TECHNICAL AND ORGANIZATIONAL MEASURES

I. ORGANIZATIONAL MEASURES

A. Information Security Governance

Data importer shall protect Customer Data, Confidential Information including Personally Identifiable Information through implementation and maintenance of policies and controls in alignment with the most recent versions of the international standard ISO27001 and 27002.

Data importer maintains security documentation describing its security measures and the relevant procedures in detail, as well as routine assessment and review documentation, and makes such available to data controller upon request.

Data importer has established a Chief Security officer with overall responsibility for information security governance and a personnel structure and responsibilities for information security systems and procedures. Data importer has established a Chief Privacy officer for privacy governance. Roles and responsibilities have been formally defined for all members of the information security and privacy teams and have been documented.

Data importer maintains an inventory of all data storage media on which Customer Data is stored.

B. Administrative Access Controls

1. Access Authorization And Workforce Clearance: An employee or contractor will be authorized to access personal data ("Authorized Users") only if the individual is deemed trustworthy based upon prior service to the data importer or the successful completion of a background check where permitted by applicable law. Data importer permits Authorized Users to access personal data only on a need-to-know basis and only as necessary to perform assigned job responsibilities.

2. Confidentiality Agreement: Before establishing access for an Authorized User, data importer requires that the Authorized User execute a confidentiality agreement that applies to the personal data or otherwise acknowledges an obligation of confidentiality.

3. Access Establishment: Data importer separates functions between those authorized to assign access rights and those authorized to establish access to data importer's information systems.

4. Review of Access Rights: On at least a quarterly basis and when an Authorized User changes positions, data importer reviews and, if necessary, revises or terminated the Authorized User's rights of access to workstations, programs and processes to limit the Authorized User's access to personal data to the minimum necessary to perform assigned job functions. Data importer will delete any personal data stored on the Authorized User's computer that no longer is needed by the Authorized User in his or her new position.

5. Denial Of Access To Terminated Authorized Users: Upon termination of any Authorized User's relationship with data importer, data importer promptly does the following: (a0 terminate the Authorized User's rights to access personal data and obtain the return of any devices (such as tokens or

key cards) used to obtain access to personal data; (b) obtain the return of all keys, key cards, and other devices that permit access to physical locations containing personal data in paper form; (c) ensure that the terminated Authorized User does not have unescorted access to areas containing personal data in paper form; (d) ensure that all personal data is removed from any computer equipment used by the terminated Authorized User before re-issuing that equipment to another Authorized User.

C. Training

Data importer provides (a) initial training to relevant personnel on how to implement and comply with its information security program, including identifying and reporting a personal data breach, and (b) periodic refresher training and security awareness reminders. Data importer permits newly hired Authorized Users to access personal data only after completion of the initial data security training.

D. Security Incident Response

Data importer has created a security incident response team (SIRT) with assigned roles and responsibilities. Data importer has implemented procedures for identifying security incidents, including personal data breaches, and a plan for responding to security incidents. Data importer periodically tests the security incident response plan. Data importer has established a mechanism for employees to report security incidents, including suspected and actual personal data breaches. Data importer requires all employees to immediately report the loss, theft, or otherwise of any equipment on which personal data is stored.

E. Third Party Sub Processors

Data Importer has a third party risk assessment and security agreement review process performed prior to engaging with third parties, and prior to any subprocessing of Customer Data or such third parties involvement in providing the Services.

II. TECHNICAL MEASURES

A. Evaluation And Monitoring

1. Risk Assessment: Data importer annually conducts an assessment of the potential risks and vulnerabilities to the systems andconfidentiality, integrity and availability of personal data.

2. Security Policies And Procedures: Data importer routinely reviews, evaluates and updates and implementes policies and procedures to reduce risks and vulnerabilities to a reasonable and appropriate level to protect the confidentiality, integrity and availability of personal data and to prevent accidental or unauthorized use, disclosure, alteration, loss or destruction. 3. System Activity Logging: Data importer has (a) enabled logging on computer systems that store personal data; (b) implemented a process for the review of exception reports and/or logs, and (c) developed and documented procedures for the retention of monitoring data.

4. System Activity Monitoring: Data importer periodically reviews information system activity records — including audit logs, access reports, privileged operations, error logs on servers, and security incident tracking reports, and changes to systems security — to ensure that implemented security controls are effective and that personal data has not been potentially compromised. Monitoring includes (a) reviewing changes affecting systems handling authentication, authorization, and auditing; (b) reviewing privileged access to production systems processing personal data; and (c) engaging third parties to perform network vulnerability assessments and penetration testing on a regular basis.

B. Risk Assessments

Data importer periodically conducts, and engaged third parties to conduct, assessments, reviews and reports on compliance with security policies and procedures. Data importer performs monthly security scans of both its internal network and servers as well as production (cloud) network and servers. Data importer performs static and dynamic scans of its software products and standard systems configurations prior to each major version release. Data importer engages a third party, at least annually, to perform an independent assessment of the information security program as well as a third party penetration test of its production systems. Data importer will make such third-party assessment reports available to data exporter upon request.

C. Protections Against Malicious Actors

1. Network and Host Security: Data importer employs intrusion detection at the network level and maintains an up-to-date host-based firewalls and access control lists (ACLs). Data importer engages in security patch management to ensure that security patches are installed as soon as is reasonably practicable.

