genpact

Transformation
Happens Here

Physical Security BPMS

Infrastructure & Logistics

Physical Security BPMS

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.

Classification: Genpact Internal

Version Control and Amendment Matrix

Version	Date	Changes	Approver	Owner/Author
4.1	01-08-12	Change in the new ID issuance Process	Sandip Chandok	Maneesh Sharma
4.2	17-09-12	Exception for Client Segregated Area	Sandip Chandok	Maneesh Sharma
4.3	08-02-13	Added Security Document Retention period	Sandip Chandok	Maneesh Sharma
4.4	14-08-13	BPMS Review	Sandip Chandok	Maneesh Sharma
4.5	04—07-14	New site added & BPMS Review	Vineet Sehgal	Maneesh Sharma
4.6	18-05-15	BPMS Review	Vineet Sehgal	Maneesh Sharma
4.7	04-09-15	BPMS Review	Vineet Sehgal	Maneesh Sharma
4.8	14-06-16	BPMS Review	Vineet Sehgal	Antara Chatterjee
4.9	07-04-17	BPMS Review	Vineet Sehgal	Antara Chatterjee
5.0	15-02-18	BPMS Review	Vineet Sehgal	Antara Chatterjee
5.1	01-03-19	BPMS Review	K Ram Kumar	Antara Chatterjee
5.2	20-02-20	BPMS Review	K Ram Kumar	Neelesh Singhal
5.3	15-02-21	BPMS Review	K Ram Kumar	Neelesh Singhal

Classification: Genpact Internal

Definitions

Security: That state where Genpact's employees, physical assets, data and reputation are adequately protected against attack and damage.

Incident: Any occurrence resulting in physical security defenses being weakened/negated resulting in potential or actual harm to employees, damage to the company, business unit, brand, or financial stability, triggered by either a sudden event or a long-standing issue.

Impact: Incidents causing unplanned downtime impacting service delivery/revenues or any event which may have the risk of impacting relationship with clients.

Material impact: Any unforeseen unplanned event beyond the control and influence of Genpact and having adverse effect on Genpact people, property, delivery or revenue will constitute Material Impact.

Non-material impact: Would constitute any unforeseen, unplanned event that would impact softer and non-tangible parameters such as client relationship etc. that will/may not have any direct impact on delivery and revenues.

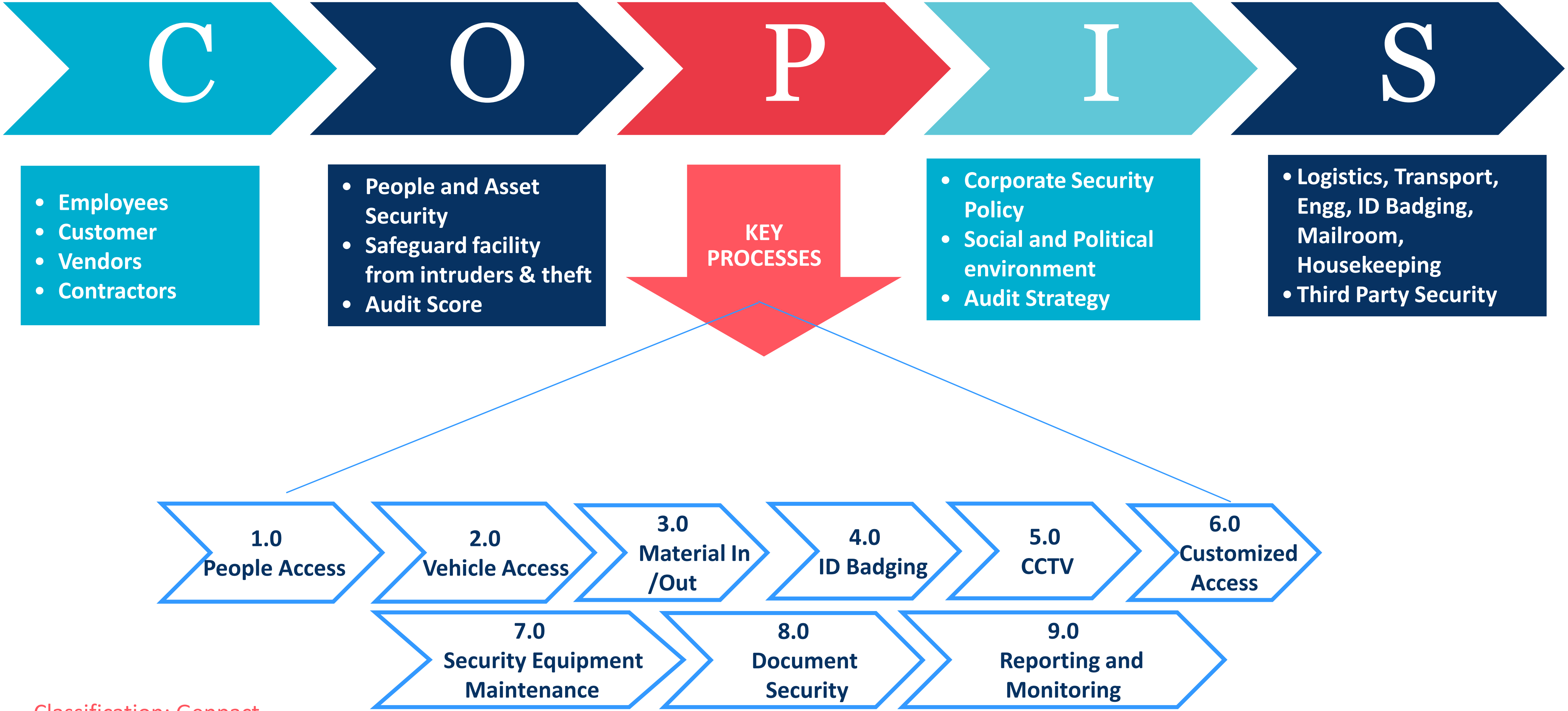
No impact: Would constitute any planned or unplanned event, the effect of which is minimal/nil/mitigated by Genpact due to the redundancies/contingencies put industry best practices or past learning's from incidents within and outside Genpact. This would also include incidents which impact softer and non-tangible parameters such as client relationship etc. that will/may not have any direct impact on delivery and revenues.

Few examples:

- Failure of Genpact electronic security systems protecting operations e.g. CCTV camera not operational; access card reader not operational
- Unauthorized person/s gain access to restricted area e.g. data center, carved out production area
- Theft of equipment e.g. computer CPU, laptop etc
- Bomb blast or a terrorist activity in a neighboring place around Genpact locations having no effect on operations

Classification: Genpact Internal

BPMS Framework



C

- Employees
- Customer
- Vendors
- Contractors

O

- People and Asset Security
- Safeguard facility from intruders & theft
- Audit Score

P

KEY PROCESSES

I

- Corporate Security Policy
- Social and Political environment
- Audit Strategy

S

- Logistics, Transport, Engg, ID Badging, Mailroom, Housekeeping
- Third Party Security

1.0 People Access

2.0 Vehicle Access

3.0 Material In /Out

4.0 ID Badging

5.0 CCTV

6.0 Customized Access

7.0 Security Equipment Maintenance

8.0 Document Security

9.0 Reporting and Monitoring

Classification: Genpact Internal

Table of Contents

0.0 Introduction

0.1 Organization Structure

0.2 Access Level

0.3 Operational Definition

1.0 People Access

1.1 Employee Access/Forgot ID employee access

1.1.1 Outstation Employee

1.2 Visitor /Vendor/HR Interview Access

1.2.1 Project/ Long Staying Customers

1.3 Resident Vendor Access

1.4 Driver Access

2.0 Vehicle Access

2.1 Issuing of Vehicle Stickers

2.2 Employee Vehicle Access

2.3 Vendor Vehicle Access

2.4 Contracted Vehicle Access

3.0 Material In/ Out

3.1 Material In

3.2 Material Out

3.3 Mail Handling

4.0 ID Badging

4.1 New ID Cards Issuance

4.2 Lost ID Card & Damaged ID card

4.3 Card Deactivation

4.4 Monthly Access Reconciliation Process

4.5 Access Grant Process

4.6 Access Card Inventory

5.0 CCTV

5.1 CCTV Equipment & Monitoring

6.0 Customized Access

6.1 Data Server Security

6.2 ODC/ Carve Outs Access

7.0 Security Equipment Maintenance

7.1 Preventive Maintenance

7.2 Corrective Maintenance

8.0 Document Security

8.1 Printer Documents

8.2 Bin Documents

8.3 Shredding Process

9.0 Reporting & Monitoring

9.1 Daily Security Report

9.2 Reconciliation of VMS Cards

9.3 Inventory Kit

9.4 Facilities Audit Process

9.5 Incident Management

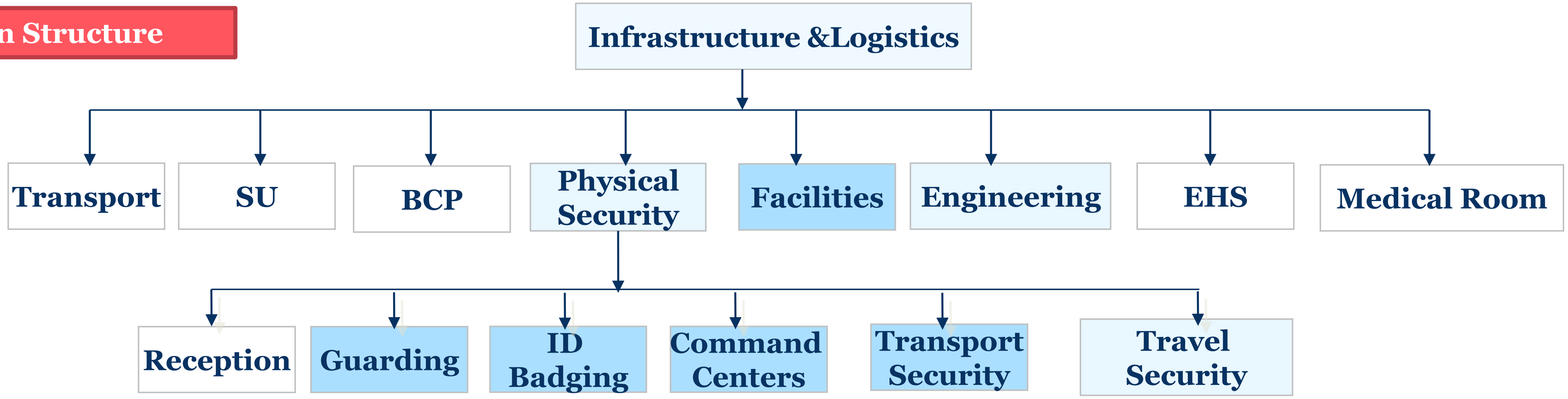
9.6 Document Reviewing

0.0 Introduction

0.1 Organization Structure
0.2 Access Level
0.3 Operational Definition

0.1 Organization Structure & 0.2 Access Levels

Organization Structure



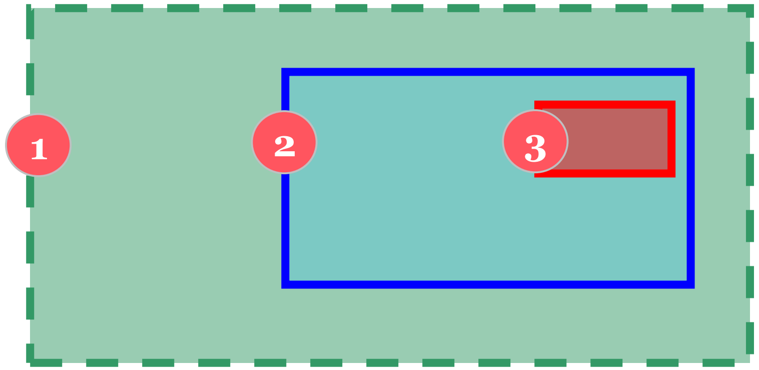
All places where responsibility is mentioned as Logistics, it is for Logistics (Facilities)

