**Exhibit C**
**P&G INFORMATION SECURITY REQUIREMENTS**

**General Terms**

1. Definition: "P&G INFORMATION" means any BUYER information created or accessed by SELLER in the performance of SERVICES for on behalf of BUYER.
2. Scope: This Exhibit applies to any SERVICES performed under the AGREEMENT.
3. Ownership and Use: All P&G INFORMATION is and remains the property of BUYER regardless of which PARTY has custody of such information. SELLER will only use P&G INFORMATION on behalf of BUYER in accordance with BUYER's instruction and as necessary to perform the services specified in the AGREEMENT, and SELLER will not collect, retain, use, disclose, distribute, sell, license, lease, transfer, or otherwise use P&G INFORMATION for any other purpose or for the benefit of any party other than BUYER.
4. Subcontractors: SELLER will obtain BUYER's written consent before providing P&G INFORMATION and/or access to BUYER's networks/systems to any third party, including affiliates of SELLER ("SUBCONTRACTOR"). SELLER will cause any SUBCONTRACTOR to enter into a written agreement that commits the SUBCONTRACTOR to adhere to security requirements no less rigorous than those set forth in this Exhibit.
5. Materiality: If SELLER fails to comply with the requirements set forth in this Exhibit, then BUYER is entitled to either suspend SELLER's performance under the AGREEMENT or terminate the AGREEMENT with immediate effect, without any penalty, liability or further obligation.
6. Conflict: In the event of a conflict, the terms of Exhibit C will take precedence over the AGREEMENT, including other Exhibits and Attachments to the AGREEMENT, and the terms of any purchase orders, releases, supplemental agreement, or other means of ordering.

**Security Requirements**

1. Compliance with Industry Standards: SELLER will utilize organizational, administrative, physical, and technical policies, standards and controls to protect P&G INFORMATION against the unauthorized or unlawful processing and against accidental loss or destruction of, or damage to, P&G INFORMATION. Such measures will be consistent with current accepted industry standards (e.g., the NIST Cyber Security Framework, ISO 27001/27002, ISO 27017, ISO 27018, SOC 2 Type II, Cloud Security Alliance STAR, etc.) and comply at all times with all applicable laws concerning the protection and securing of information. For as long as SELLER has access to P&G INFORMATION or BUYER's systems/networks, SELLER will update its security practices and controls at its own cost to continue to comply with accepted industry standards.
2. Audit: As an alternative to conducting an audit as set forth in this clause, BUYER may accept an independent verification (e.g. SOC 2 Type II report). At BUYER's request, and no more than once per year unless the initial audit identifies a material audit finding (in which case BUYER is entitled to audit the non-compliant control(s) until such material finding is remediated) or where BUYER or a relevant supervisory authority subsequently has reasonable grounds for suspecting a breach of SELLER's privacy or security obligations, SELLER grants BUYER permission and all necessary access to SELLER's computer facilities and systems and other information in order to perform an audit of SELLER's compliance with Exhibit A (as applicable), Exhibit C, and applicable laws. SELLER will cooperate with the audit by providing access to knowledgeable personnel, premises, systems/networks, policies, standards, documentation, and where possible, those same elements for any SELLER Subcontractors used to provide services to or on behalf of BUYER. At its cost, SELLER will promptly remediate any audit findings, and to the extent SELLER disagrees with such finding, work in good faith to negotiate a mutually satisfactory mitigation strategy. To the extent the PARTIES cannot reach agreement on a mitigation strategy for a material audit finding, BUYER will have the right to terminate the AGREEMENT for convenience with thirty (30) days prior written notice without any penalty, liability or further obligation. In the course of the audit, BUYER will not request, and SELLER is not obligated to provide, access to any information that is confidential third-party information.
3. Assessment and Review: SELLER shall implement a process for regularly testing, assessing and evaluating the effectiveness of the security measures it puts in place to ensure the security of the P&G INFORMATION.
4. Encryption: P&G INFORMATION must be encrypted in transit and at rest consistent with accepted industry encryption standards. SELLER will manage the encryption keys consistent with industry standards (rotated at least annually).
5. Awareness and Training: SELLER will provide information security awareness training to all its employees with access to P&G INFORMATION or P&G systems/networks that materially addresses the security requirements of this Exhibit, including best practices to detect and protect against phishing. Seller will also, at reasonable intervals, conduct phishing simulations to train its personnel to detect and protect against phishing attempts.

