Stealth(identity) uAuthenticator App Privacy Policy Addendum

Section 1 - Introduction

The purpose of this document (the "**Addendum**") is to provide an addendum to the privacy policy statement outlined in the Unisys Privacy Policy available at https://www.unisys.com/unisys-legal/privacy/ ("**Unisys Privacy Policy**"), specifically addressing the data handling practices within the Stealth(identity) uAuthenticator App ("**App**"). It aims to offer additional details regarding how data is captured, stored, managed, deleted, and protected within the App, thereby ensuring user trust and compliance with data protection regulations:

The purpose of this document is twofold:

1. **To Supplement Unisys Privacy Policy:** While the Unisys Privacy Policy provides a comprehensive framework for data protection across various Unisys products and services, this addendum focuses specifically on the data handling practices within the App. It aims to augment the existing policy by providing detailed insights into how user data is managed within the App.
2. **To Address App-specific Data Practices:** The scope of this addendum is limited to the App. It describes into specific aspects such as data capture, storage, management, deletion, and protection, offering users a detailed understanding of how their data is handled within the App environment.

By providing clear and transparent information regarding data handling practices, this Addendum seeks to empower users with the knowledge necessary to make informed decisions about their privacy and data security within the context of the App.

Section 2 – Data Capture

The App is used by customers to enroll and authenticate the biometric identity information of their individual users in conjunction with the Stealth(identity) Software (the "**Intended Purpose**"). The App captures data from individual users during registration, primarily full-frontal facial images and associated biometric templates ("**Facial Data**"), using the camera on the individual user's mobile device. The collection and use of Facial Data for the Intended Purpose is executed with user consent and adheres to the stringent privacy standards described in the section of the Unisys Privacy Policy entitled "How We Protect Your Personal Data".

Section 3 – Data Storage

After collection, Facial Data is securely encrypted and stored within customer-controlled Microsoft Azure ("**Azure**") databases. These databases are equipped with robust security measures to safeguard against unauthorized access or breaches, and to ensure data integrity and confidentiality.

Section 4 – Data Management

At Unisys, we recognize that effective data management is crucial for maintaining security, privacy, and compliance. Unisys's approach incorporates the following key practices:

4.1 Role-Based Access Control (RBAC):

RBAC assigns permissions based on predefined roles within the organization.

How It Works:

- **Roles:** Unisys defines roles (e.g., admin, manager, user) each of which has specific responsibilities and associated permissions (e.g., read, write, delete) concerning the Facial Data
- **Assignment:** Each individual user and customer administrator is assigned a role within the RBAC framework, based on their need to access and use the Facial Data for the Intended Purpose.
- **Access Control:** Users accessing the Facial Data can only perform the actions permitted by their assigned role.

4.2 Default Denial Principle:

Access to the databases containing Facial Data is denied by default unless explicitly granted.

Implementation:

- **Access Rules:** Unisys specifies rules that explicitly allow access to the Facial Data if certain conditions are met.
- **Implicit Deny:** Access to the Facial Data is denied if the applicable rule does not permit access, or if no rule applies.
- **Security First:** This approach prioritizes the security of the Facial Data over convenience.

4.3 Regular Audits and Usage Monitoring:

- Unisys conducts regular audits to ensure compliance with privacy regulations and industry standards.
- Usage monitoring helps Unisys detect anomalies and unauthorized access promptly.

By implementing RBAC, default denial, and regular audits and usage monitoring as described above, Unisys maintains a robust data management framework that safeguards sensitive information while enabling authorized users to perform their roles effectively.

Section 5 – Data Retention

Data retention policies within the App are designed to balance operational requirements with user privacy considerations. Unisys's approach to data retention includes the following key principles:

5.1 **Purpose Limitation:** Facial Data is only retained in the Azure databases for as long as it is necessary to fulfill the Intended Purpose. This includes the duration required to provide services to users, comply with legal obligations, resolve disputes, and enforce agreements.

5.2 **Retention Period:** The retention period for Facial Data varies depending on the specific context and purpose of data processing. Generally, Unisys retains Facial Data for the duration of the user's engagement with the App and as required by applicable laws or other contractual obligations. Upon the end of the user's enrollment with the App, Unisys coordinates with Azure to ensure the prompt deletion of the Facial Data from the Azure databases.

5.3 **Data Minimization:** Unisys practices data minimization by only retaining Facial Data that is relevant, adequate (e.g. only storing only facial templates), and necessary for the Intended Purpose. Unnecessary or outdated Facial Data is promptly identified and securely deleted to minimize the risk of unauthorized access or misuse.

