UK Digital Identity and Attribute Trust Framework (DIATF) Identity Verification Terms

These Product Terms govern Customer's use of the Certified Services and are incorporated by reference into the Agreement between Entrust and Customer. Capitalised terms in this Exhibit have the same meaning as in the Agreement, unless expressly defined otherwise in this Exhibit.

1. **Definitions.** The following capitalized terms shall have the meaning set forth below when used in this Schedule or any Annex (or Exhibit) attached hereto.

   a) "**Attribute"** means a piece of information that describes something about a person or an organization. A combination of attributes can be used to create a digital identity.

   b) "**Audit**" means the independent verification activity, such as inspection or examination of a product, process or service to ensure compliance to requirements with the DIATF framework.

   c) "**Certification**" means the written assurance by an independent third party, accredited by the UK Accreditation Service (UKAS), of the conformity of a product, process or service to specified requirements.

   d) **"Certified Service"** means the digital verification service provided by Entrust, as certified under the Trust Framework, that enables people to digitally prove who they are, information about themselves or their eligibility to do something.

   e) "**Component Service Provider**" means Entrust, an organization providing a service that specializes in designing and building components that can be used during parts of the identity proofing, verification or authentication processes.

   f) **"Complaints"** means expressions of dissatisfaction by Users regarding the Services experience.

   g) **"Compromised Account"** means an account that has been compromised if a thread actor has accessed it to perform actions using a gen

   h) **"Conformity Assessment Body (CAB)"** means a body accredited by the UK Accreditation Service (UKAS) to certify a product, process, or service to specified requirements. Approved trust framework conformity assessment bodies are accredited to undertake certification against the trust framework in keeping with ISO/IEC 17065.

   i) **"Digital Identity"** means a digital representation of who a user is. It lets them prove who they are during interactions and transactions.

   j) **"Identity Service Provider (IDSP)"** means Entrust, the organization providing a service that proves and verifies a user's identity for one off use at a single point in time.

   k) **"Incident(s)"** means security incidents, fraud events, integrity issues, availability issues, and any other events that could impact Users, Identity or Attribute Outputs, or the trustworthiness of the Services (including suspected compromise, misuse, or misconfiguration).

   l) **"Participant"** means a collective term to refer to all organizations that interact with the trust framework and participate in the wider digital identity and attributes market. This includes certified services and relying parties.

   m) **"Relying Party**" means the Customer (you) receiving the identity or attribute data from the IDSP under this Agreement.

   n) **"Service Retirement**" means that Entrust permanently discontinues, sunsets, or retires the Services or any material component thereof that is used for identity or attribute verification.

   o) **"Trust Framework"** means the UK Digital Identity and Attributes Trust Framework (gamma 0.4), a set of government approved rules, which draws mainly on existing standards, best practice and

legislation, that organizations agree to follow to have their service certified as a trustworthy digital verification service, available for reference at https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-04/uk-digital-identity-and-attributes-trust-framework-gamma-04-pre-release.

p) **"Trust Framework Withdrawal"** means that Entrust withdraws from, loses, suspends, materially limits, or does not renew its certification under the UK Digital Identity and Attributes Trust Framework (gamma 0.4).

q) **"User"** means an individual end user who accesses the Customer's services and whose identity or attribute data is verified or provided by the IDSP.

2. **Purpose; Acknowledgement of DIATF**

2.1. Acknowledgement. The Parties acknowledge that Entrust is (or intends to be) certified against the UK Digital Identity and Attributes Trust Framework (gamma 0.4) ("DIATF") and that, where Entrust works directly with Relying Party, Entrust must set out "flow down terms" to ensure the Relying Party supports Entrust in meeting the principles, requirements, and certification obligations of the DIATF.

2.2. The Relying Party agrees that, as a condition to consuming identities and attributes from the Certified Service, they shall:

i. Use the Certified Service only for the purposes and in the manner described in the Agreement and associated Documentation;

ii. Implement and maintain reasonable technical and organizational measures so that its own systems and processes do not undermine Entrust's ability to comply with the Trust Framework;

iii. Comply with this Schedule and any reasonable written instructions from Entrust that are necessary for Entrust to meet its certification obligations, provided such instructions are consistent with the Agreement.

2.3. No Relying Party Certification. Relying Party is not required to be certified under DIATF in order to consume digital identities and/or attributes but Relying Party will not take actions that undermine the DIATF principles as applied to the Services.

2.4. Order of Precedence. If there is a conflict between this DIATF Schedule and any other term of the Agreement, this DIATF Flow-Down schedule controls solely to the extent necessary to satisfy DIATF flow down requirements.

