Physical Security Policy

February 2021

genpact

Transformation Happens Here

Notice

The information contained in this document is not to be used for any purpose other than the purposes for which this document is furnished by GENPACT, nor is this document (in whole or in part) to be reproduced or furnished to third parties or made public without the prior express written permission of GENPACT.

Version Control

Version No.	Version Date	Changes	Owner/ Author	Approver	Date of Review/Expiry
1.0	4-11-15	Created	Antara Chatterjee	Vineet Sehgal	Until Superseded
1.1	3-23-16	Review	Antara Chatterjee	Vineet Sehgal	Until Superseded
1.2	5-1-17	Review	Antara Chatterjee	Vineet Sehgal	Until Superseded
1.3	2-1-18	Review	Antara Chatterjee	Vineet Sehgal	Until Superseded
1.4	2-8-19	Review	Antara Chatterjee	K Ram Kumar	Until Superseded
1.5	2-7-20	Review	Neelesh Singhal	K Ram Kumar	Until Superseded
1.6	2-2-21	Review	Neelesh Singhal	K Ram Kumar	Until Superseded

Agenda

1. Overview

Genpact recognizes its responsibility to maintain a secure working environment, to protect its employees, customers, vendors, premises and assets. The Global Security Policy provides the methodology to fulfill this responsibility.

GENPACT is committed to providing quality workplace conditions that foster a safe and secure environment for its Employees, Customers and Visitors, and safeguard its facility from intruders for theft, violence or any kind of physical danger.

The Security Policy shall assist the security and logistics team in the implementation and management of a Security Plan.

- Based on the effective laws this Policy specifies the internal rules, procedure and behavioral forms that guarantee the security of the Company and specifies the scope of authority, responsibility and competency of the executive organization and leaders in security issues. It regulates the application of the effective general laws and internal policies related to employees, protection of the company assets, order, security and work discipline.
- It is the responsibility of the Chief Security Officer, Site Logistics Leader, Site Logistics Manager and Security Manager to enforce this policy.

It is essential that all employees participate in the security program by:

- Taking reasonable care of their personal security.
- Taking responsibility for Genpact and customer assets in their care.
- Assisting Genpact in complying with its statutory rules, duties and regulatory requirements.
- Being knowledgeable about security policy and procedures.
- Reporting their immediate supervisor and security manager of any security risk or incident.
- The Genpact Global Security Policy contains minimum security standards that all Genpact businesses will adhere to.

2. Principles

GENPACT intends to achieve this mission by having Policies and Procedures

- A dedicated Facility Management/Security Team that owns the Policies, Procedures & Security Standards.
- Technology to monitor people and material movement within the facility;
- Trained Security Guards, where applicable, to monitor people and material movement in and out of the premises.
- Regular audits to ensure compliance and find improvement opportunities. Written recommendations/observations on process performance post the audits concerning security deficiencies to be highlighted to the Leadership Team, together with a priority list for implementation of corrective actions.

3. Business Partnership Charter

For all Genpact businesses, the global physical security team works in a cooperative manner to address the business's physical security concerns, to assess specific operating risks, and to establish mitigating security controls through the following processes:

- Risks are identified and evaluated as per likelihood and effect.
- Systems and processes are evaluated for operational efficiency and effectiveness.
- Business objectives are supported within the scope of the Security Policy.
- Security officers are deployed to manage/monitor the facilities 24*7
- Contact is continuously maintained with law enforcement, intelligence agencies and appropriate business security groups.
- Communication is maintained with business representatives and employees.
- A state of "Operational Readiness" and response to emergency situations is maintained.
- The business is assisted in implementing specific security programs and requests.
- Internal security expertise is provided.

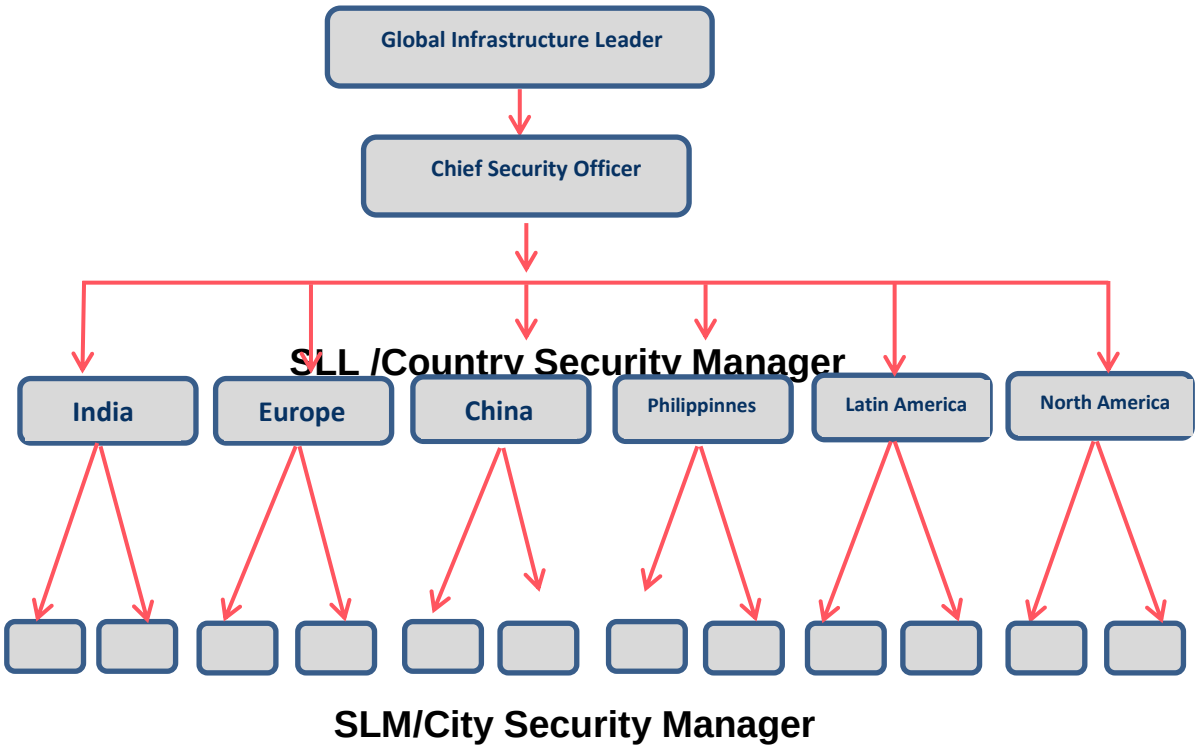
- Security contracts, budgets and allocation/chargeback processes are managed.
- Physical security functions are managed at sites and comply with legal, regulatory and policy requirements.