6. Strong Authentication:

   6.1 SELLER will maintain capability for its Services to integrate with P&G's Federation Service.

   6.2 SELLER will use multi-factor authentication for any of the following:

      1) Privileged access (e.g. system or data base level administrative access) to any servers and/or applications hosting P&G INFORMATION;

      2) Any remote access by SELLER to P&G INFORMATION.

7. Hosted Systems: SELLER will notify BUYER in writing before hosting P&G INFORMATION in a shared or cloud environment in China or Russia and will collaborate in good faith to identify an alternative to such hosting should BUYER so request. SELLER will protect (or cause its Subcontractor to protect) P&G INFORMATION hosted in any cloud environment using controls consistent with accepted industry standards (e.g., Cloud Security Alliance Cloud Controls Matrix).

8. Exit Strategy: At the termination or expiration of the AGREEMENT, SELLER will promptly return, or if requested by BUYER, securely destroy all P&G INFORMATION to BUYER unless otherwise required by applicable law to maintain, in which case SELLER will keep P&G INFORMATION confidential and securely protected until SELLER is permitted by applicable law to delete the P&G INFORMATION.

9. Records and Continuity: SELLER will maintain a records retention process and a business continuity plan for all P&G INFORMATION in SELLER's control or custody.

10. Disposal: SELLER will destroy P&G INFORMATION using a secure means of disposal (e.g. incineration or cross-cut shredding) when such data is reallocated or no longer required (either for the services or to be retained by law). Hardware containing P&G INFORMATION and BUYER licensed software must be physically destroyed or securely overwritten prior to disposal or use for another purpose.

11. Device Management: SELLER will use only securely configured, corporate-owned devices (i.e. non BYOD or hybrid/work personal use devices) to connect to BUYER networks and systems or to access or store P&G INFORMATION.

12. Access: SELLER will restrict access to BUYER systems and P&G INFORMATION to authorized individuals on strict need basis and such individuals will be required to execute a confidentiality agreement with SELLER.

    12.1 SELLER will maintain a process that both monitors and enforces access rights to BUYER systems and Information.

    12.2 Wireless access to BUYER networks and systems must be via secure connections (i.e. VPN) and over private wireless routers.

    12.3 To the extent that SELLER will access BUYER systems, SELLER will notify BUYER in writing of any SELLER employees, contractors or SUBCONTRACTORS who are terminated, removed from providing services or otherwise no longer strictly requiring access to BUYER systems (i) ten days in advance of such event if known, or (ii) within 24 hours of knowledge of such event if unanticipated.

13. Logging: SELLER must have a documented log review process. Administrators with privileged access to P&G INFORMATION must not be allowed to perform log maintenance. The following logs must be captured and actively monitored:

    13.1 Successful and failed logins of users and administrators;

    13.2 All admin access to the P&G INFORMATION and systems provided as part of the services;

    13.3 Changes to security configuration settings (password requirements, encryption settings, etc.);

    13.4 Other security relevant events (database transaction logging, database access logging, etc.).

14. Data Management: If P&G INFORMATION is stored in a multi-tenant environment, SELLER will either maintain separate dedicated hardware for P&G INFORMATION or will logically separate P&G INFORMATION from non-P&G INFORMATION. in multi-tenant environments

15. Penetration Testing: SELLER will perform or contract to perform ethical penetration testing of the environment on an at least annual basis with remediation and patching of discovered vulnerabilities.