Access Levels

Level 1: Premise Level Access/ Periphery

Level 2: Building Level Access

Level 3: Floor Level Access*



*GENPACT Floor in a multi-tenant facility, Red Zones or Carve Out/ODC

Classification: Genpact Internal

0.3 Operational Definitions

	Category	Definition
1	Owner Sole Occupier Facility (Building Type A)	Only Genpact offices in owned premises
2	Sole Tenant Facility (Building Type B)	Only Genpact offices on leased premises
3	Multi Tenant Facility (Building Type C)	Shared facility with other company offices- centralized Security and Maintenance Control

	Category	Definition	Type of Identification Issued
1	Employees	Person on GENPACT Active rolls	Authorized with GENPACT issued permanent photo ID Card on active status/ or temp ID card from VMS incase of forgot ID cases
2	Outstation Employees	Person on GENPACT active rolls but with no access rights to site being visited	Existing home site access card activated if system is compatible else provide access card with general access for the duration of travel
3	Visitors	Person expected by Employee for official purposes	VMS issued ID card
4	New Joinees	Person on GENPACT Active rolls, without permanent photo ID Cards	VMS issued ID card
5	Interview Candidates	Person expected by Employee for Interview purposes	VMS issued ID card
6	Walk-In Interviews	Person come in for Interview with reference of an existing employee	VMS issued ID card
7	Vendors	Person with whom GENPACT has signed contracts to allow occasional working on premises	Authorized with GENPACT issued photo ID Card or VMS issued ID card
8	Resident Vendors	Person with whom GENPACT has signed contracts to allow routine working on premises in the provision of logistics support	Authorized with Parent Company Card & VIF issued ID card or VMS issued ID card
9	Contractor	Person with whom GENPACT has signed contracts to allow routine working on business processes within GENPACT	Authorized with GENPACT issued photo ID Card: “Contractor“ showing parent company name
10	Clients	Representatives of companies with business relationship with GENPACT	Authorized with GENPACT issued photo ID Card or VMS issued ID card
11	Project / Long Stay Customers	Official Visitors who needs unescorted access to the facility for a continued duration.	Authorized with GENPACT issued photo ID Card or VMS issued ID card

	Category	Definition
1	Vendor Information Form	Details of Resident Vendors staff: Vendor company name, employee residential details, company stamp etc.

Genpact India Sites

NCR
- Gurugram - Phase 5
- Gurugram – Plot 22
- Gurugram - North Campus
- Gurugram-Tikri
- Gurugram - Tril
- Noida SEZ
- Noida- Capital Markets
- Noida – Stellar
- Noida - Assotech

Jaipur
- Sitapura
- JLN

Kolkata
- Unitech Infospace

Hyderabad
- Uppal
- DLF – Gachibowli SEZ
- RITP- Pocharam SEZ
- Phoenix
- Hafeezpet

