PRIVACY POLICY AND NOTICE AT COLLECTION
Effective Date: Sept. 3, 2024

Visualhawk Solutions Inc., a Canada federal corporation ("Visualhawk Solutions", "we," "us," "our," and their derivatives) provides Scotty VR™ and other video games, including any playtest program (collectively, our "Games"), websites, including https://www.scotty.game/ and https://www.visualhawksolutions.com/ and their respective subdomains (collectively, our "Websites"), and other online services (with our Games and Websites, collectively, our "Services").

1. **What does this Notice cover?**
This Privacy Policy and Notice at Collection (this "Notice") sets forth how we collect, use, protect, store, disclose, and otherwise process your Personal Information (defined below). This Notice does NOT apply to information you provide to any third party or is collected by any third party (except as otherwise provided below).
By using our Services, you are confirming that you understand English well enough to understand this Notice. Should you have questions about this Notice, please contact us by emailing us at admin@visualhawksolutions.com, so we can clarify and address your questions.

2. How do we process Children's Personal Information?
In accordance with the policies of Meta®, our Games are available to Quest Pro, Quest 2, Quest 3, and next-gen headset exclusively to users of minimum 13 years of age and older.
If you become aware that an underage user has provided us with Personal Information, please contact us by emailing us at admin@visualhawksolutions.com, so we may delete their Personal Information.

3. What categories of Personal Information do we collect?
(a) We are collecting data exclusively for running, supporting and maintaining the content of our Games in order to provide or improve the experience to the end user requesting the Content and from whom the User Data was collected;

(b) We are conducting analytics pertaining to our Games, and using such insights to improve your our Games, such insights are aggregated, de-identified, or anonymized such that we cannot identify individual users or devices from the analytics, and

(c) We are complying with applicable laws and regulations.

In addition, we are using Meta® Horizon User Data (which does not include Device User Data) solely for the following purpose:

(a) As permitted by applicable law, we are providing our users with information about or the opportunity to obtain new or existing features or functionality in a Game such user has purchased from us, or other applications being offered by your Visualhawk Solutions Inc. or Affiliate (as defined in the Developer Distribution Agreement).

Games
When you play our Games, we may process your:
• Identifiers: usernames (Game username), email address, unique or online ID (such as a third party ID from Oculus), Internet Protocol address, and hardware ID and hardware information;
• Geolocation: country;
• Commercial information: purchase history of in-game items and DLCs;
• Internet or other similar network activity: gameplay information, Game settings, and user preferences and language;
• Audio, electronic, visual, thermal, olfactory, or similar information: movement data (tracking your hands and head) and voice data; and
• Other: Oculus age category (i.e., teen, or adult) and information from the content that you send to us directly by submitting a support ticket.

4. From what sources do we collect Personal Information?
Directly From You
We may collect your Personal Information when you provide it to us directly, including the examples below.
• When you create an account for our Games, we may collect your username and Internet Protocol address.
• When you play our Games, we may collect your movement data (tracking your hands and head) and voice data.
• When you submit a support ticket, we may collect your email address, and records and copies of your correspondence.
• When you respond to a survey or questionnaire, we may collect the information you provide.

Automatically From You
We may collect your Personal Information automatically as you use our Services. For example, we may collect your Personal Information as you interact with our Websites or as you play our Games. For more information about our and third parties' use of cookies and other automatic data collection technologies and certain choices we offer to you with respect to them, please see Section 5 below.

From Third Parties
We may receive your Personal Information from or through third parties that help us provide or facilitate your access to our Services. For example, we may receive your Personal Information from the below third parties.
• Game publishers such as Meta®, : When you play our Games, we may receive your Oculus age category (i.e., teen, or adult), email address, gameplay information, Game settings, and user preferences and language. By way of another example, when you submit a support ticket, we may receive your Oculus ID.
• Social media platforms such as Discord®: When you join our Game Discord channel, we may receive your Discord username, user ID, and the information that you share publicly on our Discord channel.
We abide by this Notice when we use Personal Information provided to us by third parties. However, we may not control the Personal Information that third parties collect or how they use that Personal Information. You should review the third parties' privacy policies for more information about how they collect, use, and share the Personal Information they obtain and use.