5.4 **User Control:** Users have control over their Facial Data and can request the deletion or modification of their information as outlined in the Unisys Privacy Policy. Additionally, users are provided with options to manage their data preferences and consent settings within the App interface.

5.5 **Data Deletion:** Unisys prioritizes the secure deletion of Facial Data from the Azure databases when it is no longer necessary for the Intended Purpose. Facial images are discarded at the conclusion of specific transactions or authentication processes, while biometric templates are retained only for the duration of user registration. When Facial Data reaches the end of its retention period or becomes obsolete, templates are also deleted from our systems and the Azure databases using industry-standard methods to prevent unauthorized access or unintended disclosure. In addition, users retain control over their Facial Data and can request deletion through the App or web interface at any time.

5.6 **Data Backup and Archiving:** Unisys maintains secure backup and archiving processes to ensure the availability and integrity of Facial Data throughout its retention period. These processes adhere to stringent security protocols to protect Facial Data against loss, corruption, or unauthorized access.

5.7 **Regular Review and Update:** Unisys's data retention policies are subject to regular review and update to align with evolving legal requirements, industry standards, and best practices. Unisys regularly reviews and updates our data retention practices, ensuring they remain proportionate, transparent, and compliant with applicable regulations.

By adhering to these data retention principles, Unisys aims to strike a balance between fulfilling its operational needs and safeguarding user privacy within the App ecosystem.

Section 6 – Data Protection

Unisys is committed to data protection principles, including:

6.1 **Confidentiality:** Unisys ensures that user data remains confidential and is accessible only to authorized Unisys personnel with a legitimate need for access.

6.2 **Integrity:** Data integrity is preserved through encryption, secure storage, and regular audits to prevent unauthorized alterations or tampering.

6.3 **Availability:** Users can access their data whenever needed, while robust backup and recovery mechanisms ensure data availability even in the event of system failures or disruptions.

6.4 **Compliance:** Unisys adheres to relevant data protection regulations, including but not limited to GDPR and other applicable laws, to protect user rights and privacy.

6.5 **User Empowerment:** Unisys empowers users with transparency and control over their data, including the ability to review, modify, or delete personal information as desired.

Section 7 – Data Sharing

Unisys may share Facial Data with the following third parties, as necessary to accomplish the Intended Purpose:

- **With Unisys's contractors, agents, or business partners such as Azure,** so that they can perform services for Unisys, including generating biometric templates based on the Facial Data, performing identity verification services for the Intended Purpose, and storing the Facial Data in secure databases. Unisys does not authorize these third parties to use or disclose Facial Data except as necessary to perform services on our behalf or to comply with legal requirements. Such third parties only retain Facial Data for as long as necessary to fulfill the Intended Purpose.
- **With law enforcement authorities or other government officials** when (a) Unisys is required to do so by law or pursuant to legal process (including for national security purposes); (b) Unisys believes disclosure is necessary or appropriate to prevent physical harm or financial loss or in connection with an investigation of suspected or actual fraud or illegal activity; or (c) when Unisys believes that disclosure is necessary to protect our rights, protect user safety or the safety of others.
- **With appropriate third parties in connection with a sale or restructuring of the business**, such as a merger, acquisition, bankruptcy, or other sale of all or a portion of the Unisys's assets. In such an event, Unisys will use reasonable efforts to ensure the transferee uses Facial Data in a manner consistent with the Unisys Privacy Policy and this Addendum.

Section 8 – Customer Privacy Policies

Each customer has the option to implement their own privacy policy within the App. The App provides functionality to include the customer's privacy policy as part of the user consent screen. Typically, customers publish their privacy policy on their website for reference. Additionally, the App usage is restricted to users with a proper registration code. The App enables customer administrators to generate unique registration codes for their organization and share them

with end users, ensuring controlled access and compliance with organizational policies.

Section 9 – Integration with Unisys Privacy Policy

This Addendum seamlessly integrates with the Unisys Privacy Policy, providing additional clarity and detail specific to the App. Users are encouraged to review both documents to gain a comprehensive understanding of how their data is handled and protected within the App and broader Unisys ecosystem.

Section 10 – Changes to this Addendum

This Addendum may be updated periodically, and the updated version will be posted on the website, indicating when it was last updated. If there are material changes to this Addendum, Unisys will post a prominent notice on our website and/or provide other notice as required by law: