
- Operational logs that help monitor and debug the application.
- Backups of application data to ensure that data can be restored in case of failure.

AWS's robust security measures and compliance certifications help protect data integrity and confidentiality. You can review AWS's privacy policy at this link https://aws.amazon.com/privacy/.

OpenAI

OpenAI is employed to enhance our platform's capabilities with advanced artificial intelligence functions, such as natural language processing. OpenAI is used exclusively within our Smart Note service, a cutting-edge AI-driven tool that revolutionizes the way meeting notes are created and managed in a virtual environment.

OpenAI processes:

- user input data to provide intelligent responses and improve user interaction. That data are not stored.

We ensure that data shared with OpenAI is anonymized and handled according to our privacy policies. You can review OpenAI’s privacy policy at this link https://openai.com/policies/privacy-policy/.

Grafana

Grafana is used to monitor and visualize system performance and application metrics. It processes

- log and telemetry data to generate real-time insights and dashboards.

Data handled by Grafana are kept secure through stringent access controls and encryption methods. You can review Grafana’s privacy policy at this link https://grafana.com/legal/privacy-policy/.

4. Data Workflow

4.1. Data Ingestion

Data is collected directly from users during account creation, ensuring that we capture only the essential information necessary for providing our services.

- During registration, the only data we collect are the **user's first and last names**. Additionally, our authentication provider, Auth0, collects the **user's email address**, which we can view but do not process in any other way. This email is securely stored.
- Users also have the option to add or update personal data in their profiles, ensuring our records remain dynamic and current. This may include uploading a **profile picture**, specifying **their organizational affiliation**, and indicating **their role** within AlterlandHub. While this information is securely stored, we do not process it further.
- In our SmartNote service, we collect **users' voice data** for the purpose of further processing to create smart notes. That voice data are not stored, we only store created **smart notes** and do not process that.
- Using our launcher, users can upload a **photo** to create a personalized avatar by AvatarSDK.
- Users also have access to our drive service, where they can store files, including file types such as **JPG, PNG, MP4 and PDF**. We do not process it further.

All data are handled securely, with privacy and security maintained throughout the process.

4.2. Data Processing

Users' voice data are processed through OpenAI and is used exclusively within our Smart Note service. Additionally, when users upload a **photo for avatar creatio**n, this image is processed by AvatarSDK to generate a personalized avatar. Apart from meeting data and avatar photo processing, user data is stored without further processing, thereby reducing the risk of data corruption or unauthorized alterations. This approach ensures that data integrity is maintained while allowing for efficient data utilization and secure storage.

4.3. Data Storage

Database backups are performed daily and are retained for up to 7 days, ensuring that recent data can be recovered in the event of a failure. This daily backup routine helps to mitigate the risks of data loss due to hardware failures, software issues, or cyber-attacks. It is important to note that file backups are not included in our current data storage strategy, focusing our efforts on protecting and preserving database integrity.

4.4. Data Sharing

Files within the system can be accessed by anyone who possesses the appropriate URI (Uniform Resource Identifier), highlighting the need for careful management and distribution of these URIs. This sharing mechanism provides ease of access and collaboration, but also necessitates strict controls and user awareness to prevent unauthorized access. To enhance security, we advise users to only share URIs with trusted parties and to regularly review access permissions.

4.5. Third-Party API Usage

We share data judiciously with trusted service providers like Auth0, AWS and through integrations with OpenAI API for data processing, within our corporate group for operational purposes, and with law

enforcement as mandated by law. Our sharing practices are guided by strict protocols to ensure data security and privacy.

4.6. Data Collection for Performance Monitoring

In our continuous effort to optimize the performance of our application, we collect anonymized data regarding users' devices, including specifications such as RAM, CPU, GPU and operating system version. This data is utilized solely for the purpose of identifying and analyzing performance issues on various devices. It is important to note that this information is not linked to any individual user and remains entirely anonymous. This approach ensures that we can improve the application's efficiency and user experience while maintaining the highest standards of user privacy and data protection.

5. Security Measures

For secure software deployment, we implement best practices for secure configurations, enforce data encryption both in transit and at rest, and actively monitor our software for unusual activities. Our deployment pipeline, powered by tools like AWS CDK, integrates continuous integration and continuous delivery (CI/CD) with automated testing to identify security issues prior to deployment.

5.1. Encryption Technologies

5.1.1. Data at Rest

Our databases are encrypted by default using the Advanced Encryption Standard with a 256-bit key (AES-256), which is recognized as one of the strongest encryption standards available. Similarly, all files stored in Amazon S3 are automatically encrypted with AES-256, ensuring robust protection for stored data. Additionally, user data managed through Auth0 is also encrypted, adding an extra layer of security to sensitive personal information.