5.What categories of Personal Information we do not collect?
We will not perform, or facilitate or support others in performing, any of the following prohibited

practices (collectively, “Prohibited Practices”):

5.1 We do not retain, use, or disclose User Data for any purpose other than those described in section 4, the Meta® Privacy Policy, the SDK License Agreement, the allowed use cases of Meta® Horizon User Data described at the following link: https://developer.oculus.com/resources/publish-data-use/#duc-feature-reference and any other applicable agreements with Meta®;

5.2 We are not using User Data for marketing or advertising purposes other than those explicitly permitted in Section 4;

5.3 We are not selling, licensing, purchasing, renting, or lending User Data or similar actions, or permitting a third party to do so;

5.4 We are not using User Data to profile, discriminate, or encourage discrimination in a manner that disadvantages people based on their race, ethnicity, color, national origin, religion, age, sex, sexual orientation, gender identity, family status, disability, medical or genetic condition, or any other categories protected by applicable law, regulation, or other Meta® terms or policy. We are using User Data such as age group only to improve the user experience in our Games only when and where is compliant with applicable law or regulation;

5.5 We are not using User Data to perform, facilitate, or provide tools for surveillance nor for the collection, use, or sharing of information about people, groups, places or events for law enforcement, national security, intelligence or counter-intelligence purposes;

5.6 We are not using User Data to ascertain the identity of a natural person, including real name, or actual facial or body images, to the extent not disclosed by the User Data (for example, through use of AI, facial recognition or gait identifying technologies);

5.7 We are not combining User Data with any other data, including with data separately collected by you or received from a third party other than those explicitly permitted in Section 4;

5.8 We are not attempting to decode, circumvent, re-identify, de-anonymize, unscramble, unencrypt, reverse hash, or reverse engineer User Data that is provided to you;

5.9 We are not using User Data in any manner or for any purpose that infringes, misappropriates, or otherwise violates any intellectual property rights or other rights of any person, or that violates any applicable law or regulation;

5.10 We are not accessing or collecting User Data or allowing User Data to be collected using automated means such as harvesting bots, robots, spiders, or scrapers; or

5.11 We are not sending or submitting Device User Data (which does not include Meta® Horizon User Data) to Meta® through any of Meta®'s business tools or products, including Meta®'s Ads or Analytics tools or products.

6. How do we and third parties use cookies and other automatic data collection technologies?
Cookies are small pieces of text sent to your browser by a website you visit. They help that website remember information about your visit, which can both make it easier to visit the site again and make the site more useful to you.

Our Cookies and Other Automatic Data Collection Technologies
We may use cookies and other automatic data collection technologies on our Services to collect Personal Information, for example, regarding your interaction with our Websites. By way of another example, when you play our Games, we may automatically collect your Internet Protocol address, gameplay information, and user preferences.
Third Party Cookies and Other Automatic Data Collection Technologies
Cookies and other automatic data collection technologies on our Services may come from third parties as listed below. These cookies and other automatic data collection technologies improve your experience by helping us better tailor our Services to you.
• Google Analytics® and YouTube®: Google Analytics is a web analysis service and YouTube is a video sharing and social media platform of Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States. The Personal Information collected by Google in connection with your use of our Websites is transmitted to a server of Google in the United States, where it is stored and analyzed. Google's collection and use of Personal Information is subject to Google's privacy policy: www.google.com/policies/privacy/partners/.

Choices about Cookies
You may set your browser to refuse all or some browser cookies or to alert you when cookies are being sent (for Google: https://tools.google.com/dlpage/gaoptout). Please note that, if you disable or refuse cookies or other automatic data collection technologies, some aspects of our Services may be inaccessible or not function properly.

