Exhibit C: P&G INFORMATION SECURITY REQUIREMENTS

This Exhibit C applies to any agreement, purchase orders, releases or other means of ordering ("AGREEMENT") between SELLER and BUYER.

General Terms

1. Information Classifications: the below definitions apply to the following information classifications used within this Exhibit.
    a. "SECRET" – means any BUYER information identified as being secret information either by label or by type.
    b. "HRI" – means any BUYER information identified as being highly restricted either by label or by type.
    c. "P&G INFORMATION" – means any BUYER data or information, including PERSONAL DATA, SECRET or HRI used, created or accessed in the performance of services for or on behalf of BUYER.
    d. "PERSONAL DATA" – means any information that (i) identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household, or (ii) would be considered personal information or personal data as such term/concept is defined by applicable law. PERSONAL DATA obtained by SELLER independent of this AGREEMENT is not considered PERSONAL DATA for the purposes of this Exhibit unless it is used in connection with SELLER performing under the AGREEMENT.

2. 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.

3. 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.

4. 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 unauthorised 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

Exhibit C: P&G INFORMATION SECURITY REQUIREMENTS

NIST Cyber Security Framework, ISO 27001/27002, 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: 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 security obligations, SELLER grants BUYER permission and all necessary access to SELLER's computer facilities and systems in order to perform an audit of SELLER's compliance with this Exhibit. 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. SELLER is not obligated to disclose or make available any systems or information that is confidential third-party information. 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. As an alternative, BUYER may choose to accept an independent verification (e.g. SOC 2 Type II) of SELLER's compliance with this Exhibit.

3. Assessment and Review: SELLER will 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 Personal Data.

4. 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).

Exhibit C: P&G INFORMATION SECURITY REQUIREMENTS

5. Encryption: SELLER will not store P&G INFORMATION on any portable device or media (e.g., laptop, flash drive, Smartphone) that does not utilize industry standard, full disk (where possible) encryption. SECRET, HRI, and PERSONAL DATA must be encrypted in transit and at rest consistent with accepted industry encryption standards.

6. Web-enabled Applications: All internet facing websites accessed by BUYER employees or consumers must have industry standard tuned Web Application Firewall (WAF) and must be scanned and remediated using accepted industry standard for security vulnerabilities (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 will implement and maintain accepted industry standard account and password management controls, including:
   a. Lockout after no more than ten unsuccessful login attempts;
   b. Prohibiting user IDs, passwords and PERSONAL DATA from being displayed in a URL;
   c. Storing user passwords and reset/forgotten security questions in an encrypted manner;
   d. Re-authentication is required after no more than 30 minutes of inactivity; and
   e. Prohibiting the storage of passwords or PERSONAL DATA in persistent local storage (caches, etc.) or in any cookies, Javascript, or other web tracking technology.

7. Software Coding and Application Development Security: SELLER will implement appropriate technical and organizational measures to ensure the delivery of secure code as defined in the OWASP Application Security Verification Standard ("OWASP Verification Standard"), including but 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 based on the OWASP Verification Standard. Such security report must be provided by SELLER and reviewed and accepted by BUYER.

8. 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 requirement of this Exhibit.

9. Strong Authentication: SELLER will maintain capability for its Services to integrate with P&G's Federation Service (SAML). SELLER will use two-factor authentication for any of the following:
   9.1 Privileged access (e.g. system or data base level administrative access) to any servers and/or applications hosting P&G INFORMATION;
   9.2 Any remote access by SELLER to P&G INFORMATION.

10. Hosted Systems: SELLER will notify BUYER in writing when it hosts PERSONAL DATA or HRI in a shared or cloud environment. SELLER will protect (or cause its Subcontractor to protect) the PERSONAL DATA or HRI hosted in this cloud environment using controls consistent with accepted

industry standards (e.g., Cloud Security Alliance Cloud Controls Matrix). SELLER will collaborate in good faith to identify an alternative to such hosting should BUYER so request.

11. Exit Strategy: At the termination or expiration of the AGREEMENT, SELLER will promptly return all P&G INFORMATION to BUYER unless otherwise required by law to maintain.

12. 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.

13. Disposal: SELLER will destroy P&G INFORMATION using a secure means of disposal (e.g. incineration or cross-cut shredding) when such data is 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..

14. 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.

15. 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.
    a. SELLER will maintain a process that both monitors and enforces access rights to BUYER systems and Information.
    b. Wireless access to BUYER networks and systems must be via secure connections (i.e. VPN) and over private wireless routers.

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 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 of BUYER's PERSONAL DATA 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.

Exhibit C: P&G INFORMATION SECURITY REQUIREMENTS

17. Escrow of Source Code: Within 5 Business Days' after delivering the object code of the application or software component(s) to BUYER, SELLER will deposit one copy, on SELLER's behalf, of the application or software component(s) in source code with an escrow agent specializing in software escrows that BUYER and SELLER agree to in writing.

17.1 Updates of Source Code. If SELLER makes any updates, enhancements, or modifications to the application or software, SELLER will promptly deposit one copy, on BUYER's behalf, of that update, enhancement, or modification, and any documentation related to the update, enhancement, or modification, to the mutually agreed escrow agent.

17.2 Upkeep of Escrow Account. BUYER will pay all fees necessary to establish and maintain the escrow.

17.3 Contingent License. SELLER hereby grants to BUYER a contingent license to receive the source code from the escrow agent and to use the source code to support its use of the application or any software components in machine-readable form if SELLER:

a. whether directly or through a successor or affiliate, ceases to be in the software business,

b. fails to fulfill its obligations to maintain the applications or software components as provided in this Exhibit C or the AGREEMENT,

c. becomes insolvent or admits insolvency or a general inability to pay its debts as they become due,

d. files a petition for protection under the U.S. Bankruptcy Code, or an involuntary petition is filed against it and is not dismissed within 60 Business Days, or

e. comes under the control of a competitor of BUYER.

17.4 Escrow Agreement. SELLER and BUYER will enter into an agreement with the mutually agreed escrow agent that grants BUYER the rights set forth in Section 17.3.