P&G

Appropriate Use of Hardware and Software Policy

Approver: Kostas Georgakopoulos	**Policy Owner:** Sarah Ackerman
Scope: Global	**Legal Advisor:** Angie Stone
Effective Date: April 01, 2014	**Contact:** ackerman.s.1@pg.com
Last updated: October 16, 2018	

Contents

P&G

Appropriate Use of Hardware and Software Policy

1.0 Company Intent

The aim of the Appropriate Use of Hardware and Software Policy ("the policy") is to ensure that all P&G employees and Third Parties using hardware and software understand how to appropriately use it and know specific actions they must take to comply with this policy and applicable laws and regulations.

P&G invests in technology because we recognize the enormous potential these tools have in helping us achieve the Company's business objectives. Hardware and software applications allow us to communicate globally, to improve our understanding of consumers and to run the business. However, misuse or abuse of these tools as well as other electronic hardware/ services can lead to reduced productivity, wasted corporate resources, legal liability for the Company and/or individual, and ultimately, missed business results.

2.0 Scope

This policy applies to all employees and Third Parties using hardware and software applications to conduct business for P&G, regardless whether the hardware or software is owned by the Company or by the employee or by the Third Party. Throughout the rest of this policy, they will be referred to as "users."

3.0 Policy Statement

All P&G users of hardware and software must act consistently with our PVPs and follow the Company's expectations outlined in this policy regarding acceptable use, business information security, obtaining and using software, training, auditing, and technology scanning. In addition, P&G employees responsible for a Third Party relationship must ensure that all Third Parties using P&G-issued hardware and software follow the expectations outlined in this policy.

4.0 Accountability

The Corporate Information Security Process Leader shall administer the policy and develop procedures and other tools to support policy implementation.

This policy will be reviewed at least every two years and updated as appropriate. Any significant changes will be communicated to all users.

The Policy Owner and Approvers are assisted with policy implementation as follows:

Role	Description	Organization	Contact
Process Leader	• Facilitates the process and makes sure the decision gets made in a timely manner	Corporate Information Security	Appropriate Use Policy Owner

P&G

Appropriate Use of Hardware and Software Policy

Role	Description	Organization	Contact
Approval	• Holds final decision authority-has capability and experience to make the call and be accountable for results	Corporate Information Security	Appropriate Use Policy Owner
Contributor	• Designated by "A" or "P" for advice • Does not hold approval or veto power; does not need to agree with decision for it to move forward • Not always required	Ethics & Compliance Working Group Global Legal Compliance Global Employee Relations	Ethics & Compliance Director Appropriate Use Policy Legal Advisor Global Employee Relations
Execute	• Takes action to bring decision to life • Need to know outcome and rationale for a decision to execute with excellence	Corporate Information Security Employees Services & Solutions Ethics & Compliance Operations Legal HR Business Account Managers	Appropriate Use Policy Owner Personal Computing Associate Director Ethics & Compliance Director Legal Contact for Info Security By Business

5.0 Acceptable Use

5.1 The primary use of Company-owned hardware and software must be Company business. Personal use of Company-owned hardware and software is permitted only on a limited incidental basis, however devices enrolled in the CorporateMobile program must be used for business use only. The only acceptable personal use of a CorporateMobile device is in the event of an emergency. Storage of texts, apps, photos, files, or any other personal data is prohibited. For more information regarding CorporateMobile devices see the Global Mobility Service Policy.

Additionally, personal use must:

- Not interfere with Company business;
- Not interfere with the P&G network;
- Not involve incremental cost to P&G;
- Not interfere with productivity;
- Not further personal, non-P&G-related business interests; and

P&G

Appropriate Use of Hardware and Software Policy

- Follow all licensing and permitted use terms and conditions for the hardware and software.

You are responsible for ensuring that your personal use complies with these principles.

5.2 Using Company software or systems or a Company-owned device for P&G business to do any activity that is illegal or inconsistent with our PVPs and/or Worldwide Business Conduct Manual is a violation of this policy and could lead to disciplinary action, consistent with local law, up to and including termination. Examples include, but are not limited to:

a. Installing, viewing, downloading or storing inappropriate, offensive and/or illegal information (e.g., sexually oriented).

b. Collecting any material by illegal or unethical means (e.g., by wiretapping, spying on competition, or other methods inconsistent with our PVPs).

c. Using e-mail, instant messaging, the internet or other electronic hardware/services to make offensive (e.g., sexual or racist), obscene, discriminatory or harassing statements.