4. Scope

This Policy is applicable to all Genpact facilities, its subsidiaries, and its managed affiliate's.

5. Physical Security Organization

Genpact recognizes its responsibility to maintain a secure working environment, to protect its employees, customers, vendors, premises and assets. The Global Security Policy provides the methodology to fulfill this responsibility.



6. Policy Requirements

The Genpact Global Security Policy takes precedence over all existing physical security policies and procedures. Individual business' security policy requirements and issues as articulated in Client MSA's must be coordinated through Site Logistics Managers/ Site Security Manager. Amendments or additions to the policy will be based upon an assessment of the risk, business operating needs and identification of appropriate security solutions to those needs. These should comply with all applicable national and international regulatory requirements, standards and laws governing security practices, and related programs and systems wherever Genpact office is located.

7. Review and Evaluation

The Security policy shall be reviewed by the Chief Security Officer at least once a year or when there are significant changes, to ensure it remains appropriately updated to reflect the changes.

8. Facility protection

8.1 Layered Security

Physical Security team must assess risk and provide a "layered" security system that addresses the risks identified. This will be in accordance to the various types of facilities occupied:

1. Owned facility.
2. Leased facility (Single Tenant)
3. Leased facility. (Multi-tenant).

The concept of layered security refers to a physical security plan that provides rings of security protection around the facility. For example, any combination of:

- **Level 1** – Perimeter level controls.

- **Level 2** - Building Level controls.
- **Level 3** – Floor Level controls.
- **Level 4** – Client / Business level controls.

8.2 Entry to Facility

Entry Controls - Facility Entry (Building/Floor, as applicable) controls should provide reasonable assurance that physical access to the facility is restricted only to authorized people and material.

Entry is permitted only to the following classification of people: Employees, New Joiners, Interns, Resident Vendors, Official Visitors, Drivers, Interview Candidates, Vendors, Clients and Government Visitors.:

9. Employee Controls

9.1 ID Cards

Employees are always required to wear and display their ID cards when inside the company premise and when using official transport and only Genpact issued Lanyards will be used for wearing and displaying ID cards around the neck.

9.1.1 Non-Adherence to ID Policy

Employees are always required to wear and display their ID cards when inside the company premise and when using official transport and only Genpact issued Lanyards will be used for wearing and displaying ID cards around the neck.

9.1.2 Cards Rejected on Reader

If an employee's entry is rejected with their ID Card, he/ she would have to come back to the Security Reception/Badging to get the card status checked. Rejected card will be checked by the Badging Department for reactivation or replacement.

9.1.3 Random Checks

Security Guards, where permitted under law are authorized to randomly check the employee bags upon exiting the facility and findings noted in a register.

9.1.4 Security Checks during high alert situations

During high alert situations based on CSO's approval/communication security guards will scan or manually check the bags for employees entering the facility.

9.2 Employee Physical Access Grant & Revoke

All activities related to access grant and revoke are carried out by the Central Badging team reporting to the Chief Security Officer. New Joiners/ Vendors/Contractors access grant is facilitated by the site badging/security team.

- Employees are provided general access (access to common areas of the facility) to the facility post completion of onboarding formalities and basis confirmation from HRSS/HR. All other client segregated area access is provided post approvals from the relevant business/floor controller.
- Access to any card-based access controlled area will be provided post approvals from the relevant owner of the space or designated controllers or SPOCs.
- Either an email based or ticket-based process can be followed.
- Access swipe logs are retained for a period of 18 months
- In case of access control system going down, reasonable controls will be deployed to control unauthorized entry into the facility.
- Profile data will be retained and available for a period of 7 years

9.3 Forgot ID card

All activities related to access grant and revoke are carried out by the Central Badging team reporting to the Chief Security Officer. New Joiners/ Vendors/Contractors access grant is facilitated by the site badging/security team

9.3.1 Employee Authentication

In case an employee is not carrying his/ her Identity card, authentication of the Employee must be carried out before issuing them

the Employee- Temporary Card. Access on the employee's permanent ID card will be deactivated before issuing a temporary card. Temp cards will only be issued for a maximum of 3 consecutive business days. Business and HR leader to approve issue of temp card beyond 3 consecutive days.

9.3.2 Deactivation of Lost/Forgot Card

Access to all lost/Forgot ID cards must be deactivated immediately upon the confirmation from the employee to the security.