16. Breach Response: SELLER will notify BUYER, through BUYER's project manager and securityincident@pg.com, of any actual or suspected breach or compromise of P&G INFORMATION ("DATA BREACH") as soon as possible after becoming aware of the incident, which may be sooner but no later than within 24 hours of learning of the incident. Upon learning of the DATA BREACH, at its own cost, SELLER will: (i) promptly isolate and remedy the DATA BREACH to prevent any further loss of data, (ii) begin a thorough investigation of the incident, (iii) take reasonable actions to mitigate any future potential harm to BUYER. SELLER will regularly communicate the progress of its investigation to BUYER and cooperate to provide BUYER any additional requested information in a timely manner. Unless legally required otherwise, and in order to ensure consistent and appropriate communication, SELLER will first inform BUYER of any DATA BREACH and obtain BUYER's written consent (email permissible) before informing any third party of the DATA BREACH (including regulators, law enforcement or impacted individuals) or referencing BUYER or BUYER's affiliates in any external DATA BREACH

communication. Notwithstanding the foregoing, SELLER is entitled to inform, at its own discretion, other entities directly impacted by the underlying incident and any breach response professionals, however in so doing, may make no reference, implied or actual, concerning BUYER.

17. Web-enabled Applications: All internet facing websites accessed by BUYER employees or consumers must have industry accepted protections from external threats including those listed in the Open Web Application Security Project Top 10. These protections should include a Web Application Firewall (WAF) and/or equivalent protections. All internet facing websites must be scanned and remediated using accepted industry standard for security (e.g., Open Web Application Security Project and Open Web Application Security Project Top 10). Scans and remediation must first be completed prior to application launch. Post launch, SELLER will conduct scans at a frequency that is appropriate for the relevant application, technology and data risk. Websites also will implement and maintain accepted industry standard account and password management controls, including:

    17.1 Lockout after no more than ten unsuccessful login attempts;

    17.2 Prohibiting user IDs, passwords and PERSONAL DATA from being displayed in a URL;

    17.3 Re-authentication is required after no more than 30 minutes of inactivity; and

    17.4 Prohibiting the storage of passwords or PERSONAL DATA in persistent local storage (caches, etc.) or in any cookies, JavaScript, or other web tracking technology.

18. Software Coding and Application Development Security: SELLER represents and warrants the SERVICES do not contain any code (e.g. viruses, worms, disabling code, time bombs, Trojan horses, adware, spyware, Internet bots, malware, bugs, web bugs or other destructive, secret or self-replicating code) or other technological means whose purpose or effect is to disrupt, damage, interfere with, and/or circumvent the security of any information technology systems ("HARMFUL CODE"). SELLER will promptly notify BUYER in writing if it discovers that any HARMFUL CODE has been introduced into any BUYER system by the SERVICES.

    SELLER will implement appropriate technical and organizational measures to ensure the delivery of secure code as defined within accepted industry standards such as OWASP Application Security Verification Standard ("OWASP Verification Standard") and Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses (CWE Top 25). These standards include but are not limited to strong configuration management, application security testing, runtime exploit prevention and no vulnerable open-source code. SELLER's development will not be complete until the security of the code and application has been demonstrated via a security report. Such security report must be provided by SELLER and reviewed and accepted by BUYER.

    SELLER acknowledges that BUYER operates a Bug Bounty Program that may identify vulnerabilities in SELLER's software. BUYER will notify SELLER of any security-related vulnerabilities identified through its Bug Bounty Program or other security testing. SELLER will promptly remediate security vulnerabilities BUYER identifies through its security programs. SELLER is not responsible for any vulnerability resulting from a custom configuration, development or modification made by the BUYER, or any third party authorized by the BUYER, on the SELLER's platform functionalities.

19. PCI: To the extent SELLER stores, transmits, or processes cardholder data (as defined by the Payment Card Industry Data Security Standard, "PCI-DSS"), SELLER will obtain and maintain third-party PCI-DSS certification. SELLER acknowledges in writing that they are responsible for the security of BUYER cardholder data that SELLER possesses or otherwise stores, processes, or transmits on behalf of BUYER and will furnish evidence of current PCI-DSS certification for the relevant services. SELLER will conduct PCI -DSS required quarterly network scans on the in-scope environment via an Approved Scanning Vendor (as defined by PCI-DSS), whose use is hereby consented to by BUYER. All service providers performing work that is "in scope" of Payment Card Industry standards (PCI Service Provider or Merchants) acting on behalf of BUYER must have their PCI scope assessed by a Qualified Security Assessor (QSA) with an annual Report of Compliance (ROC).