5.3 You must refrain from using a personal device enrolled in the YourMobile Program for P&G business to engage in illegal activities of any kind, pursuant to all local laws. For more information regarding YourMobile devices see the Global Mobility Service Policy.

6.0 Business Information Security

6.1 P&G business data must not be sent to or from your personal email and must not be stored on your personal cloud services or storage (removable devices). Personal email, services, and storage are prohibited for any business use or handling of P&G business data.

Employees are permitted to use only company-issued email and cloud services for business use and handling of all P&G business data. In addition, only company-issued storage/removable devices can be used for business use and handling of P&G business data.

You must protect all Company-owned computing devices and all Company information. Examples of protection include, but are not limited to, locking devices up when not in use, password protecting the device, utilizing multi factor authentication, using encryption, and making timely backups.

6.2 You must comply with all Company information security requirements, including understanding and using the Company's data classifications (Secret, Highly Restricted, Business Use, Public) and must handle all Company data consistent with P&G's expectations, any local legal requirements, and according to the Information Asset Classification Policy.

P&G

Appropriate Use of Hardware and Software Policy

6.3 You must promptly report: 1) any loss of Company information; 2) loss of Company-owned computing devices; and 3) loss of any personally-owned devices that contain Company information. Report any loss to SECURITYINCIDENT@PG.COM.

6.4 You must refrain from collecting, accessing, using, retaining, or disclosing Secret or Highly Restricted data or Personally Identifiable Information (PII) of our employees, consumers, customers, vendors, and/or other stakeholders except when pursuant to relevant and appropriate business purposes and in accordance with the purpose for which the information was collected.

- Do not download PII or Secret/Highly Restricted data onto computing devices unless that device complies with P&G Information Security policies (http://itpolicy.pg.com) and laws governing the safeguarding of this data.
- Do not share PII or Secret/Highly Restricted data with anyone, either inside or outside our Company, who does not have a legitimate business need to know or process this data.
- Do not provide PII or Secret/Highly Restricted data to a third party vendor unless they have been properly vetted via the Privacy and Information Security Third Party Risk Management (TPRM) process.
- You must take steps to properly secure PII and Secret/Highly Restricted data from unauthorized access by third parties at all times, according to the Information Asset Classification Policy.

If you believe that any Secret/Highly Restricted data or employee, consumer, customer, vendor and/or other stakeholder PII has been disclosed or used inappropriately, send an email to SECURITYINCIDENT@PG.COM immediately. Failure to do so could subject our Company to fines and/or regulatory action.

6.5 In limited situations, where there is a legal need or requirement, a Corporate device or a personal device enrolled in the YourMobile Program used for business purposes may be required to be turned over to the Company and/or legal authorities and searched for relevant records. In such a situation both business and personal records stored on the device or accessed via the device may be reviewed in compliance with applicable law.

6.6 If a Corporate device or a personal device enrolled in the YourMobile Program used for business purposes is lost or stolen the device may need to be wiped for security purposes. Users should store separately or back up personal contacts, photos and other records to avoid losing them in the case that their device must be wiped for security purposes. Refer to the YourMobile User Agreement for the full list of circumstances under which the device could be wiped.

P&G

Appropriate Use of Hardware and Software Policy

7.0 Obtaining and Using Hardware and Software

7.1 Hardware for Business Use

- The Company will provide you with hardware appropriate to your role. If you have questions or additional needs, talk to your manager.
- Attaching or installing other hardware onto a Company-owned device is permitted in limited circumstances and must be done with caution.
- The use of hardware that could compromise the security of the device, any applications or the Company network is prohibited (e.g., Key loggers – devices that collect the keystrokes typed on a keyboard).
- Permitted hardware (and associated driver software, as needed) includes: a keyboard, mouse, USB drive, external drive, webcam, microphone and/or printer.
- When purchasing computing accessories for work, you must first review the Company process on ITSolutions to see if the accessory is available from the Company-preferred supplier.