9.4 New Joiner Entry

On the first day of the New Joiner a visitor card will be issued before a permanent card is issued. Post completion of the onboarding formalities by HRSS, the new joiner will visit the badging room/ designated place for issue of a permanent ID card. New ID card will be issued upon verification of details provided by the HRSS team

Vendor/Contractor/Consultant candidates will be issued a new ID card post completion of the formalities as detailed in the BPMS. Access will be granted for a maximum period of 3 months and reviewed at the beginning of each quarter.

9.5 Employee Access Deactivation

9.5.1 Exit Deactivation

HR informs Security team/Central Badging to deactivate the Access card through the Oracle Exit Process or on email. Access on the card will be deactivated within 24/48 business hours (as applicable). The access cards will be kept under Lock and Key and the access for the same will be deactivated.

9.5.2 Absconding Employee

The employee Manager/HR need to communicate to the badging team about any employee on uniformed absence for 5 working days. Access for absconding employees will be deactivated within 24/48 business

hours (as applicable) post email confirmation /exit trigger for deactivation of access.

9.5.3 Internal Movement

Access for employees moving /transferred from one business to another will be deactivated basis the internal movement trigger / email confirmation from HR/Manager. Access on the card will be deactivated within 24/48 business hours (as applicable).

9.5.4 Return of ID card

Any employee exiting Genpact must return their ID cards on their last working day to their HR/Manager/ Security/Facility Department. The HR (Human Resources) /ERM (Employee Relationship Manager) need to track their exiting employee and submit all returned cards to the facility team. The employee ID card once collected will be shredded by the facilities team however HID cards will be re-used after a cooling off period of 18 months. The MIL cards and lanyards will be shredded.

10. Visitor Controls

10.1 Entry to Facility

All visitors to the premises have to be authorized by an employee before they can be allowed entry to the premises. Visitor card will be issued to visitors and the Details and belongings of the Visitor would be noted. They will have to produce a Photo ID proof (Govt. Issued photo ID/company card) for authentication and declare electronic or any other assets that they will carry inside the facility.

10.2 Visitor Escort

Visitors have to be escorted at all times during their stay on the premises and only

Official Visitors should be entertained on office premises and employees cannot host Personal visitors in the office. Any visitor visiting the facility and requesting for an access card will be issued post business SDL approval. Card will be issued from the reception and has to be returned post the completion of the visit.

10.2.1 Visitor Checks

Visitors can be randomly frisked. At the exit gate the Visitor has to surrender the Visitor Card and Countersigned Visitor's Slip (if applicable) with Out Time. Security guard where permitted under law is authorized to randomly check the visitor's bags upon entry/exiting the facility and will also check the items that were declared upon visitor's entry to the facility.

10.2.2 Visitor Management System (VMS)

All Visitors processing will be done through VMS system at facilities where it is operational. Government visitors will be allowed entry to the premises without registration post confirming their identity. In the event of a large group of visitors visiting the facility and if it is felt by the operational team that VMS process will delay the entry, then approval on case to case basis will be taken from CSO and documented. In such cases, manual record will be maintained.

10.3 Interview Candidates Entry

The security guard will verify photo identification of the interview candidate before issuing a visitor / HR interview card and details of the candidate will be noted.

11. Vendor Controls

11.1 Entry to Facility

All Vendors to the premises have to be authorized by an employee, vendor supervisor, authorized escort before they can be allowed entry to the premises.

11.2 Authorized Vendor List

Site Facility and Sourcing manager are responsible to maintain an up-to-date Vendor list, containing the accurate list of contracted companies, whose employees are provided regular vendor access card to the site.

11.3 Issuance of ID card

All resident Vendors will be issued Permanent ID card post authorization from their parent company.

12. Special Events

At times the Organization holds Family Programs, where Employee relatives are invited to the premises. At such times, the Visit Coordinator should intimate the Security Reception of people expected at the premises. The visitors will undergo the Visitor Entry process to gain entry into the premises. Personal / Family visitors are only allowed on the floor during Family Connect program and basis approvals from the Business SDL and the facilities team.

13. Vehicles Entry

13.1 Entry to facility

Access controls and security screening should provide reasonable assurance that physical access to the facility, where applicable, is restricted only to authorized vehicles. Entry for Vehicles will be through designated / authorized entrances only. Security Guard may randomly check any Vehicle entering the premise. Based on the local situation all vehicles entering the facility can be checked.

13.2 Parking Sticker

Employee has to submit the following documents for issuance of a Parking Sticker:

a. Driving License copy
b. Vehicle Registration Certificate copy
c. Employee id card copy

In case the vehicle belongs to employee's relatives, a No Objection certificate and ID copy of the vehicle owner should be submitted along with the above documents. In case the employee changes the vehicle, the old parking sticker has to be surrendered and a new sticker will be issued against the same. Exit employees have to surrender the parking sticker before leaving the organization.

13.3 Employee Vehicles

Only employee vehicles with Genpact sticker/Sticker issued by facility developer would be allowed. Security Personnel will verify identity of each passenger of the vehicle entering the premises. Parking will be at owner's risk.

13.4 Personal Driver Entry

Where applicable drivers of Employee Personal vehicles would be allowed to enter the premises basis Temporary ID card issued post approvals from Logistics/Security teams. A Police Verification certificate has to be submitted for the personal drivers before ID card is issued. Green Color Lanyards with DRIVER inscribed on them will be issued to the personal drivers.

13.5 Vendor /Contracted Vehicles Entry

Only supply Vendor Vehicles carrying water, food, fuel, supplies for Convenience Stores etc. would be permitted on the premises. Vendors must authorize a select set of vehicles to be allowed on the premises and communicate to facilities team. Any other vehicle will have to be approved by the facilities team before entry to the facility.