Bangalore
- Suryapark
- SMS
- Pritech Park

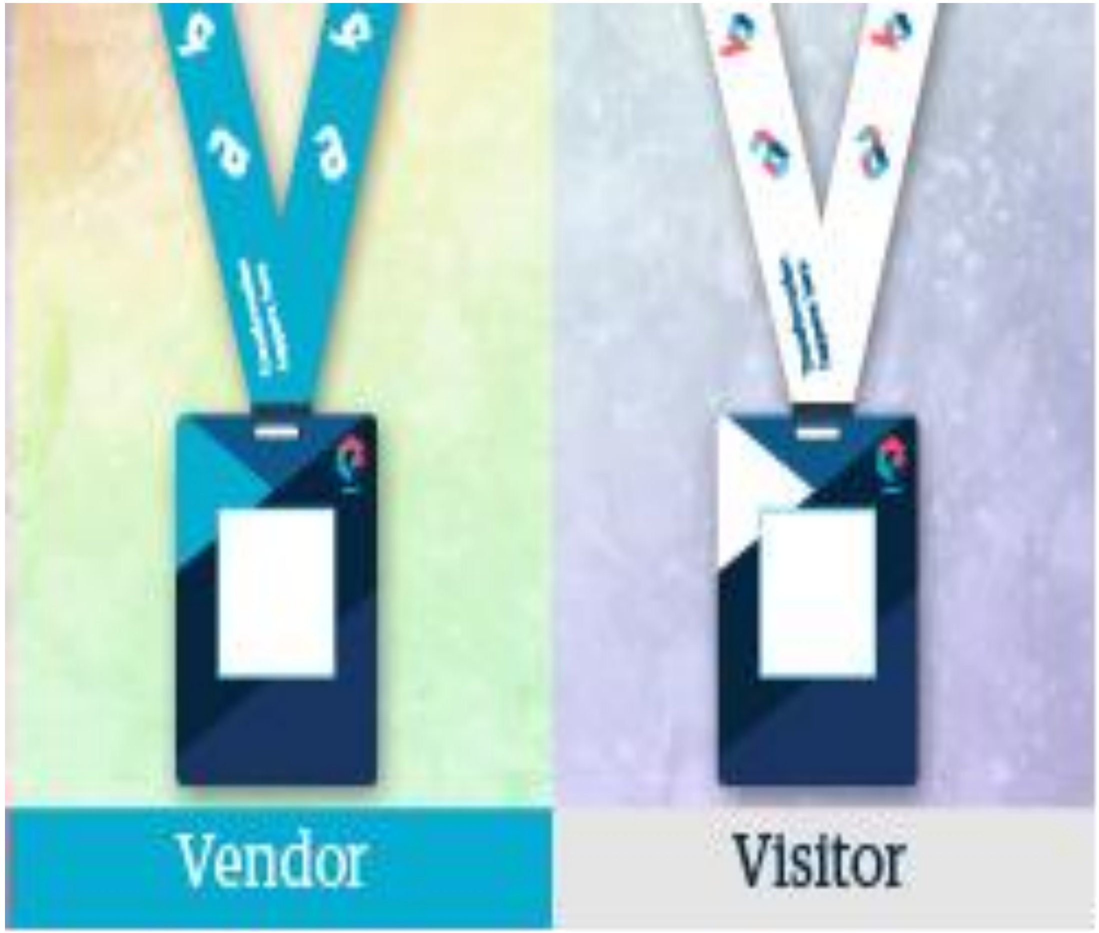
Mumbai
- Axis
- Pharmalink

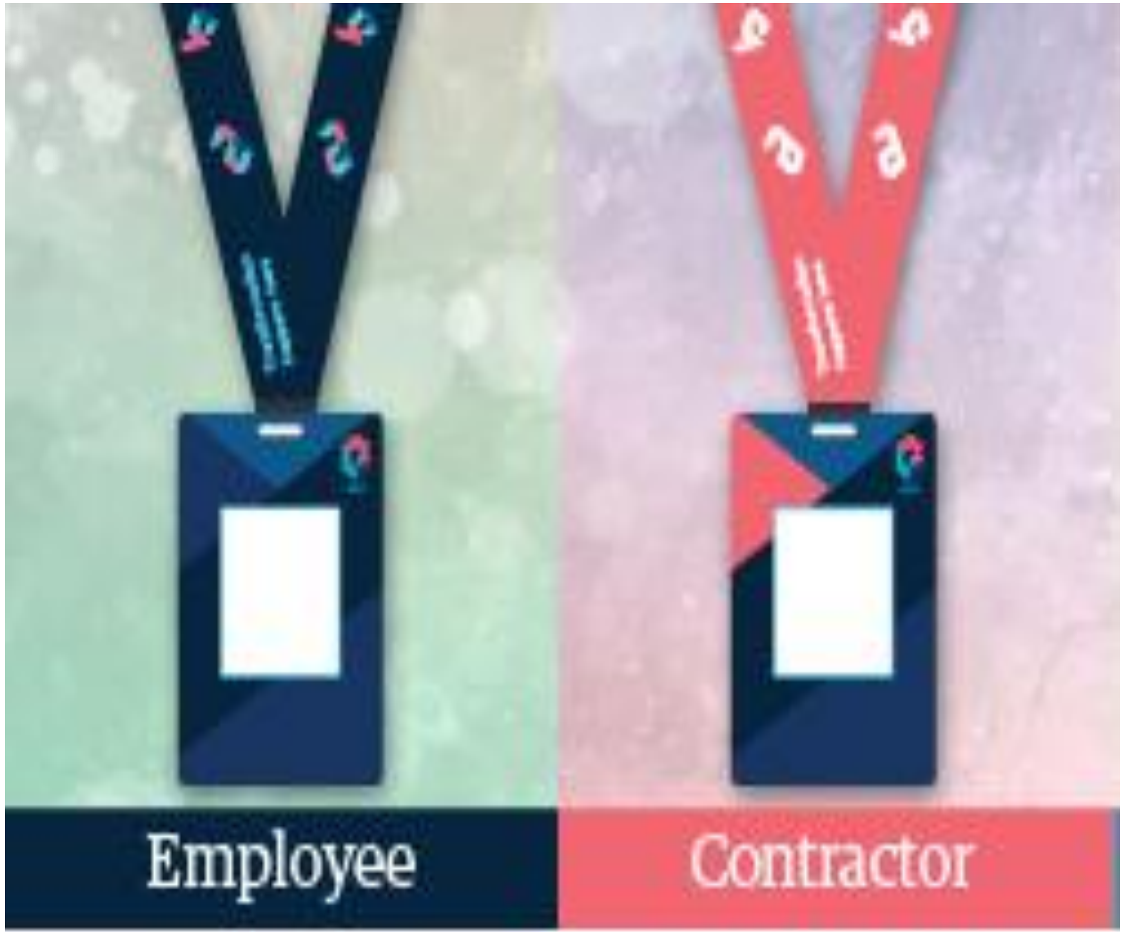
Pune
- Rage

Chennai
- Cambridge Tower

Classification: Genpact Internal

Genpact New Lanyards

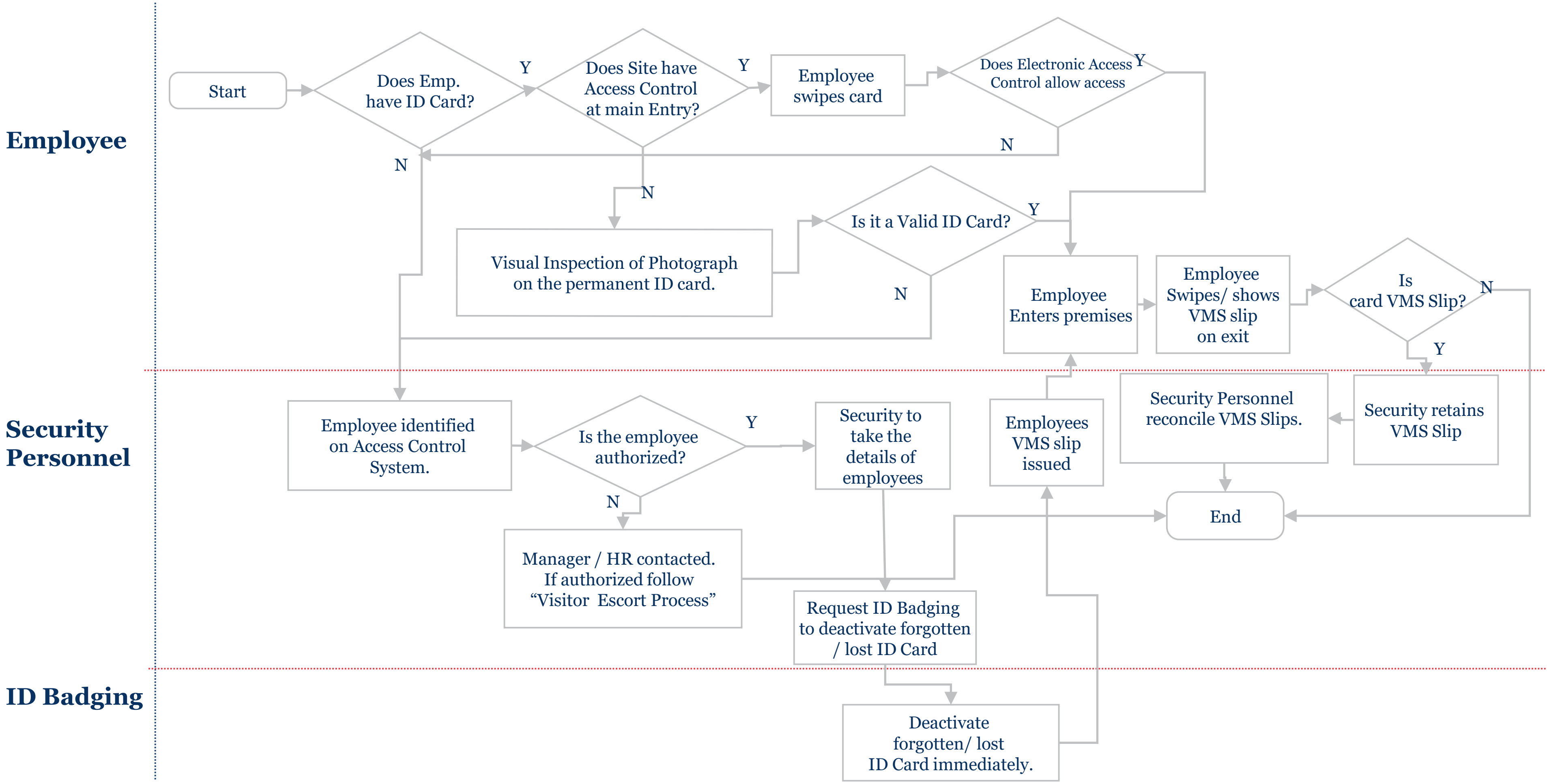




1.0 People Access

1.1 Employee Access/Forgot ID employee access
1.1.1 Outstation Employee
1.2 Visitor /Vendor/HR Interview Access
1.2.1 Project/ Long Staying Customers
1.3 Resident Vendor Access
1.4 Driver Access

1.1 Employee Access/Forgot ID Employee Access



Employee

Start

Does Emp. have ID Card?

Y

N

Does Site have Access Control at main Entry?

Y

N

Employee swipes card

Does Electronic Access Control allow access

Y

N

Visual Inspection of Photograph on the permanent ID card.

Is it a Valid ID Card?

Y

N

Employee Enters premises

Employee Swipes/ shows VMS slip on exit

Is card VMS Slip?

N

Y

Security Personnel

Employee identified on Access Control System.

Is the employee authorized?

Y

N

Security to take the details of employees

Employees VMS slip issued

Security Personnel reconcile VMS Slips.

Security retains VMS Slip

End

Manager / HR contacted. If authorized follow "Visitor Escort Process"

Request ID Badging to deactivate forgotten / lost ID Card

ID Badging

Deactivate forgotten/ lost ID Card immediately.

Definition

(1) Main Entry- Can be Perimeter level for owned sites or Building/Floor level for Leased sites.

Escalation

- Trigger: Employee appears as Resigned/ Absconding /non active on Access System.
- Employee is using someone else's ID Card.
- Person requesting entry/access – picture does not match/exist on system.
- Action: Security Guard to inform Security Supervisor/logistics.
- For employees Dark Blue card & lanyard is issued.

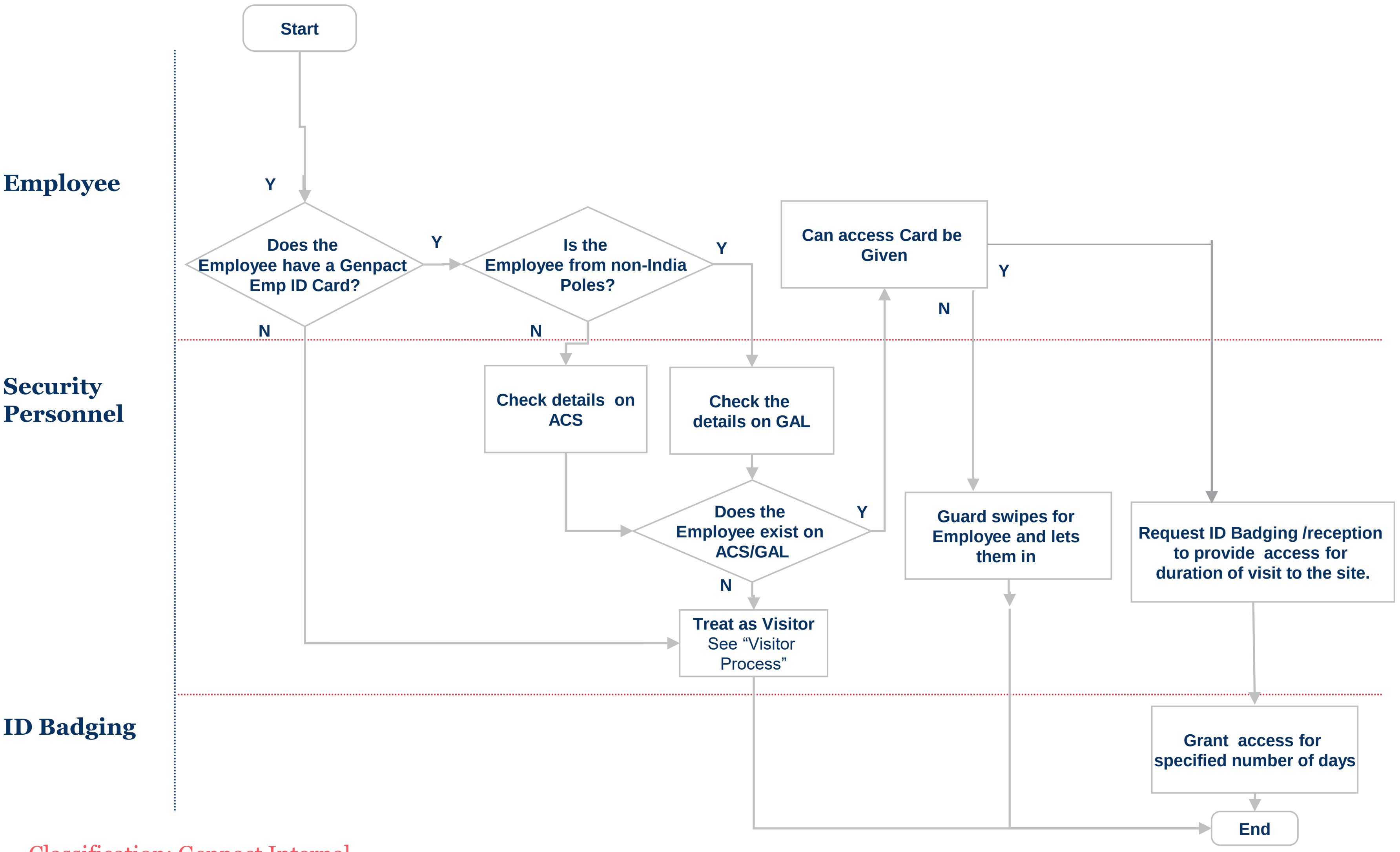
Metric

- # of Temp Cards Issued vs # Temp Cards Received
- See Site Exceptions on next slide
- Tailgating is strictly prohibited and if noticed, it has to be communicated to the employees manager/HR

Classification: Genpact Internal

genpact

1.1.1 Outstation Employee Access



Employee
Security Personnel
ID Badging
Start
Y
Does the Employee have a Genpact Emp ID Card?
Y
N
Is the Employee from non-India Poles?
Y
N
Can access Card be Given
Y
N
Check details on ACS
Check the details on GAL
Does the Employee exist on ACS/GAL
Y
N
Guard swipes for Employee and lets them in
Request ID Badging /reception to provide access for duration of visit to the site.
Treat as Visitor See "Visitor Process"
Grant access for specified number of days
End

Definition

(1)Main Entry- Can be Perimeter level for owned sites or Building/Floor level for Leased sites.