7.2 Software for Business Use

- All software anticipated for business use must be checked to reduce potential for network harm, information security issues and legal liability.
- You must follow the mandatory process that includes first checking one of the approved standard Company Application Centers before downloading any software for business use (e.g., eSupport for the SEWP and Open & Go platforms; PGToGo.pg.com/PG App Store for mobile applications; MAC.pg.com).
- To purchase software that you do not find on any of these approved Company Application Centers or on the Blocked List, the item:
    - Must be purchased from SHI.
    - Must be taken through the standard Company certification process (e.g., GRAD for SEWP and Open & Go) and then added to an approved standard Company Application Center (e.g., eSupport for SEWP and Open & Go). The standard Company certification process: 1) puts the software through a standard testing and change management process to detect and remediate conflicts with other software running on your Company-owned computer (SEWP and Open & Go), and 2) is a pre-requisite for posting a software application to an approved standard Company Application Center. If you have any questions, please send an email to grad.im@pg.com or see the GRAD process site.
    - Must not interfere with the P&G network or involve incremental cost to P&G.
- If the software does not require a purchase, you may download it as long as you have verified the following:

- The software is not on the Blocked List.
- The vendor developing/providing the software is reputable.
- The software will be downloaded from a reputable site.
- The use of the software:
  - Does not interfere with the P&G network.
  - Does not involve incremental cost to P&G.
  - Follows the terms and conditions and/or licensing agreement for the software and allows for business use.

- **It is your responsibility to ensure that all software you install complies with this policy.**

7.3 Software for Personal Use

Installing software for your personal use onto a Company-owned device is permitted only on a limited incidental basis; however devices enrolled in the CorporateMobile program must be used for business use only and therefore you must not install any software or applications for personal use on these devices. For more information regarding CorporateMobile devices see the Global Mobility Service Policy.

Additionally, personal use must:

- Not interfere with Company business, and
- Not interfere with the P&G network, and
- Not involve incremental cost to P&G, and
- Not interfere with an individual's productivity or the productivity of others, and
- Not include software listed on the Blocked List, and
- Only include software for which you have a valid license, and
- Follow all licensing terms and conditions, including permitted uses for the software, and
- Only include software from vendors that are reputable, and
- Only include software that has been downloaded from a reputable site.

It is your responsibility to ensure that your personal use complies with these principles.

7.4 Reminders and Tips for Software Installations

Remember to start your search for software with an approved standard Company Application Center (e.g., eSupport for the SEWP and Open & Go platforms; PGToGo.pg.com/PG App Store for mobile applications; MAC.pg.com). If you don't find what you are looking for there and the software is not on the Blocked List, then be sure to pay attention to the following watch outs:

P&G

Appropriate Use of Hardware and Software Policy

- Do you really need the software to meet your business need? Is there a comparable software available via one of the approved standard Company Application Centers that will permit you to meet your business objectives? Any time you install software on your own, there are potential risks.
- If the deal is too good to be true, it is likely problematic. If the online price is really low compared to the estimated retail value of the software or if the deal otherwise just seems too good to be true, do not make the purchase.
- If it doesn't look official, don't install it. If the software looks "homemade," has hand-written labels or does not include original disks or manuals, don't install it and return it if you can.
- Avoid "Back-Ups" and "Compilations" as these are indications that the software is illegal.
- Don't install software from an auction site or other questionable site. When searching the internet for software to install, look for indications that the site is a reputable business site, e.g., look to see if the site features local business trust marks like VeriSign.

  Reputable sites include (but are not limited to):

  - Official sites that provide the software or a marketplace for such software (e.g., Google Maps from google.com, AccuWeather from accuweather.com, Quicken from Intuit);
  - Sites offered by a well-known phone manufacturer (e.g., Blackberry.com and its Appworld, apple.com and the Appstore); and/or
  - Sites offered by well-known carriers (e.g., verizon.com, att.com).
- Be cautious when installing software from outside your country. Laws may vary and licenses may be limited geographically. Be sure to check into whether there are potential issues or restrictions before installing.

7.5 Illegally obtaining or downloading software or making unauthorized copies of licensed software and digital media (e.g., songs, books) for P&G business use are prohibited. These actions can cause serious legal ramifications for the Company. Additionally, exceeding the rights of a license agreement (e.g., installing excess copies, reselling to other entities, using in restricted geographies, or using software licensed for personal use for your work purposes/productivity) is also prohibited.

7.6 Distribution of Company hardware, software and information assets outside the Company to Third Parties (i.e., clients, customers, suppliers, contractors and others) must comply with Company policies, applicable licenses and copyright laws. It is your responsibility to understand any restrictions prior to distribution.