13.6 Cab Entry

Radio cabs will be allowed entry into facility for pick up and drops for employees post security checks at entry and verification of driver company id. Genpact transport vehicles are allowed inside the facility only post completion of their onboarding formalities and approvals by the site Genpact transport team.

14. Additional / Heightened Security Measures

Based on the local situation and advisory by government agencies, additional security measures may be put in place by the CSO or Site Facility Leader. This will entail the following:

- Bags will be scanned / checked while entering Genpact premises.
- Under vehicle scanning/checking will carried out.
- Vehicles entering the premises will be physically searched.
- Random checks on exit will be carried out.
- Additional guards may be deployed across sites to keep workplace safe & secure.
- Other security procedures for work place and travel security will continue to be followed.

15. Material Entry

15.1 Material In

Incoming deliveries should be properly checked, recorded at the security Reception desk. The notification of returnable / non-returnable is made on the document being carried along with the material. The employee responsible for receiving these deliveries, together with the Security Guard should ensure all supporting documents

(i.e. delivery receipts, invoices, job / purchase orders, etc.) are gathered and handed over to concerned section / person

15.2Material Out

No company property will be allowed out of the Company premises unless covered by a MRN (Material Requisition Note) duly approved by the authorized signatories except for company issued laptops and other IT equipment as issued to the employee as per the IT policy.

Genpact recognizes its responsibility to maintain a secure working environment, to protect its employees, customers, vendors, premises and assets. The Global Security Policy provides the methodology to fulfill this responsibility.

16. Mailroom Policy

All incoming mails should be scanned and stamped by security before being brought inside the mailroom / designated area. The employees handling the mails must be trained on how to identify, segregate and appropriately manage hazardous material.

17. Suspicious Packages/Objects

- If at any time a suspicious package is observed in an area, where no package should be, the local Security Administrator and designated management personnel should be notified.
- If after investigation the package is deemed suspicious, the security administrator or management should call law enforcement authorities to investigate.
- Under no circumstances should any suspicious package be touched, moved, or otherwise disturbed.
- The area around suspicious packages should be evacuated to at least 200-300 feet in all directions.

- Person finding the suspicious package or object should be available for further questioning.
- Management must pre-determine procedures for evacuation. If a suspicious package is found or threat assessment warrants an evacuation then the local Law enforcement authorities should be notified immediately.
- The local Security Administrator and/or law enforcement may determine from an assessment of the package/object size and characteristics if the entire building should be evacuated.

18. Customized Access Control

Access to the customized access areas will be strictly regulated, and limited to only those personnel necessary for its operations. The following areas will come under customized access control

18.1Server Rooms, Clean Rooms/ODC, Hub Rooms, Battery Rooms

Clean Room access would be GENPACT controlled third level access. Any client specific requirements of isolation will be addressed specifically.

18.2 Visitor Entry

For any visitor or non-access granted personnel entry, authorization must be sought from the owner of the respective space. Any Visitor can enter the access controlled areas only if escorted at all times by an authorized personnel. Visitor details should be documented.

18.3 BCP Command Center

BCP Command Center, where operational would be restricted access.

19. Red Zones & Out of Bound Areas

19.1 Red Zones

For each site the following areas would be earmarked as Red Zones.

- Data Centre/Server Room
- Hub Room
- UPS Room
- Battery Room
- Telephone equipment room
- UPS Distribution Box room
- CCTV & Engineering Room

19.2 Out-of-Bound Areas

Each site will nominate Out of Bound areas as applicable. The following areas must be ear marked as Out-of-Bound Areas:

- All AHU (Air Handling Units) rooms
- All Electrical and Plumbing Shafts
- Sub stations and DG (Diesel Generators) Rooms

No Employee will have access to Out-of-Bound Areas except Facilities, Engineering and Security team.

20. Business Carve Outs / Client-specific Restricted Area

- Client-specific restricted work areas are physically segregated and Access Controlled areas restricted for carrying out operations for a specific customer and access is granted to employee group associated with their business or supporting the business.
- For each client, basis their requirements and policies, a specific process will be defined for Employee access, Visitor access and Vendor access to these areas
- Only the designated Genpact SPOC(s)/Floor Controllers directly servicing the particular client will have the authority to approve access of such business carve out
- The Authorized Employee approves entry and accompanies visitors and vendors in the Client-specific restricted area.
- Monthly reconciliation of people having access to the carved out/access controlled areas will be carried out.

21. Lock & Key Policy

- All keys of high risk or restricted areas shall be kept in an approved key cabinet under the control of security/ designated personnel
- Duplicate keys to all offices, meeting and training rooms will be kept for safekeeping with Security and should only be used in case of emergency or unless duly authorized by the Facility Manager.
- Any key issued or handed over to any employee would be appropriately documented.
- An inventory of the key locker should be maintained on the premises at all times. It will be reviewed on a monthly basis.
- Employees who relocate or end their employment must return all keys to the custody to security staff.

22. Access Control System

- The ACS deployed at each site should be as per the regional set up across Genpact sites (Lenel Onguard, CCURE, C4)
- ACS should have photograph of each employee and should be able to record access at multiple levels
- The ACS Software should be able to provide data for number of people who gained entry and exit to the premises and access controlled areas.
- ID Badgeing should ensure that at any point of time there is access swipe data available for 18 months.

23. Transport Security (where ever applicable)

- Safety guidelines must be used to drop and pickup employees from their respective locations on a daily basis.
- Employees will be responsible for all their belongings. Genpact takes no ownership of Employee's personal assets and would not be liable for any theft during transportation.
- First pick up and last drop will not be a female employee wherever transport is provided without a security guard or other male employee will accompany in such cases.

