i3 Face Recognition Acceptable Use Policy (AUP)

Rev. 250827

This Acceptable Use Policy ("AUP") is incorporated by reference into your Master Software License Agreement or Master Services Agreement, as applicable ("Agreement").

Your right to use the i3 International Inc. / i3 America Nevada Inc. (Collectively “i3”) Software or Services may be suspended or terminated for violating this AUP under your Agreement.

Capitalized terms used in this AUP shall have the meaning given in your Agreement.

You may not use i3 International Inc./ i3 America Nevada Inc.'s Software or Services to engage in, foster, or promote abusive or irresponsible behavior or in a manner that is not in compliance with all applicable local, state, tribal, national, and international laws, rules, and regulations, including any relating to consumer protection and/or privacy.

The preceding includes, without limitation, using any data gathered using the Software or Service to assist in:

- Establishing an individual's eligibility for personal credit, loans, insurance, or assessing risks associated with existing consumer credit obligations.
- Evaluating an individual for employment, promotion, reassignment, or retention
- Evaluating an individual for education opportunities, scholarships, or fellowships
- Evaluating an individual's eligibility for a license or other benefit granted by a government agency or evaluating an individual in connection with any other product, service, transaction, or any other manner that violates applicable laws.

You may not use the Software or Service in any manner that does or is intended to:

- Cause emotional or physical harm to, discriminate against, "stalk," or otherwise harass any other person.
- Seek information about or harm minors in any way.
- Seek information about celebrities or public figures.
- Produce or distribute any defamatory, obscene, or other material that is or could be considered inappropriate.
- Infringe upon any third party's legal or proprietary rights, including any intellectual property, publicity, privacy, or any other right.
- Otherwise, use any aspect of the Software or Service for unlawful or illegal purposes.

You may not disclose data you gather using the Software or Service except for disclosures to your employees, consultants, law enforcement, a court, or a legally entitled agency that requires access to such information to perform duties or exercise rights under this AUP and are bound to confidentiality obligations.

i3 International Inc. / i3 America Nevada Inc. may audit or monitor your compliance with these requirements.

Tel: 1.866.840.0004

i3 Face Recognition Privacy Policy

Rev. 250827

At i3 International Inc./ i3 America Nevada Inc., we are committed to protecting the privacy and ensuring the security of your personal information, including any data collected through our face similarity technology. This i3 Face Recognition Privacy Policy outlines how we collect, use, disclose, and protect your facial data in compliance with applicable laws and regulations.

1. Collection of Facial Data

i3 International Inc. / i3 America Nevada Inc. collects or stores facial data through automated means when the system interacts with our applications, devices, or services.

- **Data Minimization:** We collect only the facial data necessary for the intended purpose and retain it only for as long as necessary as the user requests.
- The i3 Face Recognition system allows users to capture, store, and analyze facial data for security, access control, and operational purposes.
- This data may be retained for a period of days, weeks, or months, depending on the settings chosen by the system operator.

2. Responsibility for Data Protection

i3 provides the tools to capture and manage facial data, but the responsibility to safeguard and protect customer face data rests solely with the system operator (you, the user).

- You decide how long facial data is stored.
- You decide who has access to the data.
- You are responsible for implementing reasonable security measures (such as password protection, access controls, and encryption) to prevent unauthorized use or disclosure.

3. Use of Facial Data

We use facial data for the following purposes:

- **Identity Verification**: To verify the selected identity for authentication or authorization purposes.
- **Personalization**: To personalize your user experience, including customizing content, recommendations, or services based on facial data.
- **Improvement of Services**: To improve our products' and services' quality and functionality, including enhancing face similarity algorithms.
- **Security**: To enhance the security of our services and prevent fraudulent activities.

4. Disclosure of Facial Data

We may not disclose facial data except in the following circumstances:

- **Consent**: With your explicit consent, we may share facial data with third parties.
- **Legal Obligations**: We may disclose facial data to comply with applicable laws, regulations, or legal processes.
- **Service Providers**: We may share facial data with trusted third-party service providers who assist us in providing or improving our services.

i3's Role

- i3 does not access, use, or share the facial data stored on your system.
- i3 provides software updates and security patches to help maintain the integrity of the system.
- i3 is not liable for any misuse, unauthorized disclosure, or data breaches resulting from the user's failure to secure face data.

5. Data Security

We implement appropriate technical and organizational measures to protect facial data from unauthorized access, disclosure, alteration, or destruction. Utilize encryption, access controls, and other security technologies to safeguard the data.

User Responsibility: The operator is responsible for ensuring proper safeguards (passwords, access limits, encryption) are implemented.

Tel: 1.866.840.0004

6. Data Retention

We retain facial data only for as long as necessary to fulfill the purposes outlined in this policy or as required by law. We regularly review and delete facial data when it is no longer needed.
We limit facial data to the purposes for which it was collected and disclosed and do not use it for purposes unrelated to the original purpose without obtaining additional consent.

7. Legal & Regulatory Compliance

System operators must comply with all applicable privacy laws and regulations in their jurisdiction. This may include, but is not limited to:

- Obtaining consent from individuals whose facial data is collected.
- Notifying individuals of how long their data will be retained.
- Deleting facial data when it is no longer needed.

We follow compliance with relevant regulations governing the collection, use, and protection of facial data, such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other regional laws; including the potential impact on privacy, civil liberties, and social justice.

i3 International Inc./ i3 America Inc. proactively addresses concerns and mitigates any adverse effects.
We continue conducting regular audits and assessments of your i3 Face Recognition system to ensure compliance with legal requirements and industry best practices. Identify any potential risks or vulnerabilities and take corrective actions as needed.

8. Your Rights

You have the following rights regarding your facial data:

- **Access**: You have the right to access your facial data held by us and request information about its processing.
- **Correction**: You have the right to request correction of inaccurate or incomplete facial data.
- **Deletion**: You have the right to request deletion of your facial data under certain circumstances.
- **Withdrawal of Consent**: You have the right to withdraw consent to process your facial data at any time.

User Acknowledgement

By using i3 Face Recognition suite of products, you acknowledge and accept:

- That facial data is sensitive personal information.
- That you are fully responsible for the storage, retention, and protection of this data.
- That i3 is a technology provider and not the data controller or data custodian of the facial information collected by your system.

9. Children's Privacy

Our face similarity services are not intended for use by children under the age of 13. We do not knowingly collect facial data from children under 13 without parental consent.

10. Updates to this Policy

We may update this Face Similarity Privacy Policy from time to time. Any changes will be posted on our website, and we encourage you to review this policy periodically.

We do our best to follow compliance with relevant regulations governing the collection, use, and protection of facial data, such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other regional laws; including the potential impact on privacy, civil liberties, and social justice. i3 International Inc./ i3 America Nevada Inc. proactively addresses concerns and mitigates any adverse effects.

We continue conducting regular audits and assessments of your i3 Face Recognition system to ensure compliance with legal requirements and industry best practices. Identify any potential risks or vulnerabilities and take corrective actions as needed.

Tel: 1.866.840.0004

11. Contact Us

If you have any questions, concerns, or requests regarding this Face Similarity Privacy Policy or the processing of your facial data, don't hesitate to contact us at i3 International Inc./ i3 America Nevada Inc.

i3 International Inc.
780 Birchmount Rd, Unit 16, Toronto, ON M1K 5H4
Email Address: SecurityReport@i3international.com
Webform: https://i3international.com/contact-us
Tel.: 1.866.840.0004