3. **Relying Party Obligations**

3.1. When using Entrust Certified Services, you confirm and agree that:

i. Understanding the DIATF. You have read the DIATF and understand the roles, responsibilities, and obligations applicable to you under it.

ii. Compliance with Framework. You will reference, apply, and comply with the framework in accordance with any applicable guidance or interpretive materials that we publish or otherwise make available from time to time.

iii. Fraud Management Cooperation. You will cooperate with Entrust in supporting the identification, prevention, and management of fraudulent activity arising from or in connection with the use of the Certified Services, including, where applicable, compliance with fraud management requirements and the operation and maintenance of appropriate information security systems.

iv. Responsibility. You acknowledge and accept full responsibility for all activities you carry out within your allocated responsibilities as between you and Entrust, as defined under this Agreement and the DIATF framework.

v. Fraud Signal Sharing. Promptly notify Entrust of any actual or suspected fraud or misuse that may be relevant to identities, attributes, or transactions processed via the Certified Service, providing all reasonably necessary contextual information and logs;

vi. Integrity of Fraud Controls. Not disable, bypass, or instruct Entrust to disable fraud controls or risk indicators within the Certified Service;

vii. Investigation Support. Cooperate with Entrust and relevant authorities, as reasonably required, in any investigation or remediation of suspected fraud linked to the Certified Service.

3.2. Risk Mitigation & Controls. Where Entrust flags an identity, credential or transaction as higher-risk pursuant to its fraud policies, the Relying Party shall apply any additional mitigations and controls that the parties have agreed on to address fraud risk which may include, but are not limited to, stepped up checks or manual review.

4. **Service Retirement & Trust Framework Withdrawal**

4.1. Provider Notification. Entrust shall notify the Relying Party in writing of any Trust Framework Withdrawal or Service Retirement, in support of the Trust Framework requirement to notify relying parties and allow reasonable migration planning (DIATF Section 11.9(a)(ii) and 11.9(b)).

4.2. Relying Party Obligations. Upon receipt of notice, and to the extent the Relying Party relies on the Services in connection with identity or attribute verification:

i. The Relying Party shall take reasonable steps, through its own user-facing channels, to notify affected end Users that identities and/or attributes provided via the Services are no longer being provided as a Certified Service or that the Services are being retired, as applicable, in support of the Trust Framework requirement to notify users on withdrawal (DIATF Section 11.9(a)(i) and 11.9(b));

ii. The Relying Party shall promptly cease any representation, statement, or implication (including in user interfaces, onboarding flows, marketing materials, or contractual documentation) that identities or attributes obtained via the Services remain certified by the Trust Framework; and

4.3. Transition and Migration Support. Following a Trust Framework Withdrawal or Service Retirement, the parties shall reasonably cooperate to support an orderly transition to mitigate user confusion or misuse of identity or attribute data and Entrust will provide the Relying Party with a reasonable period of time as detailed in the Service Termination Plan to migrate to alternative providers or solutions, where applicable (DIATF Section 11.9(a) and (b)).

4.4. Data Disposal, Retention. Upon completion of a Service Retirement, and subject to applicable law:

i. Entrust shall dispose of, delete, or anonymize data it holds in connection with the retired Services in accordance with its documented retention and disposal policies; and

ii. The Relying Party shall dispose of, delete, or anonymize identity or attribute data obtained via the retired Services in accordance with its own retention obligations and applicable law, in support of the Trust Framework data disposal requirements on service retirement (DIATF Section 11.9(b)).

4.5. Regulatory Notifications Reserved. The parties acknowledge and agree that notifications to the Office for Digital Identity and Attributes (OfDIA) and to any conformity assessment body are the

sole responsibility of Entrust, in accordance with Section 11.9(a)(iii) of the Trust Framework, and nothing in this Agreement requires the Relying Party to engage directly with regulators or certification bodies.

5. **Accurate Representation** *[DIATF § 11.1(b) and 4.2.1(e)]*

5.1. No Misleading Claims. Relying Party acknowledges that the Services may form only one component of Relying Party's broader user journeys, products, or processes. Relying Party shall not represent, or permit others to represent that its entire service, onboarding process, or user experience is certified under the DIATF solely on the basis that it uses Entrust's Certified Services for identity verification.

5.2. Limited and Accurate References. Any reference by Relying Party to Entrust's certification under the DIATF shall be 1) accurate, factual, and limited in scope solely to the specific Services provided by Entrust; 2) clearly distinguished from Relying Party's own systems, processes, and decision-making; and 3) not presented in a manner that could reasonably mislead Users, regulators, or third parties as to the extent of certification coverage.

5.3. No Endorsement. Relying Party shall not state or imply that its use of the Services constitutes endorsement, approval, or certification of Relying Party's broader services, controls, or compliance posture by Entrust or by the DIATF.

5.4. Remedies. If Entrust reasonably determines that Relying Party has made a misleading or inaccurate representation regarding DIATF certification that could undermine trust in the framework or Entrust certification status, Entrust may request that Relying Party take prompt correct action, which may include clarification or discontinuation of such representations.

