Securing Company Facilities

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

1.0 Company Intent

The intent of the Securing Company Facilities policy is to ensure Facility Physical Security direction designed to provide a safe and secure work environment through the prevention of unauthorized access to P&G owned and leased facilities.

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

2.0 Policy

- All points of entry into P&G space must be controlled via receptionists, security personnel, or access control readers and only properly verified personnel (internal/external) must be allowed access.

  a. The access control system (which includes the software and hardware) must be automated and create a permanent transaction record that cannot be altered.
  b. In addition, the access control system must be owned, controlled, and managed by P&G, and capable of permitting/denying access based upon date/time and/or zones.
  c. If installing a new access control system, the facility must implement the Company standard OneKey PAC system as this system automatically syncs with P&G's HR /identity management database allowing for an updated HR/IT records automated interface.
  d. The number of entry points must be minimized and doors with access control readers must be utilized to limit access to cardholders only (i.e. not have key overrides). Note, sites designated by Global Security as High Risk must incorporate anti-tailgate security barriers at all points of facility ingress/egress; these barriers are detailed in Standard – Security Barriers for Anti-Tailgating.
  e. Reception areas must be designed to create a hardline barrier between lobby and the workspace to prevent unauthorized access to Company facilities.
  f. All ingress/egress points must be badge-in and badge-out with a protected emergency door egress release mechanism on the interior Company side of the door. (Note, badge out may not be activated as this is dependent on threat level and input by local management, however the reader must be installed).
  g. All personnel entering a Company facility must verify the badge in their 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 can install a reader on or near the reception desk to facilitate this requirement.
  h. All critical physical security systems should be connected to the site emergency power system or have some type of uninterrupted power source (UPS), either battery back-up or generator power, to ensure consistent functionality for a minimum of 2 hours.
  i. The site must maintain a regularly scheduled service/testing schedule for all security systems.

Securing Company Facilities

- In High Risk sites, such as global/regional headquarters, R&D Facilities, Planning Service Centers, Plants, Mixing/Distribution Centers, etc. there must be a site contract security service accountable to P&G.

- External Doors – all external doors must be kept closed except when in use. In addition, all exterior doors must be alarmed (ensure door "forced" and "held" alarms are programmed) with local audible and signal back to the site access system. Installation of access control system readers requiring badge in and badge out by authorized facility residents is required (Note, badge out may not be activated as this is dependent on threat level and input by local management, however the reader must be installed).

- Emergency exit only doors must be alarmed with local audible alarms and send a signal back to the access control system. There must be no hardware or key lock on the external side of the "emergency egress only" doors.

- Windows - Windows that are easily accessible from the ground up to 5 meters in height are protected with locking mechanisms and either anti-shatter film, glass-break detectors, motion sensors, CCTV or security patrol.

- Alarms – All site security alarms must be dealt with in real-time. Response from either on-site personnel or off-site responders must be immediate upon alarm activation. Multi-layered intrusion detection alarms must be activated upon site closures or instances of emergency. If a site has a panic (silent) alarm, all activations must be responded to in real-time. All site intrusion detection systems must have individual access codes for activation/deactivation that can be audited. Preventative maintenance plan and alarm testing functionality must be conducted on a minimum quarterly basis.

- Exterior Roof Access - Exterior roof access ladders must be secured via locked protective anti-climb guards to prevent unauthorized access. There is also a need to inspect the exterior sides of the building(s) to determine if there are other means to climb the building via electrical conduit, steel girders, etc. to ensure these cannot be used to gain access to the roof. If determined any of these can be climbed, they also must be protected to prevent accessing the roof.

- Interior Roof Access – Must be secured via pad lock or mortise lock (high security or replaced on a regular basis) and alarmed.

- Overhead Doors – all overhead doors (shipping/receiving areas) must be constructed of solid metallic materials that delay unauthorized access into the facility. As in all external doors, all overhead doors must be shut and locked when not in use. Locking mechanisms can include hardened padlocks (with limited keyed access), mechanical closures and steel pins. In addition, intrusion detection devices on the doors are required, to include access control system door contacts or infra-red motion detectors. CCTV must be present on the internal side of loading docks.

- Work areas, such as: offices, conference rooms, and huddle rooms within the secure perimeter must not be shared with non-P&G personnel (i.e. visitors) unless escorted by P&G personnel. This does not include non-employees issued unescorted access ID badges.

Securing Company Facilities

- If shared areas, such as: auditoriums, cafeterias, etc. are used for P&G work (within leased facilities) they must be treated as any other outside facility. Ensure Information Security principles are followed; all sensitive documents must be disposed of in the proper manner usually accomplished using a crosscut shredder or secure shredding service.

- Business Use Areas – For Example: Labs, Intermediate Distribution Frame / Main Distribution Frame (IDF/MDF) rooms, site utility rooms, record storage rooms, etc.

  a. Require additional access control procedures to be in place beyond general site access control procedures. Examples can include mortise locked doors, staffed entrances, monitored intrusion system etc.
  b. All visitors must only be allowed access via authorized escorts.

