Access Control - Company Facilities

Policy ID:	**Policy Owner:** Dave Flavin, Global Governance
Scope: All Company facilities globally	**Approver:** Steve McShea, Global Security Director
Effective Date: December 2020 **Reviewed:** 02/08/2021	**Contact:** Dave Flavin, flavin.dj@pg.com

1.0 Company Intent

The intent of the Physical Access Control - Company Facilities policy is to provide direction for Access Approvers granting physical access and to site physical security owners to follow in permitting access to Company owned or leased facilities for Authorized Personnel. This is also intended to deter and detect unauthorized access to P&G facilities.

A "policy" is a document that defines P&G's beliefs and goals regarding a specified subject area.

2.0 Policy

1. Physical Access control can be accomplished by utilizing receptionists, security officers / guards, electronic access control systems, or locks to restrict physical access to P&G facilities (Facilities installing new electronic access control systems must implement the Company standard OneKey PAC system).

2. **Authorized Personnel** will be designated by a P&G issued photo identification badge; only one permanently assigned active ID badge is permitted per individual. Authorized Personnel will present a government issued photo ID to verify their identification before their P&G badge is issued.

   Note: Authorized Personnel will be designated by HR for Employees and Retirees and Purchases / Business Unit Sponsors for Non-Employees. HR records will be checked to ensure that authorization status reflects employment status. Non-Employee access authorization status will need to be renewed every six months by the sponsor.

3. Authorized Personnel are defined as:
   a) **Employee** – employee assigned or associated with a facility as their Primary site.

   b) **Employee – Non-Site** – employee working at another facility that is not their Primary site.

   c) **Non-Employee** – person who is not a Company Employee, but his / her work supports facility or business core operations requiring a physical presence with unescorted access to the facility on a regular / weekly basis.
      Type of work requiring unescorted access is: Temp Office / Staff Augmentation, Facility Management Services, IT Management Services, Employee Management Services, Facility System Maintenance, Construction, Dining, Cleaning

   d) **Non-Employee Escorted Access Required** – person who is not an Employee needing access to a facility either to conduct business meetings, short duration services, or as a social call; requires escorted access to the facility.
      This can be Non-Employee Sales, Marketing, Business Development, Executive Management of Alliance Partner Teams, Agency, Suppliers, Vendors, or

Access Control - Company Facilities

representatives of our External Business Partners who are at a facility for the sole purpose of a business meeting

e) **Retiree** – individual who has retired in good standing from the Company and possess a retiree identification card indicating their retirement status.

4. **Access Authorization will be verified by – valid card swipe at an entry point.** Security Officers / Guards / Receptionists may also check to ensure the photo on ID to matches the badge holders

5. Employees assigned to a site should be granted 24 hour / 7-day access unless the local business unit(s) specify otherwise. After hour access, employees will be limited to one entry door controlled by site security to positively identify personnel entering via the camera monitoring system and intercom prior to permitting access

6. All personnel entering a Company facility must verify the badge in her/his possession is valid and active in the access control system by entering an access portal to present their badge to a card reader. Staffed lobbies without access reader-controlled portals will install a reader on or near the reception desk to facilitate this requirement.

7. P&G Identification Badges are required to be **visibly** displayed on the front side of the body at or above the waist by all personnel while in our facilities (note, this may be different in areas with safety constraints and should be discussed with the Global Security Site Resource)
   a) Non-Employee Daily Escorted personnel must be issued Red lanyards (to be worn around the neck) with the words Escort Required printed on them.

8. The number of entry / exit points must be minimized and doors with access readers must limit access to cardholders only (High Risk sites must utilize anti-tailgate physical security barriers).
   a) After hour entry point, must be limited to one entry door to ensure proper controls are in place for positive verification of personnel entering after hours and are authorized to be in the facility (exceptions to this can be made if a site has requirements to provide separate entrances for employees and contractors or if site has a critical business need).

9. Specialty doors (loading docks, cargo elevator lobby areas, labs, etc.) with access readers must limit access to authorized personnel only.