Escalation

- Trigger: Employee appears as Resigned/ Absconding /non active on Access System.
- Employee is using someone else's ID Card.
- Person requesting entry/access – picture does not match/exist on system.
- Action: Security Guard to inform Security Supervisor/logistics.
- For employees Dark Blue card & lanyard is issued.

Metric

- HR/ Host/Manager to share confirmation email for non pole employees

Classification: Genpact Internal

Exceptions for Employee Access and Outstation Employee Access

All visitor, vendor, HR interview, One day temp card entry will be made through Visitor Management system across all sites

VMS report is available for a period of 12 months

In case of ODC access level name change, swipe logs will be available with new name

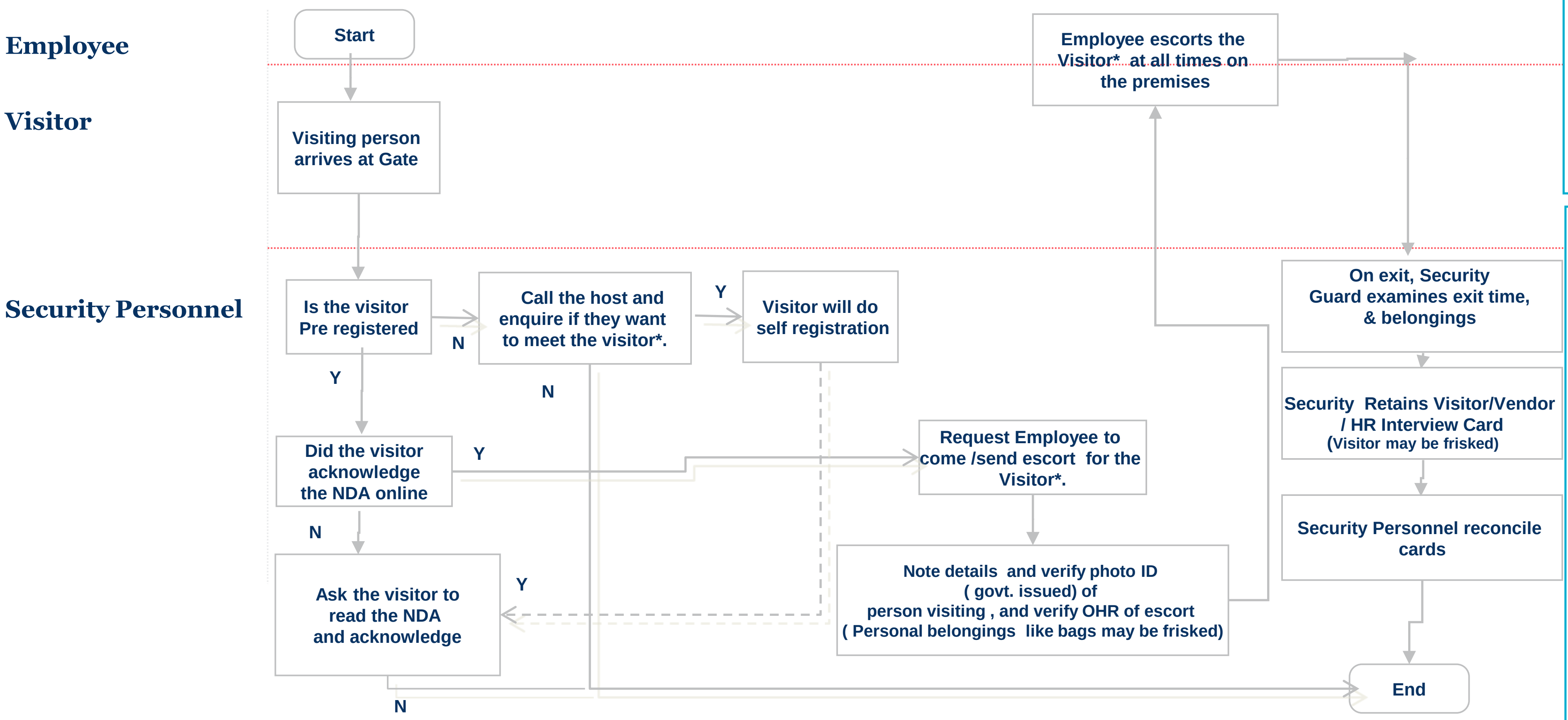
Access swipe records/logs will be retained for a period of 18 months for India locations

No exceptions for Outstation employee access

Classification: Genpact Internal

*Level 1: Premises Level Access   Level 2: Building Level Access   Level 3: Floor/ Process Level Access

1.2 Visitor/Vendor/HR Interview Access



Employee

Visitor

Security Personnel

Start

Visiting person arrives at Gate

Is the visitor Pre registered

N

Call the host and enquire if they want to meet the visitor*.

Y

Visitor will do self registration

Y

N

Did the visitor acknowledge the NDA online

Y

N

Ask the visitor to read the NDA and acknowledge

Y

N

Request Employee to come /send escort for the Visitor*.

Note details and verify photo ID (govt. issued) of person visiting , and verify OHR of escort (Personal belongings like bags may be frisked)

Employee escorts the Visitor* at all times on the premises

On exit, Security Guard examines exit time, & belongings

Security Retains Visitor/Vendor / HR Interview Card (Visitor may be frisked)

Security Personnel reconcile cards

End

Escalation

- Trigger: Person visiting forces entry.
- Person taking access for non-official reason
- Escort does not come to receive the visiting person.
- Suspicious findings during frisking
- Action: Security Guard to inform Security Supervisor/logistics.

Metric

* Visitor – Vendor, HR Interview candidates, Visitors (eg : clients, auditors, family members)

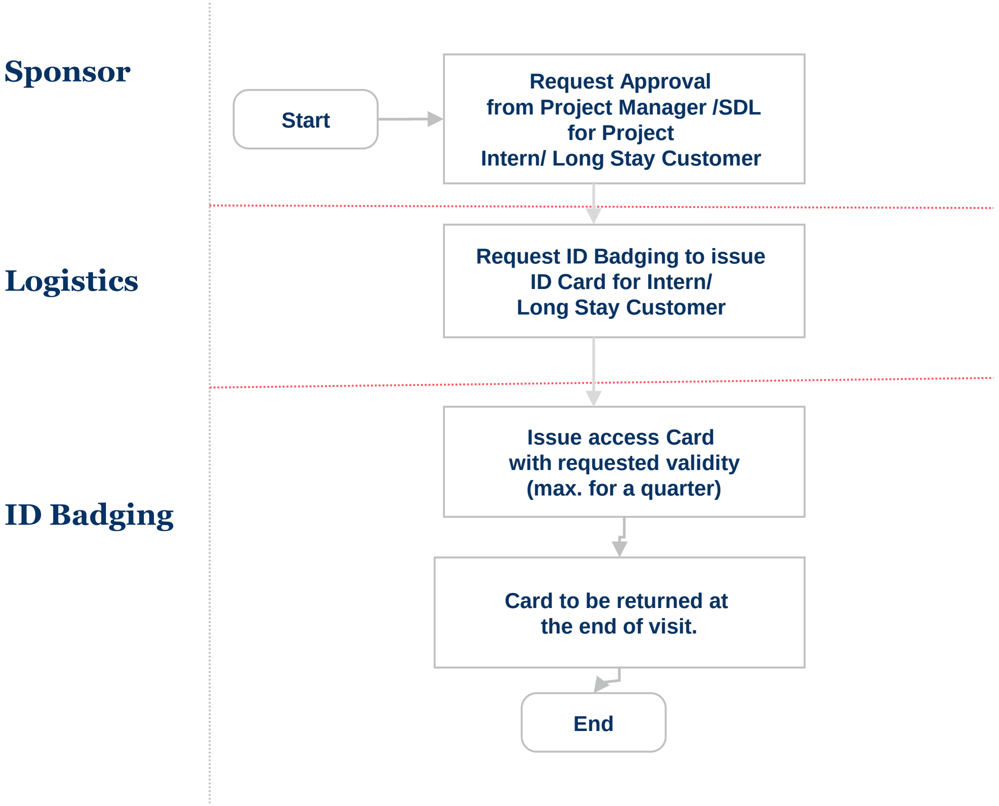
- # of visitor /vendor Cards issued vs # of cards returned
- Noting of belongings on entry, verifying of belongings on exit

Exception(*) See Site Exceptions on end section Exception list

- Government Visitors: (Exempt from card issuance process) would be escorted by Security Personnel/ Logistics to the Reception or to meet the person concerned.
- HR Interviewees: Escorted by HR/Security at all times.

Classification: Genpact Internal

1.2.1 Project/ Long Staying Customers


Sponsor
Logistics
ID Badging
Start
Request Approval from Project Manager /SDL for Project Intern/ Long Stay Customer
Request ID Badging to issue ID Card for Intern/ Long Stay Customer
Issue access Card with requested validity (max. for a quarter)
Card to be returned at the end of visit.
End

*Level 1: Premises Level Access

Level 2: Building Level Access

Level 3: Floor/ Process Level Access

Escalation

- Trigger: No approval received from SDL (service deliver leader - Band 4D and above)
- ID Card not received from Sponsor
- ID Card Lost
- Action: ID Badging to inform Logistics
- SDL- service deliver leader - (Band 4D and above)
- SLM - Site logistics manager.