24. CCTV

Close Circuit TV Cameras have to be installed in all the facilities, and should be used for monitoring the day-to-day operations in and around the premises. CCTV Cameras should be installed to cover the following areas:

1. Entrances and Exits ,Lobby/Visitor area/Waiting room
2. Red Zones
3. Fire Exit Doors
4. Perimeter Walls (own facility)

- Camera will be placed at the entry & exit doors on both sides and for emergency exits only on one side.
- All CCTV camera spread across the building will be backed up by UPS power supply.
- The back up retention period is 30 days for CCTV footage or as defined by customer MSA.(basis CSO approvals)
- During periodic maintenance, personnel must ensure that the vision of the CCTV surveillance system and beam detectors is not restricted by any obstruction.
- Employees are responsible for their belongings (assets) inside the facility and Genpact will take no responsibility of the loss. Personal belongings will not be checked in CCTV.
- CCTV records for personal loss cannot be viewed. It can be viewed only on special request and approved by the Business leader /Facility Manager or the Security Manager. In case required for any specific incidents, the HRM/Compliance manager of the employee/process may be permitted to view basis approvals from facility manager/security manager.
- If theft of any official equipment is reported, the CCTV cameras can be used to verify location and events. Necessary actions can be initiated against the person, once identified.
- Escalation for faulty CCTV Cameras – Security Guard checks all CCTV Cameras and maintains a log in the CCTV register. In case of discovering a faulty camera, the security guard will inform the same to the Site Engg team and mark the facility manager. A ticket will be logged with the AMC vendor and record maintained of the same.
- Photography is prohibited at Genpact sites and any exception has to be approved by the SLL/Security Manager.
- CCTV footage can be shared with government authorities on the basis of valid executive order.

25. Employee Responsibility

It is the responsibility of each employee who is issued equipment from the company to ensure the security of that equipment. The employee must take reasonable measures to secure, protect and know the location of this equipment at all times and should make efforts to avoid any damage to, or loss of the equipment. In the event the equipment is lost or stolen, the employee must report the loss to their manager.

Additionally, if the equipment contains Genpact or customer information, the site Business Information Security Officer must also be informed..

26. Personal Property

Employees, clients, visitors, contractors, etc. are responsible for safeguarding their personal property. Personal items of value should not be left unattended and should be taken home at the end of the working day and not kept in unlocked desk drawers or other unsecured areas overnight or over vacation periods. GENPACT takes no ownership of Employee's personal assets and would not be liable for any theft. Any article of personal property found unclaimed in the office will be deposited with the security team who will hand-over the same to the concerned employee after verification and record for the same should be maintained. In the event the articles not claimed for a period of 3 months, the same will be disposed-off post consultation with the Site Logistics Leader

27. Maintenance of Security Equipment/ Systems - Preventive Maintenance

27.1 Access Control

Post warranty, Preventive Maintenance will be carried out for security equipment under AMCs (Annual Maintenance Contracts). Frequency of checks should be once a month or as specified in the Site Maintenance Plan or by the OEM. All sites have to follow security equipment maintenance as per schedule.

27.2 CCTV System

Post warranty, Preventive Maintenance will be carried out for CCTV equipment under AMCs (Annual Maintenance Contracts). Frequency of checks should be once a fortnight or as specified in the Site Maintenance Plan or by the OEM.

28. Security Equipment Maintenance

- The Security Team must inform facilities & Engineering Team about any malfunctioning equipment.
- The Engineering team (along with the respective Vendors) will maintain the equipment basis the planned preventive maintenance (PPM) calendar as per OEM recommendations and the Annual Maintenance Contracts / warranties.
- Downtime of security equipment will be documented by the security team and reported to the business/compliance teams as well.

29. Third Party Security Controls

29.1 General Controls

- The Security Service Provider, where applicable, shall provide Security Services as per contract.
- Security Personnel will be deployed on each GENPACT site in accordance with local applicable laws and regulations
- Service provider should also warrant that it has carried out background / reference check as applicable.
- Security guard will follow Post & Site Instruction or instructions provided by logistics/ security team from time to time.

29.2 Escalation/Incident Management Procedures

- All Security Guards should report any incident or accidents to the CCTV Security Supervisor/Crisis Response number.

- The shift Security Supervisor /ERT Supervisor should immediately inform Duty Logistics Officer and / or Facility Manager
- The Site Logistics Manager should notify Site Logistics Leader/Chief Security Officer depending on the nature/criticality of the crisis.
- All security incidents will be documented on Archer and appropriate leadership shall be informed.

30. Crisis Management

For any emergency, a quick response is desirable. Site Facility Manager should ensure the following:

- Alarm system for Fire is functional round the clock.
- CCTV Cameras will be used to monitor floors and perimeter.
- Emergency Numbers will be 24 Hrs manned by trained Security Personnel and functional. The Emergency Number should not be used for out-going calls.
- Facility Cell should be functional and manned 24 Hrs.

31. Travel Advisory

Genpact will provide travel security advisory information to employees traveling to areas of high-risk on behalf of the organization.

Genpact has partnered with ISOS (International SOS) to support our employees while they are travelling on assignments. ISOS classifies all countries for travel and medical risks.