10. Multiple Company facilities in the same general vicinity must attempt to utilize similar access control systems (Company standard OneKey PAC system) to enable employee access to all facilities during normal business hours. Site access for employees can be granted by site reception/security after verification the employee is currently active for their home site.
    a) Employees residing at a facility with the Company standard OneKey PAC system will receive an automated clearance to only the perimeter doors of other OneKey PAC system facilities (exception to this are Product Supply sites) to gain entry during normal business hours (subject to local business unit requirements).

    b) Employees residing at a High Risk classified facility must have role based / auditable access control procedures in place to limit access to sensitive areas, such as: Innovation Space / Lab work areas / Proprietary Manufacturing processes, etc. to only those with a business need verified by the area owner.

    c) Employees must possess a P&G Identification Badge and have a valid OneKey site listed in their primary location in People Finder (if location free / work from home status the primary location would be the site you are considered associated with or nearest to your location).

Access Control - Company Facilities

11. Employees without their assigned P&G Identification Badge must show a government issued picture ID and be verified in the site security access control system or with their direct reporting manager as an active employee.
    a) A picture must be taken of the employee through the Visitor Management solution. The visitor management label with name/photo should be affixed to the case housing the temporary access card.

    b) Employees will be issued a temporary access badge valid for a limited period and to be assigned through the Passage Point Visitor Management solution.

    c) Temporary badges that are not linked to the access control system must have a time sensitive sticker that indicates when the badge is no longer valid.

    d) P&G Identification Badge deactivation requests are limited to the SAP system / Employee's immediate manager or one up managers, Site HR Leader, and/or Global Security. Site security personnel should record the name, date and time of person requesting access deactivation and ensure this is noted in the site security log.

12. Non-Employee Unescorted Access must be granted during normal business hours only. Refer to the Policy – Access Control – Non-Employee Unescorted Access After-Hours for exceptions to this policy.

    a) Non-Employee Unescorted Access badges **will expire within 6 months** from the date of issue or sooner if indicated.

    Digitized Non-Employee Unescorted Access process:

    Click here to access the Digitized Non-Employee Unescorted Access process and form

    b) Non-Employee Unescorted Access individuals must have T#'s and the P&G Identification Badge will automatically expire at 6 months if IT access is not renewed by sponsor.

    c) If the Non-Employee Unescorted Access individual has forgotten their assigned P&G Identification Badge, they must be issued a temporary Non-Employee Unescorted Access badge. A picture must be taken of the non-employee through the Visitor Management solution. The visitor management label with name/photo should be affixed to the badge or case housing the temporary access card. Temporary badges that are not linked to the access control system must have a time sensitive sticker that indicates when the badge is no longer valid. The temporary Non-Employee Unescorted Access badge must be signed out and in daily.

    d) P&G Identification Badge deactivation requests are limited to the Sponsor, Site HR Leader, and/or Global Security. Site security personnel should record the name, date and time of person requesting access deactivation and ensure this is noted in the site security log.

    e) Critical non-employees meeting the requirements of item 3 c) except for "regular / weekly basis" can be granted a temporary day badge provided their entrance is preauthorized by a P&G sponsor or a key business partner sponsor approved by P&G.

13. Non-Employee Escorted Access individuals are required to register with Reception / Security. P&G Sponsors and Critical Facility and IT Infrastructure Service Providers can authorize Visitor / Non-Employee escorted access individuals to enter the facility. They must be escorted by Employees or Non-Employee possessing unescorted access badges. Non-Employee may only host a visitor during the normal course of their work specifically related to their business on site as required by P&G (subject to local business unit requirements) while in non-common areas of

Access Control - Company Facilities

the facility. No personal visitors can be brought in by Non-Employees. Sites may elect to make visitor escort by P&G Employee only based on the work occurring at the site.

a) Non-Employee requiring an escort must present a government issued picture ID and be issued a temporary Non-Employee Escorted (Visitor) badge.

b) Non-Employee Escorted Access individuals must have a sponsor and may not enter the facility without an escort; the sponsor is responsible for escorting the visitor by meeting them at reception and returning them to reception at end of visit. Use the Company Standard Passage Point Visitor Management module (refer to Process - Visitor Management - Passage Point - OneKeyPAC.v1).

c) Non-Employee Escorted Access individuals must have a photo taken and printed on the temporary label badge issued through Visitor Management solution at the reception desk.

d) Non-Employee Daily Escorted personnel must be issued Red lanyards worn around the neck with the words Escort Required printed on them.