Metric

- # of Cards printed

Exceptions for Visitor & Project Long Staying Customers

Visitor Access

All Sites

- For existing customers, in case of requirement, access will be provided basis helpmate ticket by Host
- Only the following categories of people will be allowed to escort

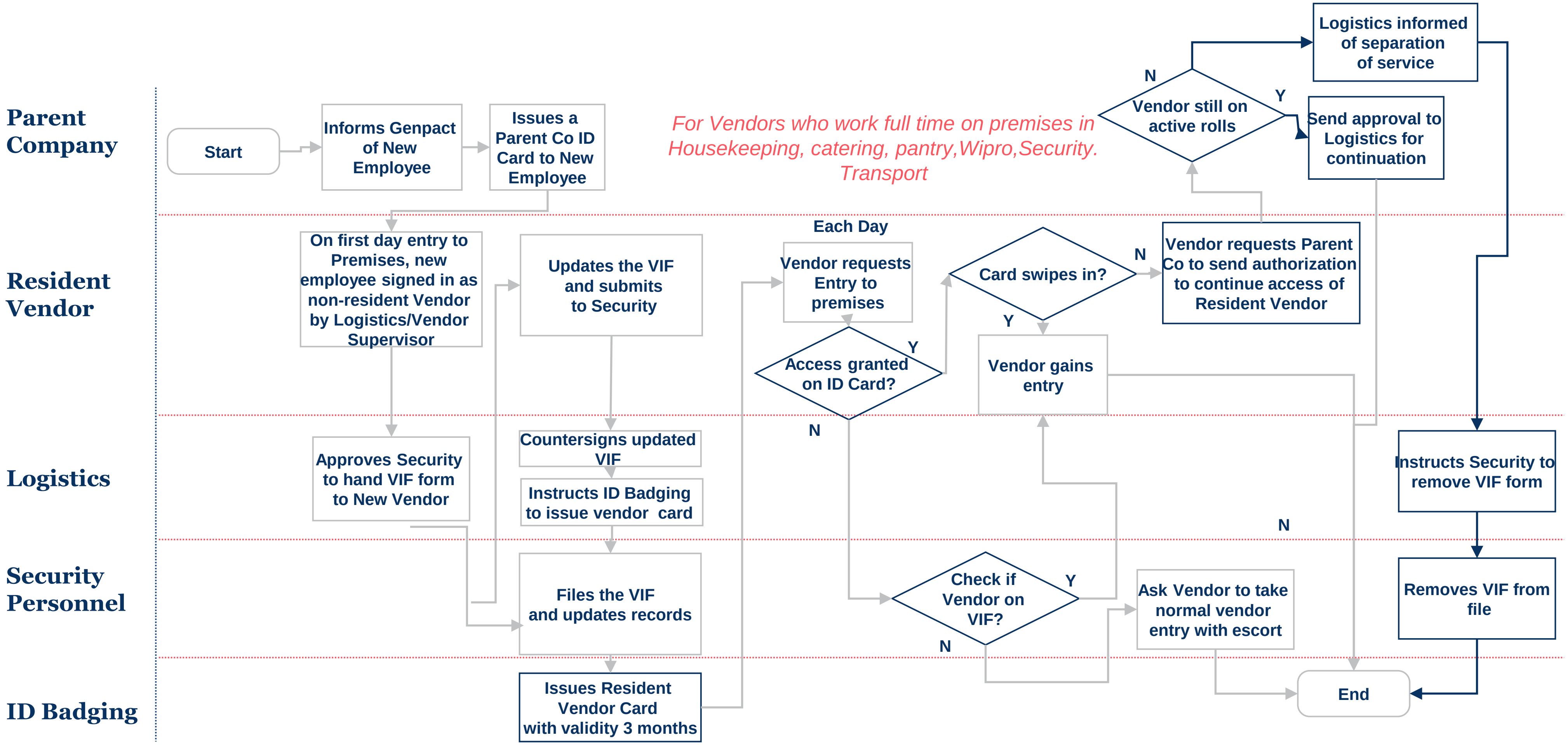
  1. Any Genpact Employee
  2. Any Vendor with authorised access card (Wipro , Parishram , facility services, security etc)
  3. Anyone on list authorized by Logistics

- Visitor – White lanyard and card is issued.
- Vendor – Light Blue lanyard and card is issued.
- HR Interview – White lanyard and card is issued.
- Contractor – Red Lanyard and card is issued.
- Personal Driver- Green

All visitor, vendor, HR interview, entry will be made through Visitor Management system.

Classification: Genpact Internal

1.3 Resident Vendor / Contractor Access



For Vendors who work full time on premises in Housekeeping, catering, pantry,Wipro,Security. Transport

Parent Company

Start

Informs Genpact of New Employee

Issues a Parent Co ID Card to New Employee

Vendor still on active rolls

N

Logistics informed of separation of service

Y

Send approval to Logistics for continuation

Resident Vendor

On first day entry to Premises, new employee signed in as non-resident Vendor by Logistics/Vendor Supervisor

Updates the VIF and submits to Security

Each Day

Vendor requests Entry to premises

Access granted on ID Card?

Y

N

Card swipes in?

N

Y

Vendor requests Parent Co to send authorization to continue access of Resident Vendor

Vendor gains entry

Logistics

Approves Security to hand VIF form to New Vendor

Countersigns updated VIF

Instructs ID Badging to issue vendor card

Instructs Security to remove VIF form

N

Security Personnel

Files the VIF and updates records

Check if Vendor on VIF?

Y

N

Ask Vendor to take normal vendor entry with escort

Removes VIF from file

ID Badging

Issues Resident Vendor Card with validity 3 months

End

Escalation

- Trigger: Vendor Supervisor not available to sign-in New Vendor
- Incomplete/ Incorrect VIF updated
- Vendor ID Card expired
- Vendor not on VIF, but claims submitted VIF
- No response from Parent Co on Vendor access status
- Action: Security Guard to inform Security Supervisor
- Security Supervisor to inform Logistics
- Logistics to inform Site Logistics Leader

Metric

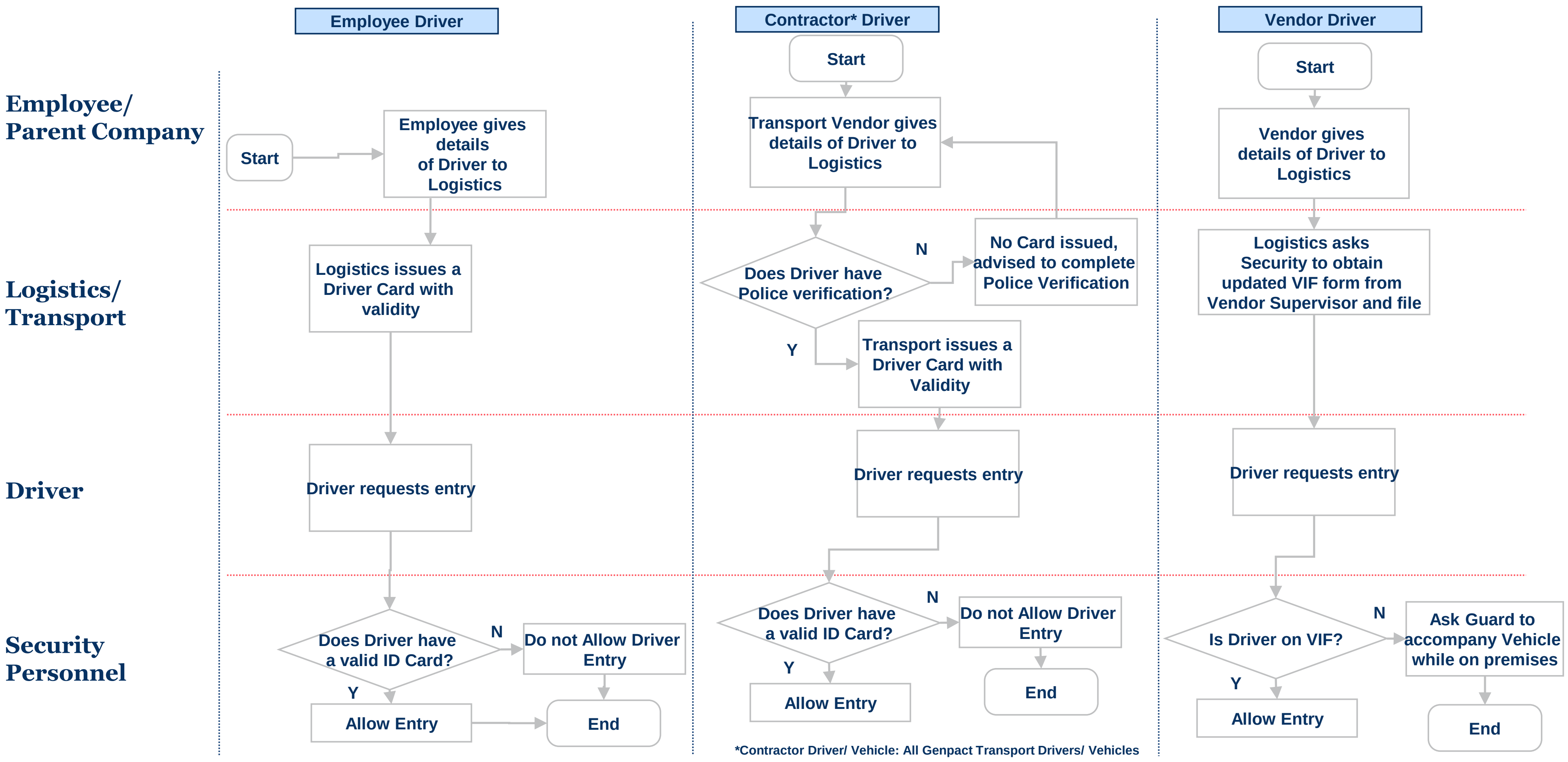
- # of VIF submitted vs # of New ID Cards created

PVC/BGC is mandatory for all vendor staff card creation and access

- # of Vendors on VIF vs # of Vendors Cards deactivated on a monthly basis
- (*) See Site Exceptions on next slide

Classification: Genpact Internal

1.4 Driver Access



Employee/ Parent Company

Logistics/ Transport

Driver

Security Personnel

Employee Driver

Start

Employee gives details of Driver to Logistics

Logistics issues a Driver Card with validity

Driver requests entry

Does Driver have a valid ID Card?

N: Do not Allow Driver Entry

End

Y: Allow Entry

End

Contractor* Driver

Start

Transport Vendor gives details of Driver to Logistics

Does Driver have Police verification?

N: No Card issued, advised to complete Police Verification

Y: Transport issues a Driver Card with Validity

Driver requests entry

Does Driver have a valid ID Card?

N: Do not Allow Driver Entry

End

Y: Allow Entry

*Contractor Driver/ Vehicle: All Genpact Transport Drivers/ Vehicles

Vendor Driver

Start

Vendor gives details of Driver to Logistics

Logistics asks Security to obtain updated VIF form from Vendor Supervisor and file

Driver requests entry

Is Driver on VIF?

N: Ask Guard to accompany Vehicle while on premises

End

Y: Allow Entry

Escalation

- Trigger: Driver does not have ID Card
- Driver has an invalid ID card
- Action: Security Guard to inform Security Supervisor
- Security Supervisor to inform Logistics
- (Logistics to inform Transport Supervisor)
- (Logistics to inform Transport Manager)
- Logistics to inform Site Logistics Leader

Metric

- # of Drivers taking entry without ID Cards
- All driver to be issued ID post PVC submission

Personal Drivers are to be issued Green Lanyard

Exception

- For all Special Visits, Luxury vehicles are arranged for, with no vendor sticker. Security only verifies the name of Visitor.