Employees' travel is subject to the following guidelines:

- Severe Risk Countries – No Travel is permitted
- High Risk Countries – Only essential travel to be approved by CSO and travelers to receive security brief prior to travel. Business to confirm if travel is essential and unavoidable and get the consent form at Appendix signed by employee before travel
- Medium Risk Countries - Employees to receive security brief prior to travel
- Low and Insignificant Risk Countries – No restriction on travel

32. Event Security

Genpact Security Coordinators must ensure that appropriate security measures are provided at events and venues. The degree of protection will be commensurate with the risk involved. A risk assessment prior to the actual event will be conducted, which will include liaison with event planners, local police and emergency services, transportation coordinators, venue staff and security personnel. This will be coordinated by the site security team along with the event organizing team.

33. Document Shredding

Security must ensure that a sensitive document destruction process is established in each facility.

The shredding program must follow these guidelines:

- Dedicated shredders – Documents may be shredded in office by the document owner or designated person.
- Building shredders – When the shredding of documents is done centrally for the building it must include the following :
- Locked collection containers/ shredding boxes to be provided on the floors.
- Control of material being moved from the collection container to the shredder. It is acceptable for one person to move collection containers to the shredder when the containers are locked and the person moving them does not have access to the key
- Control during the shredding process. It is acceptable to use outsourced personnel for this purpose, if it is part of their job description and their contractual relationship with the company.
- Record of shredding will be maintained and signed by witnesses.
- Outsourced shredding – Document shredding programs outside Genpact facilities by an outsourced company must include a contract and stipulate that the shredding company is liable and responsible for failure to properly handle, secure and shred all documents.

34. Armed Guards and Firearms Policy

No Employee, Contractor, Vendor, or Visitor in a Genpact facility or its businesses may possess or carry a weapon, which includes Firearms (Real or Toy), Knives (Real or Toy), Police Batons or Clubs, Explosive Devices, Stun Guns, Mace or Pepper Spray, Brass Knuckles, or any other item that could cause bodily harm to another person while inside a GENPACT facility unless expressly authorized to do so by CSO via the policy exception process. It may be appropriate, under exceptional circumstances, and in accordance with the requirements of the "Prohibited Weapons" Section of this Global Security Policy, for certain Genpact personnel (security) to possess and carry lethal and/or non-lethal weapons in connection with the performance of their security-related duties. This Policy is designed to ensure that only appropriately licensed, properly trained, and duly authorized personnel are permitted to possess and carry weapons in connection with the performance of their security-related services. In such cases where local law or risk assessment requires the possession of weapons by security staff, the designated security officer will maintain appropriate documentation in the security file as well as on their person. When local law/situation requires the deployment of armed security personnel, the local law will take precedence over this Policy. The usage of weapons has to be approved by Genpact CSO

35. Site Selection

Genpact facilities team is responsible for the site selection, design, construction and maintenance of any owned or leased property and shall ensure that the site meets local and Global Security Policy requirements. CSO/Site Security Manager will sign off the security requirements at the design stage of any new site.

The following shall be considered:

- Facility design that provide minimal disruption of operational continuity if a security event occurs.
- Local crime rates and statistics.
- Emergency response times.
- Proximity to higher risk businesses or organizations.
- Proximity to hazards (ex. - chemical plants, fuel storage facilities, etc)
- Evacuation infrastructure
- Security team will work closely with the projects team from the site fit out stage of any new facility/floor.

36. Pre-Employment / Background screening

Prospective security guards & teams and out sourced service providers will be subject to applicable regional policy standards. Where allowed by local law, the below requirements should be applied accordingly.

All prospective security guards & teams must undergo an approved background assessment/police verification process that is designed to identify individuals who pose an unacceptable risk to personnel, corporate and customer assets.

The background assessment process must include the following, unless prohibited by local law:

- Verification of government issued identification.
- Criminal Background Check
- Verification of educational degree, professional certifications, etc or highest level of education attended.
- Pre-employment drug testing where legally permissible
- Personal References - Two or three character references from people who are neither related, nor residing with the candidate.

Where local law prohibits obtaining the above information, local Human Resources should define minimum standards.

All information gathered in the pre-employment screening process must be classified and maintained as confidential by the appropriate Human Resources or security teams.

37. Investigation of suspected employee wrongdoing

In order to foster an atmosphere of cooperation and fairness, investigations of suspected employee wrongdoing will be handled as follows:

- Security team/investigator will notify the Genpact Legal Team and the Senior Human Resources (HR) representative of the particular business or their

designees of the general nature of the investigation, including an investigation plan

- Security team/investigator will explore and discuss with the General Counsel and Senior HR representative or their designees the personnel-related options should any employee admit having committed any theft, bribery, fraud, or policy violation that results in a loss or should any employee fail to cooperate in the investigation.
- At the conclusion of an investigation, security team will make a finding of fact and recommend any disciplinary action that, in the investigators experience and judgment, is deemed appropriate.
- The business which employs the individual/Genpact legal team is responsible for deciding the action to be taken at the conclusion of the investigation, including, but not limited to, termination of employment.

38. Law enforcement request for assistance

From time to time, law enforcement agencies request that Genpact provides special assistance to them in connection with investigations they are conducting. All such requests will be complied with appropriately in consultation with the legal team.

It is part of security team's mission to assist Genpact in responding to law enforcement requests for assistance.