7. Data release to law enforcement agencies
In furtherance of legal and safety objectives: We may access, use, and share with others your Personal Information for purposes of safety and other matters in the public interest. We may also provide access to your Personal Information to cooperate with official investigations or legal proceedings (e.g., in response to subpoenas, search warrants, court orders, or other legal processes).
• In connection with a sale or other transfer of our business: In the event all or some of our assets are sold, assigned, or transferred to or acquired by another company due to a sale, merger, divestiture, restructuring, reorganization, dissolution, financing, bankruptcy, or otherwise, your Personal Information may be among the transferred assets.
• As we may describe to you when collecting your Personal Information: There may be other situations when we collect your Personal Information and simultaneously describe the purpose for that collection.

Lawful Basis
We only collect, use, or store your Personal Information for a lawful basis such as:
• you voluntarily provide it to us with your specific, informed, and unambiguous consent (for example,

through our Game Discord channel);
• it is necessary to provide you with a Service that you have requested (for example, providing you access to our Games);
• we have a legitimate business interest that is not outweighed by your privacy rights (for example, to ban users); or
• it is necessary to protect your vital interests or the vital interests of others (for example, where necessary to protect the safety of one of our users or someone else).

8. In what situations do we disclose your Personal Information?

We may disclose your Personal Information to a third party, such as a service provider or contractor for a business or operational purpose, or with your consent. When we disclose Personal Information for a business or operational purpose, we enter into a contract with the service provider or contractor that describes the purpose and requires the service provider or contractor to both keep that Personal Information confidential and not use it for any purpose except performing the contract. These service providers and contractors include our:
• backend platform service providers such as for error and crash reporting;
• email service providers;
• game analytics providers; and
• customer support representatives and providers.
We may also disclose your Personal Information:
• to our subsidiaries and affiliates;
• to our lawyers, consultants, accountants, business advisors, and similar third parties who owe us duties of confidentiality;
• to a buyer or other successor in the event of a sale, merger, divestiture, restructuring, reorganization, dissolution, or other transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which Personal Information retained by us pertaining to the users of our Services is among the assets transferred;
• to comply with any court order, law, or legal process, such as responding to a government or regulatory request;
• to enforce any contract we may have in effect with you;
• if we believe disclosure is necessary or appropriate to protect the rights, property, or safety of us, our users, or others; and
• if you have consented to such a disclosure.
We do not sell, rent, or share your Personal Information for cross contextual behavioral or targeted advertising, automated decision-making, or profiling purposes.

9. How is my Personal Information protected?

Our Retention, Purpose Limitation, and Security Policies
We protect your Personal Information through a combination of collection, security, and retention policies.
• Limited retention: We retain each category of Personal Information only for as long as necessary to fulfill the purposes for which the Personal Information was provided to us or, if longer, to comply with any legal obligations, to resolve disputes, and to enforce contracts. To determine the appropriate retention period for Personal Information, we consider the amount, nature, and sensitivity of the Personal Information, the potential risk of harm from unauthorized use or disclosure of the Personal Information, the purposes for which we process the Personal Information and whether we can achieve those purposes through other means, and the applicable legal requirements. For example, subject to the foregoing considerations, it is our policy to delete your Personal Information if we stop operating our Games or the feature through which the Personal Information was acquired.

• Purpose limitation: We will use your Personal Information only for our Services you choose to access and for the purposes notified to you, unless we otherwise obtain your consent. We limit the collection of Personal Information to what is adequate, relevant, and reasonably necessary for those purposes.
• Security measures: We use reasonable security measures to ensure a level of security appropriate to the volume and nature of Personal Information processed and risk involved, considering the size, scope, and type of our business, and have implemented technical, administrative, and physical security measures designed to protect your Personal Information from unauthorized access, disclosure, use, and modification. As part of our privacy compliance processes, we review these security procedures on an ongoing basis to consider new technology and methods as necessary. However, please understand that our implementation of security measures as described in this Notice does not guarantee the security of your Personal Information. In the event of a security breach, we will notify the proper regulatory authorities and any affected users of the breach within 72 hours after we become aware of the breach to the extent required by applicable law.