(*) See Site Exceptions on end section Exception list

Driver will not be allowed entry if forgot ID and no temporary card to be issued

Classification: Genpact Internal

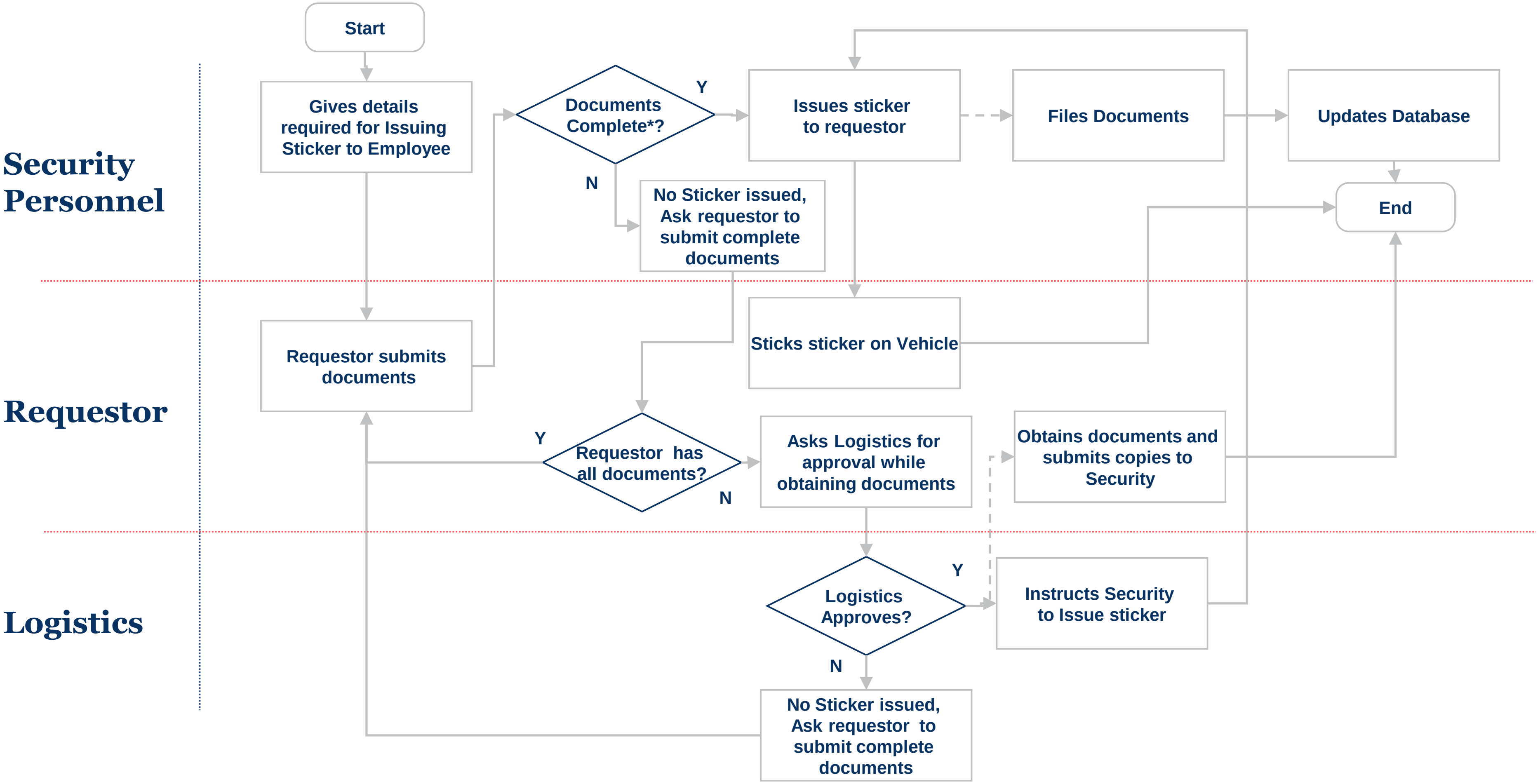
No Exceptions for Vendor , Resident Vendor and Driver Access

Classification: Genpact Internal

2.0 Vehicle Access

2.1 Issuing of Vehicle Stickers
2.2 Employee Vehicle Access
2.3 Vendor Vehicle Access
2.4 Contracted Vehicle Access

2.1 Issuing of Vehicle Stickers


Security Personnel
Requestor
Logistics
Start
Gives details required for Issuing Sticker to Employee
Documents Complete*?
Y
N
Issues sticker to requestor
Files Documents
Updates Database
End
No Sticker issued, Ask requestor to submit complete documents
Sticks sticker on Vehicle
Requestor submits documents
Requestor has all documents?
Y
N
Asks Logistics for approval while obtaining documents
Obtains documents and submits copies to Security
Logistics Approves?
Y
N
Instructs Security to Issue sticker
No Sticker issued, Ask requestor to submit complete documents

Escalation

- Trigger: All documents of requestor vehicles are not received
- Action: Security Guard to inform Security Supervisor / logistics

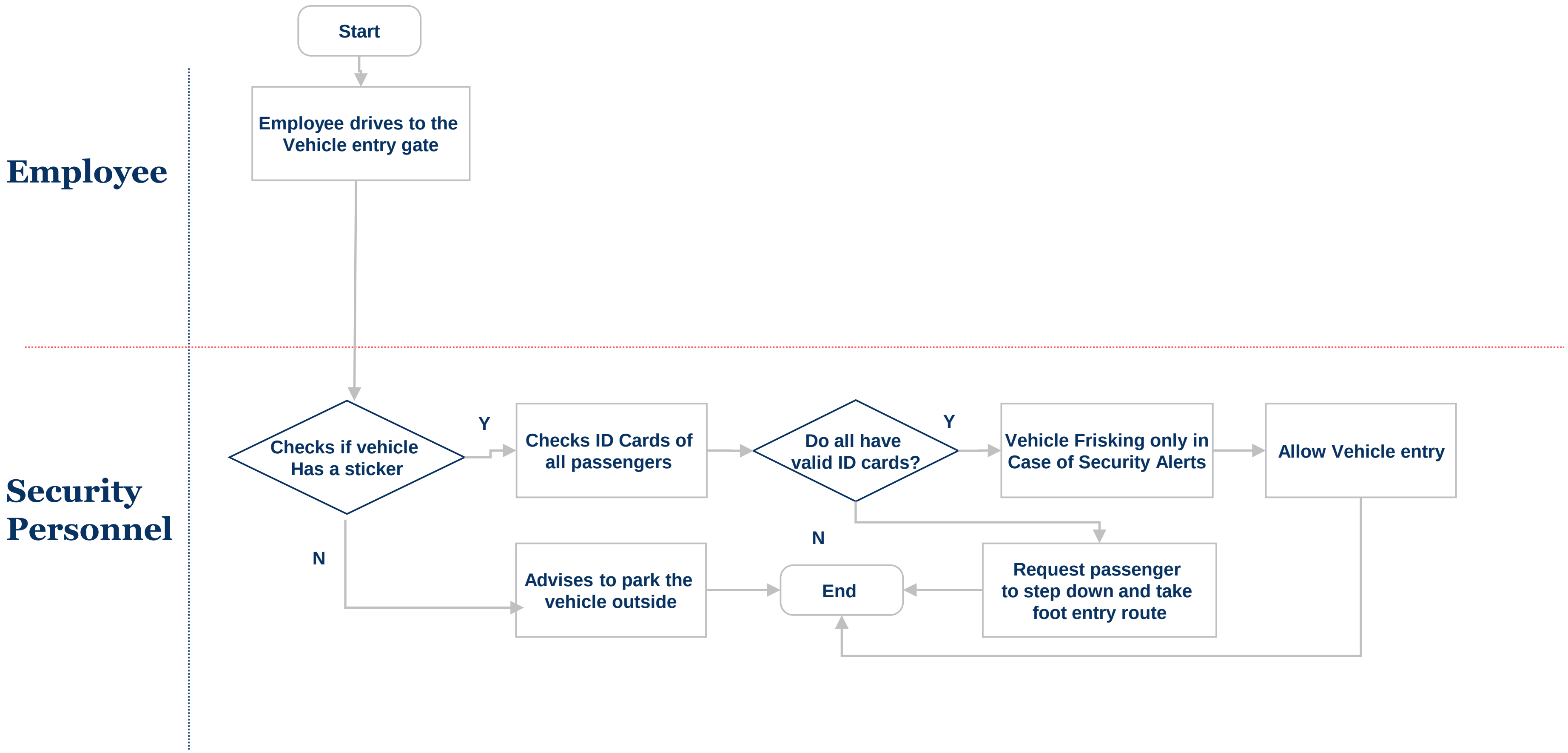
Metric

- # of new Vehicle Stickers Issued

- Mandatory Documents:
- i. Copy of Genpact ID card
- ii. Copy of Driving License Copy
- iii. Copy of Registration/ Challan/ Insurance (anything to give proof of vehicle registration)
- iv. NOC if vehicle not in Employee's name along with Govt ID proof of the individual

Classification: Genpact Internal

2.2 Employee Vehicle Access


Employee
Security Personnel
Start
Employee drives to the Vehicle entry gate
Checks if vehicle Has a sticker
Y
N
Checks ID Cards of all passengers
Do all have valid ID cards?
Y
N
Vehicle Frisking only in Case of Security Alerts
Allow Vehicle entry
Advises to park the vehicle outside
End
Request passenger to step down and take foot entry route

Escalation

- Trigger: Frisking of vehicles shows a suspicious object
- Car Accident on premises
- Action: Security Guard to inform Security Supervisor
- Security Supervisor to inform Logistics
- Logistics to inform Site Logistics Leader
- Vehicles should be personal and not commercial