39. Security Responsibilities

The Site Logistics Manager/Security Manager/Site security team's Key deliverables include:

- Have an oversight of Security Policies and Procedures for their respective sites.
- Review of the Security Daily Report to identify and facilitate equipment requirement or maintenance.
- Review the Visitor Entry record and understand any special reasons for increased number of visitors on a particular day
- Primary point of contact for the Third Party Contract Security Guard agency

- Make certain that the contract agency performs to the specifications mandated by GENPACT and the contract document
- Facilitate any special/ VIP visits which may need additional Security.
- Periodically meet with other GENPACT Security Officers / Site Logistics Leaders to share information of challenges faced and risks mitigated.
- Provide Security awareness and communication to employees of respective facility
- Ensure that Security Awareness is part of New Hire Program.
- Ensure Sites are audited on a regular basis.
- The Site Logistics Manager and Security Manager; post required approvals should be granted access to all areas of the facility, including General Access, Red Zones, IT areas, Client-specific Restricted Areas and others. This is to provide flexibility of operations during emergency.

40. Security Manager Responsibilities

- Manage Security program.
- Administer policy and procedures as they relate to all security programs and personnel including guard management and deployment
- Continue to coordinate program of security training.
- Administrator training, and the dissemination of relevant information
- Ensure that security incidents are reported and corrective actions are implemented as necessary.
- Assist with identification, investigation and correction of any security risks.
- Liaison with representatives of local police departments and civil authorities, and regulatory agencies.
- Review the effectiveness of security programs and implement corrective procedures.
- Review and approve emergency notification procedures
- Ensure that new security equipment / systems and/or processes adequately meet policy requirements
- Ensure that Security Self-Audits are conducted and documented in all facilities
- Follow-up and ensure that any discrepancies noted in Security Self-Audits are corrected
- Initiate Policy Exception process where required
- Conduct security Risk Assessments on all new construction, remodeling and acquisitions or as required by changes in environmental conditions

- Ensure that security service providers are reputable with proper qualifications, adequate infrastructure and proven track record. Through the implementation of a vendor selection process, in compliance with corporate standards to include: request for proposal “RFP”, bidding process and contracts.

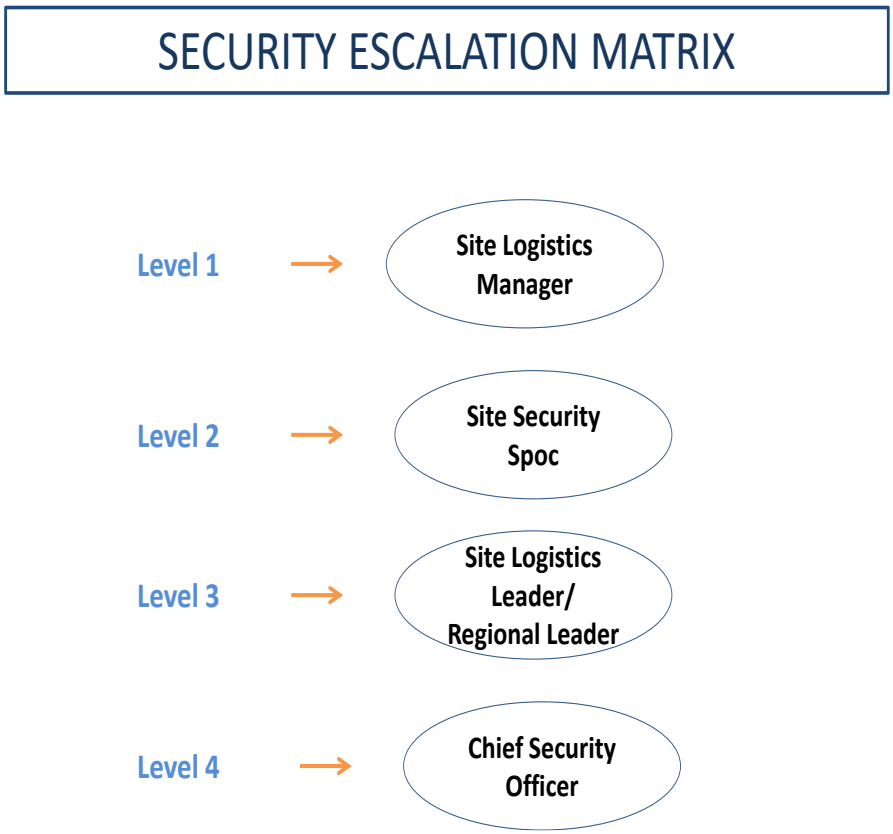
41. Security Self-audits

Security Manager’s shall conduct annual security self-audits in all facilities to monitor the effectiveness and application of all security programs.

The Business/Country Security Coordinator may require more frequent self-audits based upon an assessment of the risk.

The security Manager is responsible for reviewing all security self-audits and ensuring that appropriate corrective action is taken to remediate any problems noted.

42. Security Incident reporting – Security Escalation Matrix (As per appointment)



43. Requirements for Performance of Risk Assessments

Security Risk Assessments must be undertaken in the following cases:

- New construction projects
- Changes to local law and regulatory requirements
- Renovations or alterations for owned or leased space
- Business acquisitions
- Facility acquisitions
- Compliance inquiries or findings

Periodic Independent risk assessments will be carried out across Genpact facilities on required basis. The periodicity of such assessment will be once in 3 years or earlier basis requirement. Site security teams will coordinate this in consultation with the CSO.

44. Security Contracts Guidelines

44.1 Security (MSA/SOW) contracts

All security (MSA/SOW) contracts must meet the specifications and requirements of the Global Security Policy and Genpact procurement policies.

44.2 Vendor Selection Process:

A minimum of 3 vendors must be considered and reviewed. To qualify a vendor for security services, the following must be completed:

- Vendor name, address, and type of business
- Reference checks
- Examination of the vendor's financial and infrastructure capabilities
- Review of the vendor's standing within the security industry.
- Certification that no principals of the company have been convicted of any crime involving dishonesty, assault or morals violations.