5.1.2. Data in Transit

To safeguard data as it travels across networks, each API service employs AES-128-GCM encryption. This method ensures that data remains secure during transmission, protecting it from interception or unauthorized access. AES-128-GCM provides a balance of strong encryption and performance, making it suitable for real-time data transmission needs.

5.2. Authentication and Authorization

5.2.1. Adaptive Authentication

Adaptive authentication is implemented to dynamically adjust security measures based on user behavior and risk factors. This means that additional authentication steps may be triggered in response to unusual login patterns or other indicators of potential threats. By using adaptive authentication, we can enhance security while maintaining a user-friendly experience by applying stronger measures only when necessary.

5.2.2. Role-Based Access Control (RBAC)

AlterlandHub operates on a Role-Based Access Control (RBAC) system, which centralizes and streamlines the management of user permissions across the platform. RBAC allows us to assign

access rights based on user roles, ensuring that individuals have only the necessary permissions for their duties. This method simplifies access control, reduces administrative overhead, and minimizes the risk of unauthorized access by adhering to the principle of least privilege.

5.3. Third-Party Security Vendors and Integrations

5.3.1. OAuth Providers

We share data judiciously with trusted service providers like Auth0, AWS and through integrations with OpenAI for data processing, within our corporate group for operational purposes, and with law enforcement as mandated by law.

6. Endpoint Security

6.1. User Data Input Endpoints

Every front-end feature that requires user input is linked to a dedicated API endpoint, ensuring a structured and secure handling of user data. These endpoints are meticulously designed to manage specific user interactions, facilitating seamless and efficient data processing. By segregating input endpoints, we can better monitor and control data flow, enhancing both performance and security.

6.2. Endpoint Protection Measures

To safeguard our endpoints, we employ a multi-layered security approach incorporating robust measures such as strong authentication and authorization protocols to ensure only verified users can access the system, a Web Application Firewall (WAF) to filter and monitor HTTP requests and block malicious traffic, and Role-Based Access Control (RBAC) to manage user permissions effectively, ensuring users access only necessary data and resources, thus maintaining strict access controls and enforcing the principle of least privilege across the platform.

7. Compliance and Regulatory Adherence

At Alterland, we place a significant emphasis on compliance with essential regulations and standards that are vital for safeguarding our clients' data and ensuring the security of our systems and services. Adhering to these regulations is a critical component of our risk management strategy and is instrumental in building trust with our users and business partners.

7.1. GDPR Compliance

Alterland adheres to the General Data Protection Regulation (GDPR), implemented by the European Union to protect the personal data of EU citizens. Our commitment to GDPR compliance encompasses a comprehensive range of actions and procedures designed to protect personal data and ensure transparency in its processing.

Before processing any personal data, we obtain explicit consent from our users. We inform them of the purposes for which their data will be processed and provide them with the option to withdraw their consent at any time. In case of a breach, we notify the relevant supervisory authorities and, where necessary, the individuals affected. We provide ongoing training for our employees on data protection

and GDPR compliance to ensure that everyone is aware of their responsibilities and best practices in this area.

8. Continuous Security Monitoring and Improvement

8.1. Security Information and Event Management (SIEM)

In the near future, our system will incorporate Grafana for advanced data visualization and monitoring. Grafana will enable us to create dynamic, real-time dashboards that visualize security metrics and system performance, providing a comprehensive view of our security posture. By integrating SIEM capabilities with Grafana, we aim to enhance our ability to detect, analyze, and respond to security incidents efficiently.

8.2. Continuous Security Assessment

We employ continuous security assessment practices to monitor and evaluate the security of our systems on an ongoing basis. This involves real-time tracking of network activities, user behaviors, and system operations to identify any anomalies or potential threats. Through proactive monitoring, we can swiftly address security issues before they escalate, ensuring the integrity and reliability of our services.

8.3. Vulnerability Management

As part of our Vulnerability Management strategy, all software packages are regularly updated to address known vulnerabilities and enhance system security. Regular updates ensure that we benefit from the latest security patches and improvements, reducing the risk of exploitation. However, it is important to note that we do not currently operate a formal security vulnerability reporting system, which may be a future area for development to further bolster our security framework.

9. User Privacy and Data Protection

9.1. Privacy Policy

We have established a comprehensive Privacy Policy that outlines our practices regarding the collection, use, and protection of personal data. This policy is available at the following link: Privacy Policy. The Privacy Policy provides detailed information on how we handle user data in compliance with applicable data protection regulations, ensuring transparency and trust.

9.2. Data Minimization

We adhere to the principles of data minimization, collecting only the data necessary for the specified purposes. By limiting data collection to what is essential, we reduce the risk of data exposure and enhance privacy.