Metric

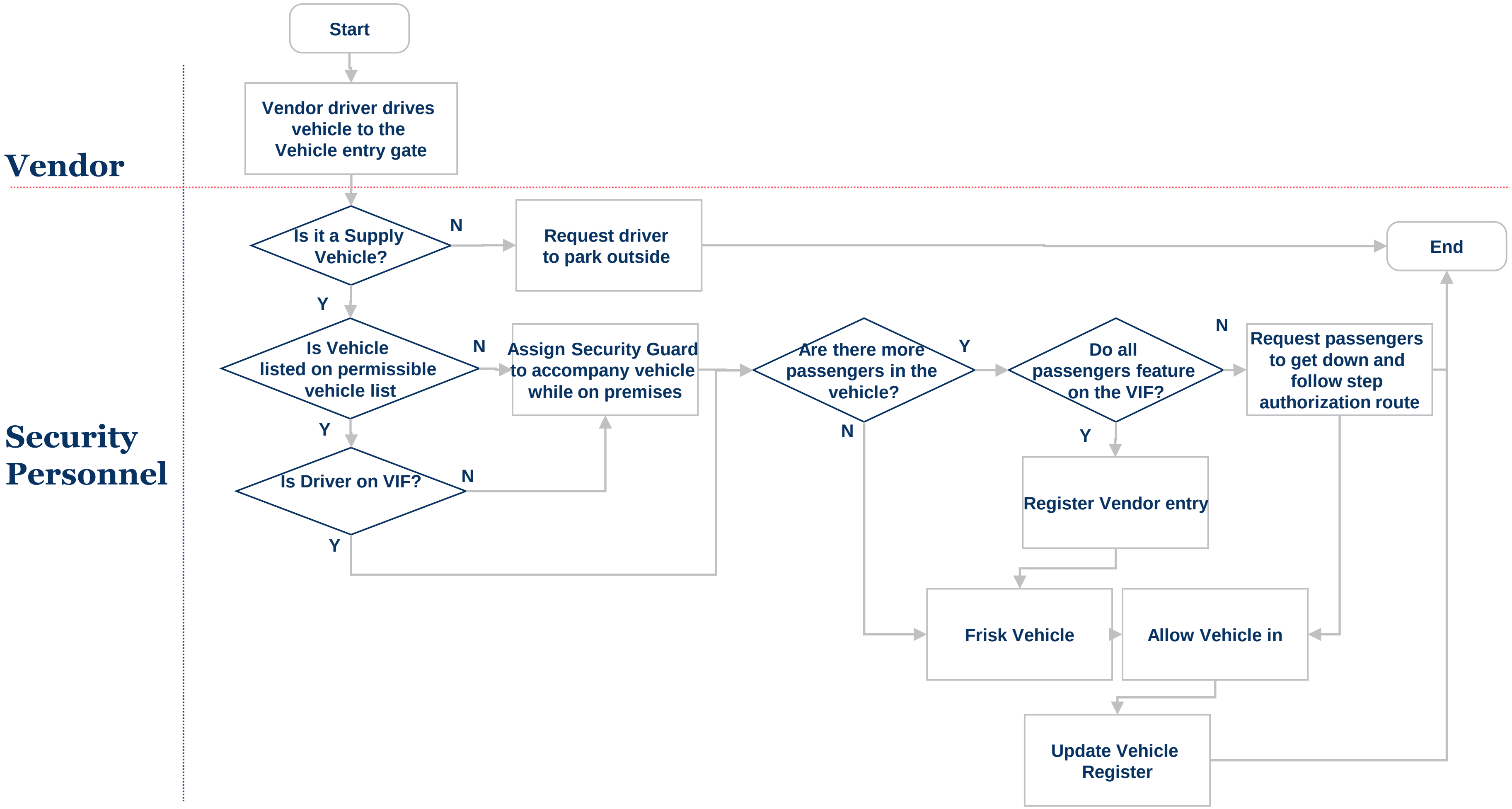
- # of Cars in vs. # of Cars out in 24 hrs
- # of vehicles frisked at the gate

Exception

- (*) See Site Exceptions on end section Exception list

Classification: Genpact Internal

2.3Vendor Vehicle Access


Vendor
Security Personnel
Start
Vendor driver drives vehicle to the Vehicle entry gate
Is it a Supply Vehicle?
N
Request driver to park outside
End
Y
Is Vehicle listed on permissible vehicle list
N
Assign Security Guard to accompany vehicle while on premises
Are there more passengers in the vehicle?
Y
Do all passengers feature on the VIF?
N
Request passengers to get down and follow step authorization route
Y
Is Driver on VIF?
N
N
Y
Register Vendor entry
Y
Frisk Vehicle
Allow Vehicle in
Update Vehicle Register

Escalation

- Trigger: Frisking of vehicles shows a suspicious object
- No Guard available to escort vehicle
- Passengers refuse to get off vehicle
- Action: Security Guard to inform Security Supervisor
- Security Supervisor to inform Logistics
- Logistics to inform Site Logistics Leader

Metric

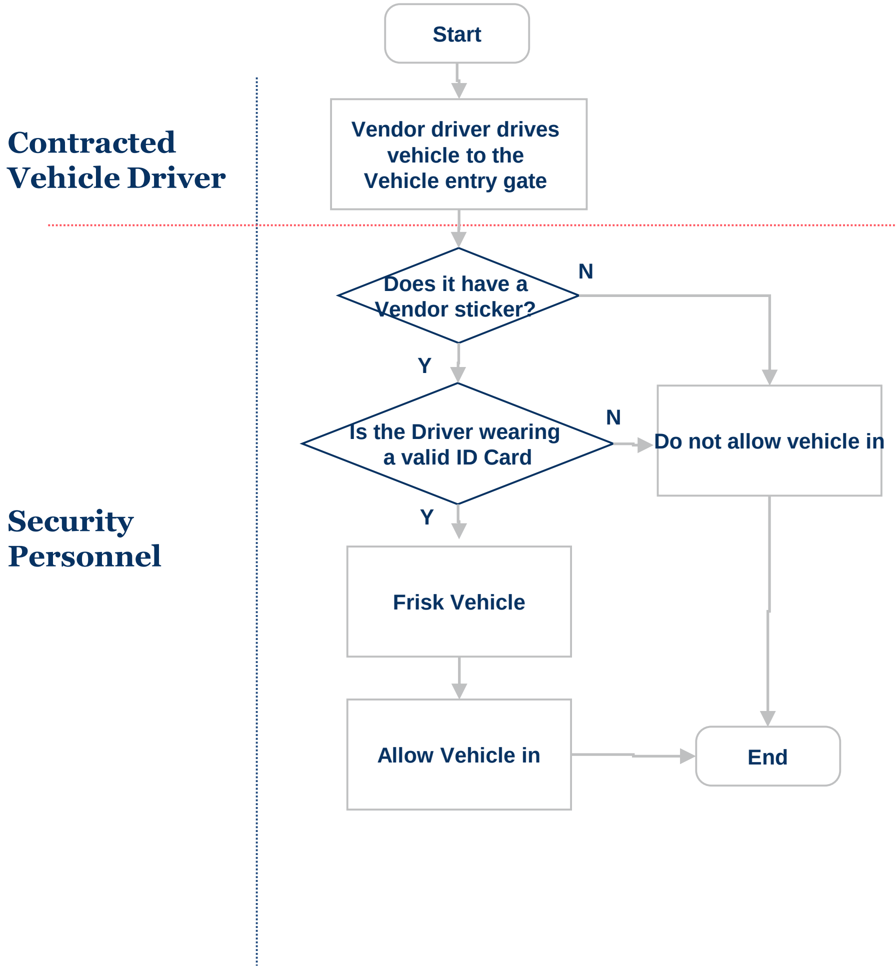
- # of Vendor Cards issued vs # of Vendor Cards returned

Exception

- (*) See Site Exceptions on end section Exception list

Classification: Genpact Internal

2.4 Contracted Vehicle Access


Start
Contracted Vehicle Driver
Vendor driver drives vehicle to the Vehicle entry gate
Security Personnel
Does it have a Vendor sticker?
N
Y
Is the Driver wearing a valid ID Card
N
Y
Do not allow vehicle in
Frisk Vehicle
Allow Vehicle in
End

*Contractor Driver/ Vehicle: All Genpact Transport Drivers/ Vehicles

Escalation

- Trigger: No Vendor Sticker on vehicle
- Frisking of vehicles shows a suspicious object
- Driver not wearing an ID Card
- Action: Security Guard to inform Security Supervisor
- Security Supervisor to inform Logistics
- Logistics to inform Site Logistics Leader

Metric

- # of Vendor Cards issued vs # of Vendor Cards returned

Exception

- Entry for Luxury Vehicles with Senior Customers
- (*) See Site Exceptions on end section Exception list