- Before distributing to Third Parties, the P&G employee responsible for the Third Party relationship must ensure that Third Party employees who use Company-owned hardware and/or software understand this and other applicable Company policies.

P&G

Appropriate Use of Hardware and Software Policy

- This employee also is responsible for ensuring we retrieve any computing devices or software copies from Third Parties (i.e., clients, customers, suppliers, contractors and others) when the licenses have expired and/or our relationship with these third parties has ended.

7.7 You must not transfer or move Company-owned computing devices to another site/country (e.g., next assignment, relocation) without first consulting your management to ensure that proper transfer procedures (e.g., Fixed Asset Transfer process) are followed. In some cases there are strict government regulations concerning the transfer of workstations and related technology.

7.8 Third Parties using Third Party-owned computing devices may not download, use or copy Company-owned software (e.g., Microsoft Office), unless such distribution of software is explicitly permitted by P&G's licensing terms.

8.0 Training / Performing Self Audits

8.1 You are responsible for performing mandatory self-audits to ensure all installed software is approved for use and compliant with all license agreements.

8.2 You are required to certify completion of the Appropriate Use training when requested by the Company. You will receive an automated reminder to complete this training.

9.0 Technology Scanning (from the Global Employee Privacy Policy)

P&G is committed to protecting your personal privacy while also protecting Company assets. To ensure system integrity, security and application performance, the Company routinely manages network and system usage. However, we do not scan individual computer use unless there is a legitimate and specific reason to do so.

If a concern is raised regarding a user's use of the Company's assets or the Company is legally required or subpoenaed, individual scanning may be imposed. However, this will be proportional to the specific need and in compliance with applicable laws and the Company's Global Employee Privacy Policy. Before scanning of an individual can be carried out, the approval from the appropriate Global Officers is required.

10.0 Requesting Policy Exceptions

P&G does not permit exceptions to this policy.

P&G

Appropriate Use of Hardware and Software Policy

11.0 Monitoring and Enforcing the Policy

Make sure you understand and comply with this Policy and seek help if you have any questions about the proper course of action.

You are expected to report any known or suspected violations of this policy through available Company resources. All reports are investigated thoroughly and promptly. No one who participates or cooperates honestly and completely in P&G's investigation of a report will be subject to retaliation for doing so. Please refer to the WBCM for the appropriate process to follow to report violations.

12.0 Discipline

In doing the right thing, we must dedicate ourselves to complying with this policy. Individuals who fail to comply with this policy will be subject to disciplinary action, up to and including termination. All disciplinary action will be applied in a manner consistent with local law. In some circumstances, applicable regulatory authorities may impose fines and penalties on individuals.

13.0 Definitions and Acronyms

Computing Device / Hardware: Devices such as desktop computers, laptop computers, virtual desktops, notebooks, iPads, tablets, mobile phones, Smartphone's (e.g., Blackberry, iPhone), and Personal Digital Assistants (PDAs) (e.g., Palm Pilot).

Electronic Hardware / Services: Printers, faxes, copiers, desk phones and Voice over IP (VOIP) phones, USB drives, external hard drives, CD/DVD players, external file storage provided by cloud service providers, web conferencing services, and other similar services.

One Mobile Program: Mobility Service that provides exempt employees with improved flexibility when it comes to meeting their mobility needs. It consists YourMobile and CorporateMobile services.

PII: Personal Identification Information; any information that identifies an individual – such as name, physical address, email address, employee ID, government ID, photograph, or any combination of this or other information that might identify an individual.

PVPs: Purpose, Values, and Principles

Software Application: Software used for conducting any P&G business which is installed on a computing device, whether such device is owned by the Company or by the user.

User: In this policy, "user" refers to both employees and Third Parties.

P&G

Appropriate Use of Hardware and Software Policy

14.0 Reference Documents

Asset Classification Definitions	https://pgone.sharepoint.com/sites/PGSecurity/Pages/Information_Asset_Classification.aspx
Global Employee Privacy Policy	https://pgone.sharepoint.com/sites/PrivacyCentral/Pages/employeepolicy.aspx
Worldwide Business Conduct Manual	https://pgone.sharepoint.com/sites/ecoportal/Lists/EcoDocumentDownloaderMainModule/DispForm.aspx?ID=2
Global Mobility Service Policy	https://pgglobalenterprise.service-now.com/kb_view.do?sysparm_article=KB0012050