**NON-FUNCTIONAL REQUIREMENTS**

**Dependability**

DE.1. The messaging system shall be available at all times except for short, infrequent scheduled maintenance times.

DE.2. The messaging system shall have an uptime of at least 99.5%.

DE.3 The messaging system shall be designed to be efficient and scalable, accommodating larger volumes of users and data over time without service degradation.

DE.4 The system shall utilize a distributed network architecture to ensure optimal availability.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Security**

SE.1 The messaging system shall use end-to-end encryption on message data and any other necessary architecture that will protect messages from unwanted access and modification.

SE.2 The messaging system shall be designed to protect against common security threats, including injections and data breaches.

SE.3 Users shall be authenticated such that only authorized users can send or receive messages.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Regulatory**

RE.1 The organization shall comply with international and federal law specific to where services are available. The organization shall also endeavor to comply with state and local regulations to the best of its ability or where necessary.

RE.2 The messenger service shall comply with applicable data protection laws, including but not limited to, GDPR, CCPA, and other relevant regional or national regulations.

RE.3 The organization shall obtain explicit consent from users prior to collecting and processing their data in accordance with regulatory requirements in regard to user consent and privacy. Refusal to provide consent may result in the organization’s inability to provide service to the user.

RE.4 The organization shall fulfill required reporting mandates including disclosures related to data breaches and audits.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Ethical**

ET.1 Messaging data shall be stored temporarily on the cloud for 1 month unless the user chooses to backup their data.

ET.2 The organization shall rely on user feedback from the platform to decide on future modifications to the system.

ET.3 The service and organization shall prioritize user privacy and data protection with strict confidentiality while adhering to regulatory obligations.

ET.4 The service shall not collect or store user data beyond what is absolutely required for essential functionality.

ET.5 User data shall not be shared unless: it is essential for the functionality of the service, in which case only necessary data required to provide the service will be shared, or when required to comply with a lawful order.

ET.6 The service shall have policies and mechanisms in place to prevent service abuse.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Usability**

US.1 The messaging system shall offer multilingual support, including but not limited to English, Spanish, Chinese, and French..

US.2 The messaging system shall ensure accessibility for users with various disabilities including those with speech, visual, auditory, physical, and others, in accordance with applicable federal laws and regulations.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Environmental**

EN.1 The messaging system shall be compatible with modern versions of common operating systems and environments, including but not limited to Windows, macOS, specific linux distributions, and mobile operating systems such as iOS and Android.

EN.2 The messaging system shall require internet connectivity in order to send or receive new messages.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Operational**OP.1 There shall be a schedule for routine maintenance, software updates, and security patches.

OP.2 The organization shall follow industry-standard monitoring and logging practices.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Development**

DV.1 The organization’s development team shall adhere to industry standards for secure coding practices.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Performance**

PE.1 Messages shall be delivered in real-time with minimal latency.

PE.2 The messaging system shall support 100,000 messages per second.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Space**

SP.1 The user shall have an attachment size limit of 100 MB.

SP.2 The user shall have a message character limit of 918.

SP.3 Messages shall be compressed and encrypted at rest on the users device, requiring the smallest storage footprint as possible.

SP.4 Cached photos, messages, and drawings can be limited to a size specified by the end user.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Accounting**

AC.1 The organization shall maintain records of costs that involve development, testing, maintenance, and any other relevant project work.

AC.2 The organization shall release earning reports on a regular basis to provide transparency regarding its financial performance and motives. Releases shall comply with federal regulation and standards and be accessible to the public and to stakeholders.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Safety/Security**

SA.1 The organization shall conduct audits and vulnerability assessments and address issues during routine maintenance.

SA.2 There shall be access controls in place to define who can perform specific actions such as managing user accounts and pushing updates within the messaging system.

SA.3 The messaging system and services managed by the organization, shall undergo auditing and penetration testing at least every three years by a third-party organization. The details of the audit and penetration test shall be released to the public after any critical findings are addressed, up to three months after the findings are received.