Your Practices and Activities

Your practices and activities are likewise very important for the protection of your Personal Information. You should take certain steps to help protect your Personal Information, such as being mindful of what you share publicly in our Games or Game Discord channel, including the below.
• Do not use your real name when selecting a username.
• Do not share your real name or anything private about yourself or anyone else with other users of any Game or Game Discord channel.
• Do not pick a password that is easy to guess, and do not share your password.

Please remember that we have no control over what other users do with the content of your communications and no responsibility or obligation regarding other users.

10. How do we treat Personal Information transferred to the Canada?

Place of Business

We may store or process your Personal Information outside of the country where we collect the information or the country in which you reside. Our primary place of business is in the Canada. You should understand that we may transfer some or all of your Personal Information to the Canada to carry out certain operational and processing needs as described in this Notice.

Transfer Mechanisms

When transferring Personal Information out of foreign countries, we implement technical, organizational, and physical safeguards to protect your Personal Information. Please contact us if you have questions related to the relevant transfer mechanism for your Personal Information.

11. What rights do you have to your Personal Information?

Right to Access, Correct, Delete, or Restrict Processing

Subject to any limitations and exceptions under applicable law, you have the right to request access to your Personal Information and exercise the below rights.
• You have the right to correct or update certain types of Personal Information. In many cases, you can review or update your account information by accessing your account online.
• You have the right to request deletion of your Personal Information. If you choose to have your Personal Information removed from our Services, we will carry out your request within 7 days of account verification, subject to extension, and we will only retain minimal Personal Information to document your request and the actions we took to carry out your request.
• You have the right to restrict certain processing of your Personal Information and the right to object to some types of processing of your Personal Information.
• You have the right to withdraw your consent at any time.
• You have the right to lodge a complaint regarding our collection, storage, or processing of your

Personal Information with a data protection supervisory authority in the country where you live or work.
We will comply with your requests in accordance with, and subject to, applicable law. For example, we are not required to delete your Personal Information if we have an overriding legitimate ground for retaining that information, such as to prevent fraud. Please note that we are legally prohibited from carrying out requested actions in some instances, including (1) when we are unable to confirm your identity or (2) where doing so would adversely affect the rights or freedoms of others. Further, we are not required to carry out a requested action in some instances, including where the request is considered excessive.

We are Here to Help
Please email us at admin@visualhawksolutions.com with the subject line "Privacy Request" if you would like to exercise any of the rights described above or if you have questions regarding your rights.

12. How to delete your Personal Information
You have the right to request deletion of your Personal Information. If you choose to have your Personal Information removed from our Services, your request will be respected and actioned upon, regardless of the circumstance, unless otherwise required by law.
To have your Personal Information deleted send an email request to : admin@visualhawksolutions.com with the text "Personal Information delete request" in the subject line.

13. Additional Notice for California, Colorado, Connecticut, Utah, and Virginia Residents
California Online Privacy Protection Act
The following applies to California residents:
• We do not track users of our Services over time and across third party websites or online services and therefore do not respond to Do Not Track signals. We are not aware of any third party that tracks users of our Services over time and across third party websites or online services. Please note that Do Not Track is a different privacy mechanism than the Global Privacy Control, a legally recognized browser-based control that indicates whether you would like to opt out of the processing of your Personal Information for certain purposes.

California Shine the Light Law
The following applies to California residents:
• California residents may request information from us concerning any disclosures of Personal Information we may have made in the prior calendar year to third parties for direct marketing purposes. If you are a California resident and you wish to request information about our compliance with this law or our privacy practices, please contact us by emailing us at admin@visualhawksolutions.com.

