The Procter & Gamble Company
General Offices
2 Procter & Gamble Plaza
Cincinnati, Ohio 45202-3315

June 2018

Valued External Business Partners:

Information Security is critical in today's business world. P&G expects our External Business Partners to keep P&G Information secure and protected by classifying and handling it appropriately. P&G External Business Partners are expected to follow P&G guidelines which ensure that P&G information is treated in line with its sensitivity and risk of exposure.

As of July 1, 2018, P&G is deploying a new information asset classification framework that strengthens our approach to protecting and handling company information. The security classifications of P&G Information Assets are now as follows:

1. **Public Information.** Information assets that have been explicitly authorized by the P&G information asset owner for public access. Examples: P&G Annual reports, P&G press releases once published.
2. **Business Use.** Data that is shared on a limited basis. Examples: Commercial requests for proposals, contracts (except for specific Innovation Agreements), P&G Policies, Purchase Orders.
3. **Highly Restricted.** Data that is shared on a very restricted basis. Examples: Vendor Master Data Documents, Investigation Reports, Formula Cards, most Innovation Agreements.
4. **Secret.** Data that involves the most restricted access (very few individuals) and requires a high degree of Confidentiality, Integrity, and Availability. Examples: Major Product Innovations, some Acquisition & Divestiture information, some Innovation Agreements.

Personal Data. Personal data, also known as PII – Personally Identifiable Information, is classified based on the types of data processed (name, consumer email address, etc.) and volumes of personal data processed or handled by the end user. Third Parties collecting or processing PII as part of the activities provided to P&G must be specifically assessed on their Privacy handling capability. The personal data classification will match with the other classifications in this document (e.g., Business Use, Highly Restricted, etc.) and therefore involve similar handling requirements.

P&G Information Assets (except "Public Information") must be kept confidential, and made available only to those who have a legitimate 'need-to-know' to fulfil their duties or contractual responsibilities, and may only be released to the public in accordance with legal requirements, P&G policies, or P&G management direction.

- Please work with your P&G contact to learn more about acceptable collaboration tools. Note that usage of portable storage media is highly discouraged by P&G.
- At the end of the contractual agreement with P&G, please make sure all P&G information assets are destroyed (using industry standard applications) or returned to P&G.

If you suspect your device containing company information has been compromised, first (if possible), reset your password and then report the issue to SecurityIncident@pg.com and you will be instructed on when and how to respond if required. For additional assistance with Information Classification, talk to your P&G Sponsor/Contact or send an email to: pgsecurity.im@pg.com.

Thank you for your support in protecting P&G Information.

Sincerely,

Stewart Atkinson
The Procter & Gamble Company
Chief Purchasing Officer