6. **Complaints and Disputes Handling** *[DIATF § 2.2.4(b) and 11.2(a)-(c)]*

6.1. Documented Processes. Each party shall have in place policies and procedures for the resolution of complaints and disputes received from Users or other relying parties about the provisioning of the Certified Services and any other related matters ("Complaints and Disputes"), save that (i) the Customer will be responsible for providing direct first line support to Users in respect of any Complaints and Disputes; and (ii) Entrust will provide reasonable support to the Customer in respect of any Complaints and Disputes which the Customer is unable to resolve following its reasonable efforts under 6.1(i).

6.2. Accessibility. Entrust shall maintain publicly accessible information through which the Relying Party may raise complaints, inquiries, or other support requests relating to Entrust's Certified Services, including via Entrust's publicly available support page or privacy statement. Relying party shall likewise maintain accessible contact details for complaints or disputes relating to Relying Party's own services or user journey which shall include expected handling timelines and escalation processes, as appropriate.

6.3. Coordination. Where a complaint or dispute is received by Entrust, Entrust shall redirect the User to Relying Party as the first point of contact, in accordance with the complaint and dispute handling model and the agreed contact points as further described in this Section 6. Entrust shall reasonably cooperate, upon written request, to support any investigation and resolution to the extent directly related to the Certified Services

6.4. Regulatory Channels. Each Party shall retain appropriate records of complaints and disputes within its control. Where requested, Relying Party shall provide Entrust with relevant information relating to complaints or disputes connected to the Services to enable Entrust to respond to requests from the Office for Digital Identity and Attributes ("OfDIA") or a conformity assessment body in support of Entrust's certification and ongoing monitoring obligations.

7. **Identity Repair** *[DIATF § 2.2.6; 12.5.5]*

7.1. Identity Repair Support. Relying Party shall maintain a documented process to support Users who may be victims of identity theft in connection with transactions supported by the Services.

i. provide clear and easily accessible contact details through which Users may seek support for identity-related issues arising in Relying Party's services or user experience;

ii. include procedures to direct Users to appropriate identity repair steps, including advising Users to follow the Action Fraud identity fraud victims's checklist; and

iii. ensure that Users are not required to restart identity journeys unnecessarily where identity repair or investigation is already in progress.

7.2. Coordination. Where an identity related issue is attributable to, or best addressed by, Entrust's Services, Relying Party shall:

i. promptly escalate or refer the User to Entrust using agreed handoff mechanisms;

ii. cooperate with Entrust by sharing relevant information within Relying Party's control, subject to applicable law; and

iii. support coordinated resolution so that responsibility for identity repair is clear and Users are not passed between parties without resolution.

7.3. Evidence to Support. Where Entrust is able to confirm that an instance of identity theft has occurred in connection with the Services, and where requested by a rightful User, Relying Party shall not unreasonably hinder Entrust's ability to provide supporting evidence to the User for onward identity repair, including interactions with law enforcement, financial institutions, or other service providers.

7.4. Dependency on External Authoritative Source. Nothing in this Section requires Relying Party to independently investigate identity theft beyond its own systems or to assume Entrust's certification obligations and each Party remains responsible for identity repair actions within its respective control.

8. **Third-Party Service Flow-down Terms**

8.1. Vendor Flowdowns. Certain components of the Services rely on data, systems, or services provided by third-party suppliers ("Third-Party Providers"). To the extent required by Entrust's agreements with such Third-Party Providers, Customer agrees to comply with and be bound by the applicable downstream requirements set out in this Agreement. Customer acknowledges that access to and use of the portions of the Services dependent on Third-Party Providers is conditional upon Customer's acceptance of such requirements

8.2. Customer Provided Data. Entrust and Third-Party Providers shall not be liable for any loss, damage, or claim arising from or relating to:

i. errors, omissions, or inaccuracies in any information, data, materials, instructions, or scripts provided by or on behalf of Customer in connection with the Services; or

ii. any actions taken by Entrust in accordance with Customer's specifications, directions, or instructions.

8.3. Third Party Availability. The Services rely in part on data made available by third-party providers. The availability of such data is outside Entrust's control. If any required dataset is withdrawn, discontinued, or otherwise becomes unavailable to Entrust, Entrust may suspend or discontinue the affected Services upon thirty (30) days' prior written notice to Customer. Any such suspensions or discontinuation shall not constitute a breach of the Agreement. Entrust will use commercially reasonable efforts to provide advance notice where reasonably practicable.

9. **Warranties and Disclaimers**

9.1. General Disclaimer. Except as stated in these product terms and the Agreement, the Certified Services are provided as is and as available, and Entrust disclaims other warranties, including implied warranties of merchantability, fitness for our particular purpose, and non infringement to the maximum extent permitted by law.

10. **Access Decisions.**

10.1. Customer acknowledges and agrees that Entrust does not make, and is not responsible for making, any decision to grant or deny access to Customer's services requested by Users. Entrust's role is limited to providing authentication response options, which may include (i) "Clear" or (ii) "Consider," as selected by Customer for use in its evaluation process. Customer remains solely responsible for determining, based on such responses and any other factors it deems relevant, whether to approve or reject access to its services.