- Highly Restricted / Secret Areas - For Example: New Initiative Security team collaboration spaces, Site Data Centers / Server Rooms, Innovation areas/Labs, government compliance program areas, executive meeting spaces, etc.

  a. Must have role based / auditable access control procedures in place utilizing an access control system pin pad reader (individual pin-codes) with access for authorized personnel only managed by area business owner.
  b. Intrusion system and recorded CCTV coverage linked to site system following Company standards.
  c. CCTV Camera looking towards the door from the inner side.
  d. The exterior walls of the room must extend from floor to deck to prevent climbing over the wall via ceiling access.
  e. The door(s), hinges are either on the inner side or secured against easy removal.
  f. There are no exterior signs that indicates the real function of the room.
  g. Requires an audit trail that indicates who entered with the date and time of entry into the area recorded in the access system.
  h. The area business owner must conduct quarterly reviews of room physical access control reports, access reader overrides from authorized access system users, alarm data, and CCTV recordings.
  i. All visitors must only be allowed access to the area via full-time authorized escorts.

- Install camera system in select areas to improve facility monitoring capability, all views must be digitally recorded and archived for a minimum of thirty days/maximum sixty days.

  a. All camera images must be recorded following Company record retention policy and local law/regulations regarding recording of images. Must comply with Privacy Policy and all security related cameras must be linked to central CCTV system of facility.
  b. All personnel entry doors (in staffed reception, personnel entry only without reception or guard present, stairwell/emergency exit only, etc.) must have CCTV positioned on them; they must not be installed with the intention to surveille individual workstations or conference rooms
  c. Vehicle entrances to our facilities (Plant and Distribution Center Shipping & Receiving, R&D Innovation Centers, and General Offices with garages) must also be equipped with cameras to record images of vehicle license plates and drivers entering and exiting the facility.

Securing Company Facilities

d. Consideration must also be given to loading dock internal areas and restricted areas, such as: cash handling operations, records storerooms, site utilities and/or senior management office areas.

- Key/Lock Control – All site key/lock controls are to be established and managed per the local business unit needs. Minimum expectations include establishing a management system for the site that documents, tracks, creates and maintains key/lock inventory control for all mortise style door locks, padlocks and miscellaneous office locks (desks, filing cabinets, storage lockers, etc.). In addition to the establishment of an inventory control system – the site should document quarterly reviews of the system to ensure the proper use and accountability of assigned/un-assigned company keys/locks.

- Customization Sites – all areas of the facility engaged in customization practices must be segregated from site operations and have restricted access. Any finished goods and promotional items (inserts, coupons etc.) must be securely stored within the customization area and a method of reconciliation of content inventory must be deployed. Any individual personnel storage areas must be separated from the customization areas and exit searches of personnel must be conducted (per local regulations).

- Parking areas must be well lit and illumination levels must be adequate to support CCTV recordings and in accordance with P&G Lighting Standards. It is required to monitor parking lots with cameras and conduct patrols with security personnel. Personnel escorts must be provided upon request.

- Leased Facilities - in addition to implementing the above-mentioned security practices, in a leased facility the building property management/landlord may provide various services as part of the lease. These may include security, cleaning services, mail handling, etc. The following precautions must be taken:

  a. Security Services - Ensure a list of all personnel authorized to access P&G areas is maintained, this must include P&G employees, cleaning services, security personnel, mail personnel, shipping and receiving personnel, etc. Individual's names must not be added to this list without prior notification and approval of the P&G representative. Access to the facility for P&G and non-P&G individuals must be removed immediately upon departure of employ. Security Service must be accountable to P&G; this can be the same service provider used by the landlord or a different security service provider.
  b. Cleaning Services – Maintain current list of personnel which includes managers and supervisor's emergency notification phone numbers. Hours of service must be strictly controlled and access to the facility must be only for the hours required to complete predetermined tasks. Ingress and egress of cleaning personnel during their work hours must be strictly controlled and minimized to only what is needed to accomplish required tasks. Trash removal must be strictly controlled by site security, ensure all sensitive documents are shredded and be aware of their disposal/removal procedures.
  c. Tenant screening/due diligence prior to entering into a lease contract of our facilities to ensure they are not competitors. This must also be accomplished when exploring the option to lease space on behalf of the Company in a multiple tenant facility. The screening process must also include data gathering on tenant's company profile, visibility level in community/country/world and if the company conducts controversial

Securing Company Facilities

business operations. Carefully weigh the risk of business interruption due to other tenant's high profile (e.g. Embassies) for civil disturbance (including picketing, riots, bomb threats, etc.).

d. Mail Services – Provide and maintain procedures for shipping, receiving, processing, and distributing of all Company mail. Attention must be given to providing procedures for authorization of individuals designated to sign for courier shipments and deliveries. Avoid having Company mail mixed with mail of other facility tenants.
e. Information Security - special emphasis in training employees to avoid work related conversations when in public/shared spaces must be conducted to ensure non-P&G employees do not overhear conversations.
f. Ensure all items listed above are negotiated and incorporated into the contract prior to signing the lease and taking occupancy of the facility. Attention must be given to access control issues regarding who can access the facility/P&G space and how they can access the facility/P&G space. The most effective method for reducing risks associated with public/shared spaces is to design them so that all the required support functions are available in a self-contained area outside of P&G areas. These concerns must also be addressed and incorporated into the contract.

3.0 Policy Risk Acceptance

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 - Risk Acceptance Form.