44.3 Request for Proposal (RFP) Process

Once vendors have been qualified an RFP may be issued to vendors who have been selected to respond as part of the overall bid process. The RFP should include:

Generic information as to the service or work to be performed that may include:

- Type of service or work (Alarm Monitoring, guard service, etc.)
- Location
- Date to commencement
- Time period for completion
- Vendor contacts

44.4 Scope of Work to include specific information regarding the service or work that should include:

- A detailed description of the service or work which answers all questions the vendor may have in preparing a response
- Quantities of equipment or parts
- Number of Personnel required
- Work schedules

The process can be detailed further and should not be restricted to the above alone.

45. Power & Telecommunications cables:

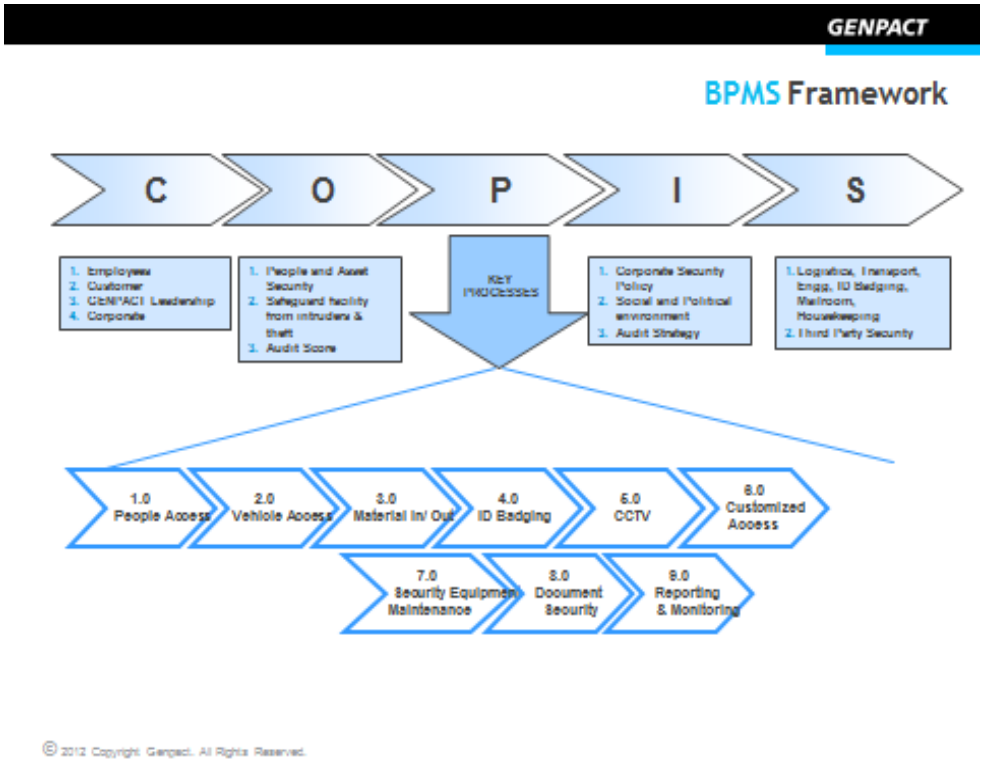
Genpact shall take adequate measures to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage

46. Exception Handling

Any exception on documented security policy/procedure can be made only post approvals from the Genpact Chief Security Officer (CSO).

47. Linkages - Physical Security BPMS

For detailed process around key physical security controls, please refer Physical Security BPMS.



© 2012 Copyright Genpact. All Rights Reserved.

48. This policy superseded any previous document on this subject.

Appendix

GENPACT [insert Entity Full name] Acknowledgement and release

Name: _____ (Please Print)

I have been given an option to travel to _____ [insert name of country] (the 'Travel'). Genpact has included this country on its list of countries where there is risk to travel. I hereby acknowledge that:

- I have been informed that the Travel entails risk from persons and entities which are outside the control of Genpact.
- I have received a risk briefing on the Travel from Genpact, including suggestions on precautions and safety measures that I can take to minimize the risks of the Travel. I have reviewed the briefing, and had the opportunity to ask all questions that I have regarding the Travel and the risks that this Travel entails (the 'Risks'). I understand and acknowledge the Risks.
- I understand and acknowledge that I have been given the opportunity to refuse to undertake the Travel. I am agreeing voluntarily to the Travel and to accept Risks.
- I agree to take all suggested precautions and safety measures and exercise appropriate caution during the Travel.
- I understand that during the Travel I am covered by insurance procured by the company. Genpact's sole and exclusive liability to me for the Risks is through recovery against such insurance.
- This release is made in consideration of the benefits of undertaking the Travel. I, on behalf of myself and anyone who has or obtains any legal rights or claims through me, acknowledge and aver that I am participating in the Travel voluntarily and release, hold harmless, discharge and agree not to bring suit against Genpact, its parents, subsidiaries, affiliates, divisions, joint ventures, and related entities, including but not limited to their successors and assigns, and their past and present directors, officers, agents, employees, fiduciaries of any employee benefit plan or policy, in both their individual and representative capacities, from all waivable claims, demands, actions, judgments or other loss or harm arising from or in conjunction with any acts or omissions of all aforesaid parties of any kind whatsoever, including but not limited to, any injuries to person, property, real or personal or any other claim of loss or harm caused by or arising out of my voluntary participation in the Travel.

Having read this release and understanding its terms, I execute it voluntarily and with full knowledge of its significance.

Employee's Signature: _____
Date: _____

Thank you.