2. Anti-Malware Protection: Data importer ensures that protections against malicious software (e.g., anti-virus protection, spyware detection software, etc.) are installed before computers and other devices are connected to any of data importer's networked systems. The software is kept current.

D. Technical Access Controls

1. Unique User ID/Secure Passwords: All Authorized Users will be assigned a unique user ID and will be required to create a strong/complex password, or to use a biometric identifier, to access data importer's network. Systems requiring entry of a password suppress, mask or otherwise obscure the password so that it cannot be viewed by an unauthorized person. All passwords are encrypted while in storage. Authorized Users are required to change passwords on a regular basis. Authorized Users are prohibited form sharing passwords with any other person.

2. Access Restrictions: Data importer has implemented technical controls so that each Authorized User will be able to gain access only to those categories of personal data to which access is necessary to perform assigned job responsibilities.

3. Encryption: Data importer encrypts personal data in transit, using Transport Layer Security (TLS) encryption. Data importer encrypts personal data at rest using 256-bit AES encryption or stronger. Mobile devices and portable electronic storage media used to store personal data must be encrypted.

4. Remote Access: Data importer permits remote access to its networks only via secured, authenticated connections utilizing a Virtual Private Network ("VPN") plus IP restrictions and MFA.

5. Secure Disposal: Data importer has established procedures for the secure and permanent destruction of personal data stored in paper and electronic form.

E. Contingency Planning

1. Back-Ups: Data importer backs up personal data on a regular schedule (daily incremental, weekly full). Back-ups are encrypted and stored in a using zone redundant, cloud storage apart from the primary storage. PoliteMail's redundant backup storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original or last-replicated state from before the time it was lost or destroyed. Restoration processes are tested within 60 days systems deployment, and at least annually.

2. Protection from Disruptions. Data importer uses various systems and monitoring processes and equipment to protect against loss of data due to power supply failure, line interference or other network interruptions.

3. Business Continuity/Disaster Recovery: Data importer maintains contingency and emergency and plans for the systems and facilities which process Customer Data. Data importer has developed and maintains a business continuity/disaster recovery plan to ensure that data importer can promptly resume service and restore data exporter's access to personal data in the event of a physical or technical incident occurrence (for example, fire, ransomware attack, vandalism, system failure, pandemic flu, and natural disaster).

F. Change and Configuration Management

Data importer maintains policies and procedures for managing changes to production systems, applications, and databases processing personal data and for documenting the changes.

G. Data Disposal

Data importer uses NIST-800 processes to delete Customer Data when it is no longer needed. For cloud services production systems, this is by permanent destruction of encryption keys and logical disposal of cloud storage drives (NIST 800-88).

H. Incident Response Process

Data importer tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time.

Data importer maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.

For each security breach that is a Security Incident, notification by data importer (as described in the "Security Incident Notification" section above) will be made without undue delay and, in any event, within 24 hours of evidence of breach.

III. PHYSICAL SAFEGUARDS

A. Data importer limits physical and logical access to facilities and systems where data is processed or stored to identified, authorized individuals. Data importer's facilities where personal data are physically secured against unauthorized access by, for example, keys, access cards, and/or security guards. Guests and service providers must register at a reception area and are prohibited from unescorted access to data importer's facility.

B. All servers and network equipment containing personal data are maintained in a location subject to controlled physical access. Only authorized employees may have unescorted access to secure areas where servers and network equipment are located. Video surveillance cameras monitor secured areas where production servers, data storage and other production network equipment are located.

C. Only authorized employees may have unescorted access to areas with computers and other electronic resources that permit access to personal data. Access is restricted by a proximity card or keyor some similar method. Physical access rights are promptly terminated when an employee no longer needs physical access to areas containing electronic resources that permit access to personal data.

D. Data exporter requires authorized personnel to ensure that all equipment (computers, laptops, etc.) utilized to access to personal data, that are assigned to, or regularly used by, them are maintained and used in a manner consistent with their function and such that the possibility of damage and/or loss is minimized.

E. Except for equipment designed to be portable, such as laptops, computer equipment used to access personal data should not be removed from data importer's premises without prior authorization.

IV. PERSONAL DATA MANAGEMENT

A. Privacy by Design Data Minimization

Data importer has subjected its systems and applications used to process personal data to a review for compliance with privacy-by-design and privacy-default principles and has applied the results of that review to the design of its systems and applications that process personal data. Data importer's systems and applications have been designed to collect, use, disclose, and otherwise

process the minimum personal data necessary to provide the services that are the subject of the Parties' underlying Agreement.

Data importer's systems and applications have been programmed to automatically delete personal data in accordance with the underlying Agreement, or data controllers data retention instructions, unless data importer is required by law to retain personal data for a longer period of time.

B. Accountability

Data importer maintains a record of processing activities that complies with GDPR, art. 30, with respect to its processing of personal data received form, or created or received on behalf of, data exporter. Data importer shall make such records available to data exporter upon request.

C. Data Subject Rights

1. Correction/Update Of Personal Data: Data importer provides options through its website to allow data subjects to request correction, updating or removal of their personal data and/or provides multiple methods (e.g., chat bot, webform, e-mail address) by which data subjects may submit requests. Such requests shall be referred to the data controller, and data importer shall assist with any corrections as necessary..

2. Erasure: Data importer has established internal procedures and technical mechanisms to ensure that personal data can be permanently deleted from production systems and back-ups in response to a request from a data subject or data controller, if and to the extent required by GDPR, art. 17.