14. Company retirees are permitted to access our facilities (subject to local business unit requirements) during normal business hours and should present the Company issued retirement identification. They must also present a government issued picture ID and, if needed, issued a temporary access badge.

15. The site PSL working together with the TPSP assigned to the facility must conduct periodic reviews of site physical access control reports (quarterly / at least semi-annually) ensuring no employees have more than one active ID badge and terminated employees are deleted. Non-employee physical access reviews at OneKey Corporate Building sites for active badges must have a non-employee name, company name, T-number, sponsor identified, only one active badge, no inactive badges after 60 days. All other sites for non-employee physical access reviews non-employee name, company name, sponsor identified, only one active badge, no more than 6 months for expiration date.

    Physical Security access control reports need to be reviewed for the following:

    Employee:

    No employees have more than one active ID badge, terminated employee badges are deleted

    Non-employee OneKey Corporate Building sites:

    Non-employee name, company name, T-number, sponsor identified, only one active badge, no inactive badges after 60 days

    Non-employee all other sites:

    Non-employee name, company name, sponsor identified, only one active badge, no more than 6 months for expiration date

    Note: physical access control reports require circumstantial scan authorization and there is a global approval for 1LOD and 2LOD reviews on record retained by Global Security; there is a retention limit of 1 year unless directed otherwise by local regulations.

    For OneKey Reports follow this link to obtain:
    OneKey Physical Access Control Reports

    Or send request to:
    Jay Yelton; yelton.jj@pg.com Primary
    Chad Wehrman; wehrman.cc@pg.com Secondary

16. Requests for Badge Swipe Data cannot be performed without proper approvals.

    a) Employee – When a request for badge swipe data of an employee is received, the requestor must complete the Badge Scan Approval Process Employee form below. If the investigation

goes beyond badge swipe data a Level 3 Scan Request, as outlined by Global Employee Relations, must be submitted. The link to the Level 3 Scan Request is provided below.

Badge Scan Approval Procedure - Employees

Global Ethics and Compliance site:
https://pgone.sharepoint.com/sites/ecoportal/pages/Policies-Resources.aspx

Understanding Scan Process:
https://pgone.sharepoint.com/sites/PrivacyCentral/Pages/CenterCourt/Scanning.aspx

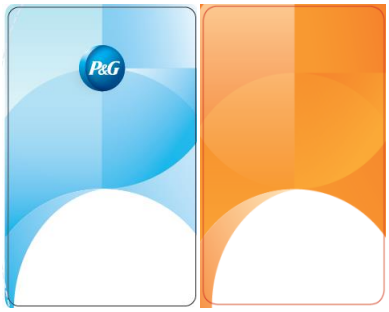
b) Non-Employee – When a request for badge swipe data of a non-employee is received, the requestor must complete the Badge Scan Approval Process Non-Employee form below and gain approval of the Site PSL. If the investigation goes beyond badge swipe data a Level 3 Scan Request, as outlined by Global Employee Relations, must be submitted.

Badge Scan Approval Procedure - Non-employees

17. The standard Company P&G Identification Badge design is blue for employees and orange on front and back for Non-Employee Unescorted Access.

c) All returned P&G Identification Badge must be removed from the access control database (by removing the card's number and all clearances) and the badge must be destroyed by shredding on site.

d) The site Physical Security Leader should either mandate P&G Identification Badge be renewed every three years, OR at a minimum, require all site personnel to update their photos, which will be saved in the access control system database.



3.0 Policy Declaration of Risk Acceptance

Declaration of Risk Acceptance to policy are discouraged as they require additional governance and follow-up often resulting in additional risk for P&G. If there is a strong business case, requests for risk acceptance to Global Security Policies must be submitted by following the guidelines of the Policy – Declaration of Risk Acceptance Form.