Data Protection Policy

Effective Date: July 1, 2026
Last Publish Date: July 1, 2026
Last Review Date: April 27, 2026

1. Purpose

The purpose of the Data Protection Policy is to establish a framework for understanding, handling, and protecting P&G data. This framework supports the confidentiality, integrity, and availability of data, thereby minimizing financial, reputational, and operational risks while enabling the organization to achieve its business objectives.

2. Scope

This policy applies to all Procter & Gamble employees, contractors, joint venture participants, non-employees, and external business partners.

3. Policy Requirements

P&G is dedicated to maintaining strong data protection practices guided by key objectives that promote confidentiality, integrity, and availability of information. The following objectives will be prioritized based on data value, risk assessment, and business needs:

- Minimize data and protect by default by limiting data collection, access, retention, and exposure to what is necessary for legitimate business purposes.
- Ensure secure handling and sharing of data in accordance with established protocols.
- Maintain data security based on business value and risk, ranging from encryption (at rest and in transit), through access control mechanisms, to data loss prevention measures.
- Provide regular training to foster a culture of data protection.

Refer to the dedicated P&G Standards listed in the Appendix section of this policy to understand how to comply with the above requirements.

4. Policy Compliance

4.1. Compliance Measurement

Compliance with this policy will be validated through various methods, including but not limited to reports, internal and external audits, and feedback to the policy contact.

4.2. Exceptions

Any exception to the policy must use the established IT Compliance Exceptions Process.

4.3. Non-Compliance

Violating this Policy may result in disciplinary action, consistent with local laws. Employees affected by this Policy are expected to read and follow it, directing any questions to the Policy Contact.

5. Definitions and Terms

Item	Definition or Terms
Data Breach	*An incident where unauthorized access to data occurs.*
Data Loss Prevention (DLP)	*Protective measures are applied at different points or channels where the leakage may occur (e.g. email, instant messaging, Internet browsing, or portable storage devices). Sometimes also referred to as information leakage protection involves the implementation of technical solutions that scan/monitor systems and networks to prevent and detect the leakage (i.e., unintended disclosure) of information.*

6. Appendix or References

Related Standards, Policies and Processes

Standards linked to this policy:

- **Encryption Standard**
- **Information Asset Classification Framework & Handling and Protection Standard for End User**
- **IT Compliance Exceptions Process**

Additional standards to be considered:

- **Acceptable Use of PG Tech Standard**
- **Account and Privileges Management**

6.1. Review and Update History

Date	Performed By	Summary of Review or Update
04/02/2026	*Andrea Di Fonzo*	*Creation of Data Protection Policy document.*