State Privacy Laws
The following applies to California, Colorado, Connecticut, Utah, and Virginia residents (in the event of a conflict between this Section 11 and any other section in this Notice, this Section 11 controls):
• Right to Know and Access: You have the right to request that we disclose certain information to you about our collection and use of your Personal Information. Once we receive and confirm your verifiable consumer request, we will disclose to you the following, to the extent retained by us:
o the categories of Personal Information we collected about you;
o the categories of sources for the Personal Information we collected about you;
o our business or commercial purpose for collecting, selling, or sharing that Personal Information;

o the categories of third parties with whom we disclose that Personal Information;
o the specific pieces of Personal Information we collected about you (also known as a data portability request); and
o if we sold or shared your Personal Information, two separate lists disclosing (1) sales, identifying the Personal Information categories that each category of recipient purchased, and (2) disclosures for a business or operational purpose, identifying the Personal Information categories that each category of recipient obtained.
• Right to Deletion: You have the right to request that we delete any of your Personal Information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we will delete (and direct our service providers and contractors to delete) your Personal Information from our records, unless an exception under applicable law applies. We may deny your deletion request if retaining the information is necessary for us or our service providers or contractors to:
o complete the transaction for which we collected the Personal Information, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide our Services that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you;
o help to ensure the security and integrity of our Services to the extent the use of your Personal Information is reasonably necessary and proportionate to those purposes;
o debug our Services to identify and repair errors that impair existing intended functionality;
o exercise free speech, ensure the right of another user to exercise their free speech rights, or exercise another right provided for by law;
o comply with the California Electronic Communications Privacy Act;
o engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the Personal Information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided consent;
o enable solely internal uses that are reasonably aligned with user expectations based on your relationship with us and compatible with the context in which you provided the Personal Information; or
o comply with a legal obligation.
• Right to Correction: You have the right to request that we correct inaccurate Personal Information. Once we receive and confirm your verifiable consumer request, we will use commercially reasonable efforts to correct the inaccurate Personal Information, taking into account to the nature of the Personal Information and the purposes of the processing of the Personal Information.

No Discrimination

We will not discriminate against you for exercising any of your privacy rights under applicable law. Unless permitted by applicable law, we will not:
• deny you our Services;
• charge you different prices or rates for our Services, including through granting discounts or other benefits, or imposing penalties;
• provide you a different level or quality of our Services; or
• suggest that you may receive a different price or rate for our Services or a different level or quality of our Services.

Verifiable Consumer Requests

To exercise your rights described above, please c email us at admin@visualhawksolutions.com with the subject line "State Privacy Rights." Only you, or someone legally authorized to act on your behalf, may

make a verifiable consumer request related to your Personal Information. The verifiable consumer request must:

• provide sufficient information that allows us to reasonably verify you are the person about whom we collected Personal Information or an authorized representative; and

• describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with Personal Information if we cannot verify your identity or authority to make the request and confirm that the Personal Information relates to you. We will only use Personal Information provided in a verifiable consumer request to verify your identity or authority to make the request.

Response Timing and Format

We endeavor to respond to a verifiable consumer request within 45 days of its receipt. If we require more time, we will inform you of the reason and extension period in writing. If you have an account with us, we will deliver our written response to that account. If you do not have an account with us, we will deliver our written response by mail or electronically, at your option.

Any disclosures we provide will only cover the 12-month period preceding the receipt of verifiable consumer request, unless you request a longer period of time for Personal Information we collected about you after January 1, 2023. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

To appeal a decision regarding your verifiable consumer request, please submit your appeal using one of the two methods above. Your appeal should include an explanation of the reason you disagree with our decision. Within 60 days of receipt of an appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions.

For data portability requests, we will select a format to provide your Personal Information that is readily usable, easy-to-understand, and should allow you to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

14. How will we notify you of changes to this Notice?

We reserve the right to change this Notice from time to time consistent with applicable law. If we make changes to this Notice, we will notify you by revising the date at the top of this Notice and provide you with additional notice such as an in-Game notice or email notification.

15. How can you contact us?

If you have questions, email us at admin@visualhawksolutions.com

If you are a law enforcement agency, please email us at admin@visualhawksolutions.com with your request for Personal Information with the subject line “Law Enforcement Request.”

To have your Personal Information deleted send an email request to : admin@visualhawksolutions.com with the text “Personal Information delete request” in the subject line.

Sure! Here’s a sample add-on for your Oculus VR game privacy policy tailored for compliance with European Community regulations, including GDPR. This section should be appended to your existing privacy policy. Note that it's always a good idea to have legal counsel review any privacy policy to ensure full compliance with local laws and regulations.

Addendum for the European Community

1. Introduction

This addendum is designed to provide additional information specific to users located in the European Community (EC) in compliance with the General Data Protection Regulation (GDPR) and other applicable data protection laws. It supplements our general privacy policy and outlines how we collect, use, and protect your personal data in accordance with European regulations.

2. Data Controller

For the purposes of GDPR, the data controller responsible for your personal data is:

Visualhawk Solutions Inc.

21 Kenilworth Rd.

Brampton, ON, L6V2B2

Canada

Email address for querries: admin@visualhawksolutions.com

3. Legal Basis for Processing

We process your personal data based on the following legal grounds:

- **Consent:** Where you have given us explicit consent to process your data for specific purposes.
- **Contractual Necessity:** To perform our obligations under the terms of service or any agreements with you.
- **Legitimate Interests:** Where processing is necessary for our legitimate interests, provided these do not override your rights and freedoms.
- **Legal Obligation:** Where processing is required to comply with a legal obligation.

4. Data Collection

We may collect and process the following categories of personal data:

- **Identifiable Information:** Such as your email address, and account details.
- **Technical Data:** Including IP addresses, device identifiers, and usage data related to your interaction with our VR game.
- **Usage Data:** Information on how you use our services, including interactions and preferences within the game.

5. Data Sharing and Transfers

- **Third-Party Service Providers:** We may share your data with trusted third-party service providers who assist us in operating our services, provided they are bound by confidentiality obligations.
- **International Transfers:** If your personal data is transferred outside the European Economic Area (EEA), we ensure that appropriate safeguards are in place, such as Standard Contractual Clauses approved by the European Commission.

6. Data Retention

We will retain your personal data only for as long as necessary to fulfill the purposes outlined in our privacy policy or as required by law. Specific retention periods are as follows:

- **Account Information:** Retained for the duration of your account activity and for a period of [specify period] after account deletion.
- **Usage Data:** Retained for [specify period] to analyze and improve our services.

7. Your Rights

Under GDPR, you have the following rights regarding your personal data:

- **Right to Access:** Request access to your personal data and obtain a copy of it.
- **Right to Rectification:** Request correction of inaccurate or incomplete data.
- **Right to Erasure:** Request deletion of your personal data where it is no longer necessary or if you withdraw your consent.
- **Right to Restrict Processing:** Request restriction of processing under certain circumstances.
- **Right to Data Portability:** Request transfer of your data to another data controller in a structured, commonly used, and machine-readable format.
- **Right to Object:** Object to processing based on legitimate interests or direct marketing.

To exercise these rights, please contact us at admin@visualhawksolutions.com. We will respond to your request within the timeframe required by GDPR.

8. Data Security

We implement appropriate technical and organizational measures to protect your personal data from unauthorized access, disclosure, alteration, and destruction. These measures are reviewed and updated regularly to maintain high standards of security.

9. Complaints

If you believe we have not complied with GDPR, you have the right to lodge a complaint with the relevant data protection authority in your country of residence.

10. Changes to This Addendum

We may update this addendum from time to time to reflect changes in our practices or legal requirements. Any updates will be posted on our website, and we will notify you of significant changes.