Classification: Genpact Internal

No Exceptions for Employee Vehicle Access

*Level 1: Premises Level Access

Level 2: Building Level Access

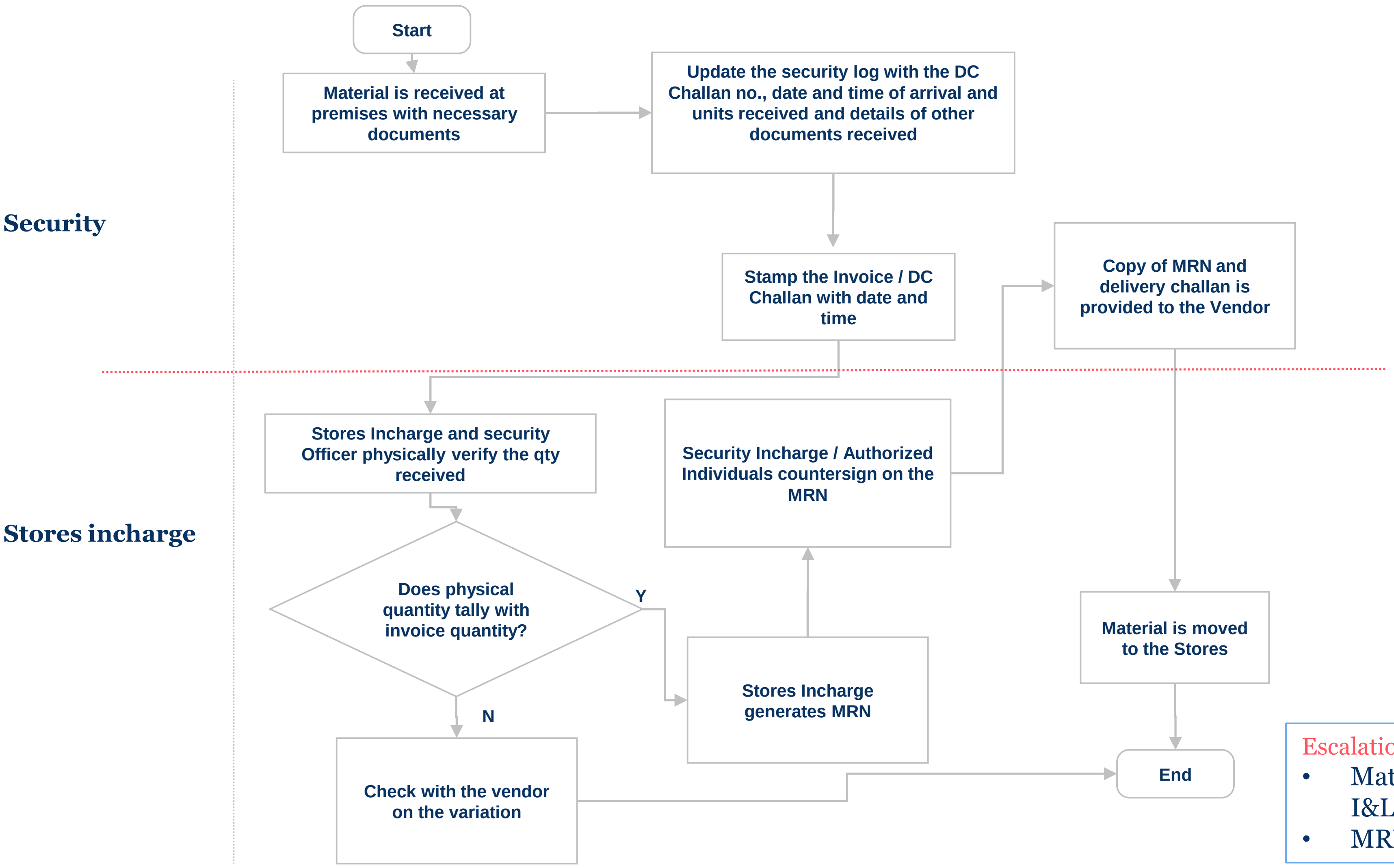
Level 3: Floor/ Process Level Access

Classification: Genpact Internal

3.0 Material In/ Out

3.1 Material In
3.2 Material Out
3.3 Mail Handling

3.1 Material In

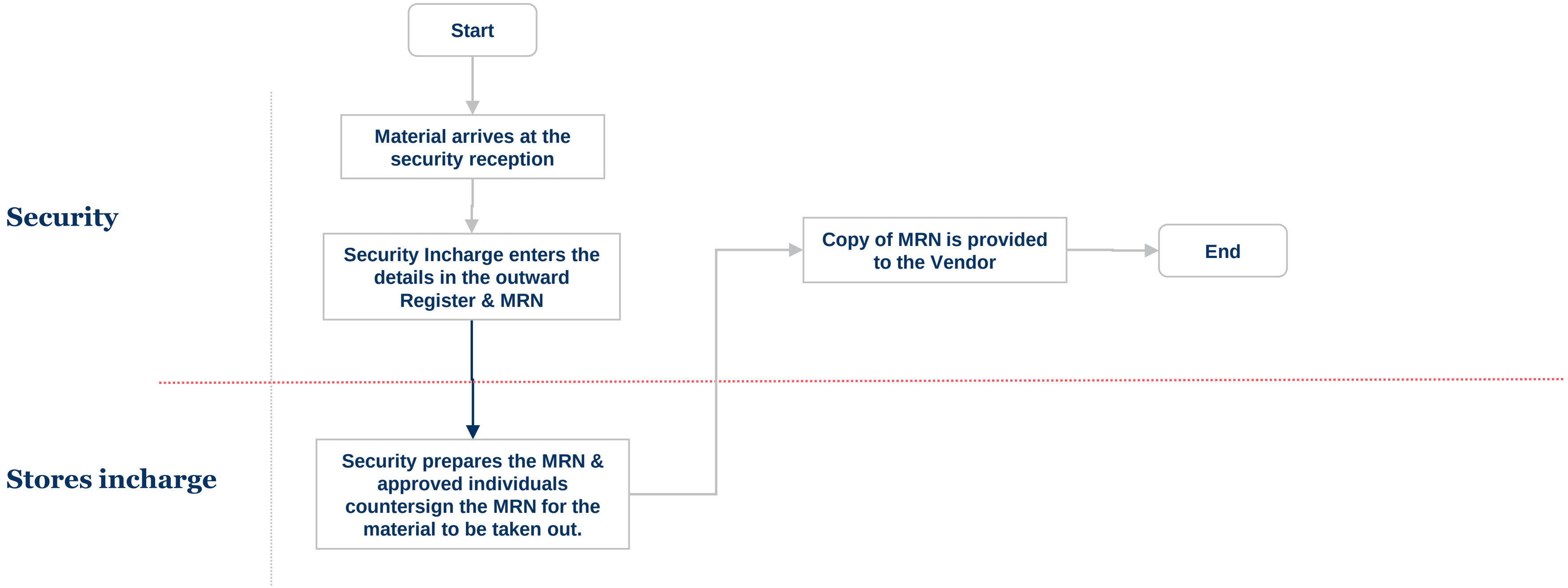

Security
Stores incharge
Start
Material is received at premises with necessary documents
Update the security log with the DC Challan no., date and time of arrival and units received and details of other documents received
Stamp the Invoice / DC Challan with date and time
Copy of MRN and delivery challan is provided to the Vendor
Stores Incharge and security Officer physically verify the qty received
Does physical quantity tally with invoice quantity?
Y
N
Security Incharge / Authorized Individuals countersign on the MRN
Stores Incharge generates MRN
Material is moved to the Stores
Check with the vendor on the variation
End

Escalation :

- Material coming without authorization from I&L
- MRN not signed by I&L

Classification: Genpact Internal

3.2 Material Out

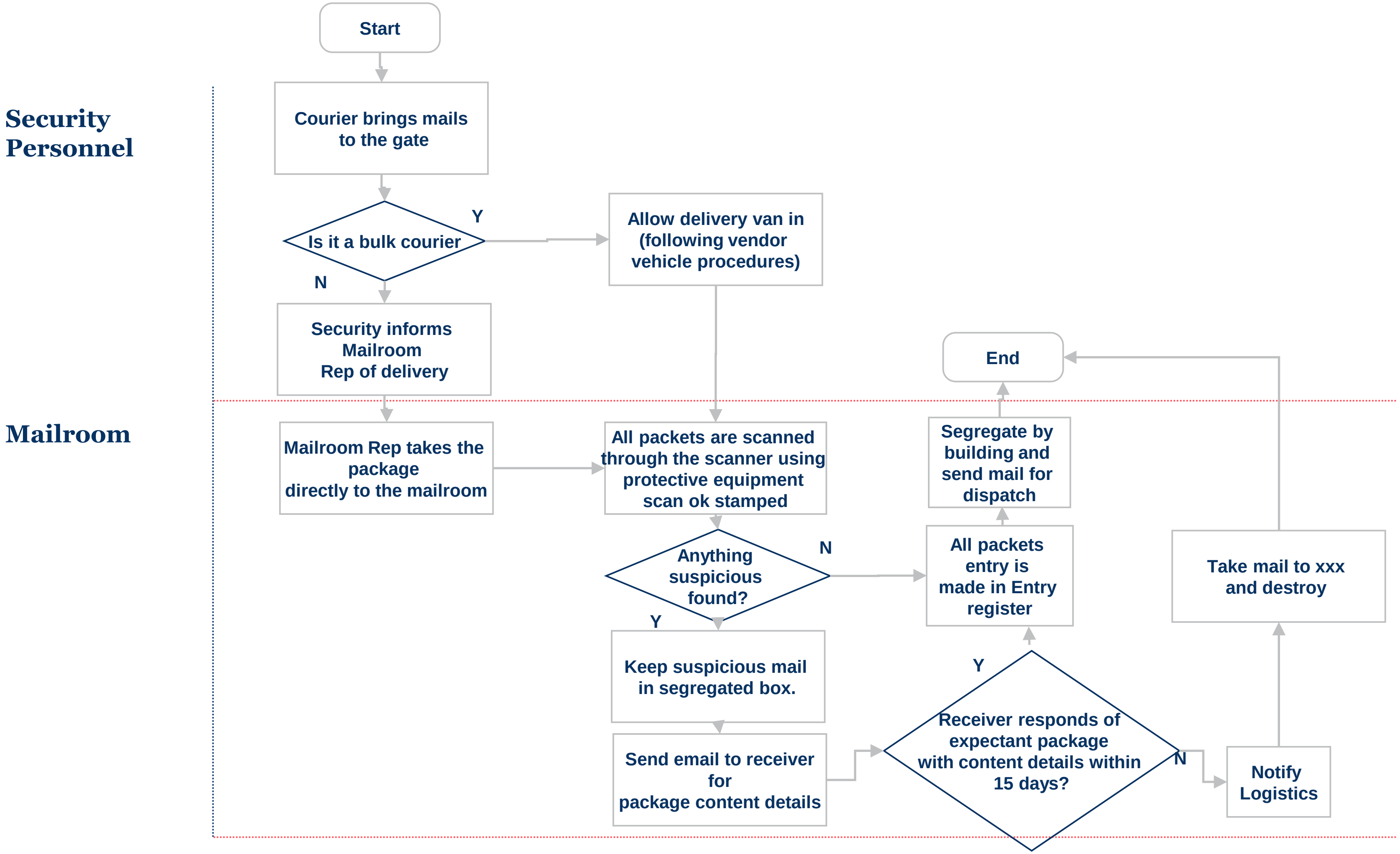

Start
Material arrives at the security reception
Security Incharge enters the details in the outward Register & MRN
Copy of MRN is provided to the Vendor
End
Security
Stores incharge
Security prepares the MRN & approved individuals countersign the MRN for the material to be taken out.

Escalation :

- Material going without authorization from I&L.
- MRN not signed by I&L

Classification: Genpact Internal

3.3 Mail Handling



Start
Security Personnel
Courier brings mails to the gate
Is it a bulk courier
Y
Allow delivery van in (following vendor vehicle procedures)
N
Security informs Mailroom Rep of delivery
Mailroom
Mailroom Rep takes the package directly to the mailroom
All packets are scanned through the scanner using protective equipment scan ok stamped
Anything suspicious found?
N
All packets entry is made in Entry register
Segregate by building and send mail for dispatch
End
Y
Keep suspicious mail in segregated box.
Send email to receiver for package content details
Receiver responds of expectant package with content details within 15 days?
Y
N
Notify Logistics
Take mail to xxx and destroy

Escalation

- Trigger: Suspicious mail received and no response from Receiver
- No details of Receiver on Mail
- Action: Mailroom Employee to inform Supervisor
- Mailroom Supervisor to inform Logistics
- Logistics to inform Site Logistics Leader

Metric

- # of suspicious mails received in a day
- # of suspicious mails destroyed in a day

Exception

- (*) See Site Exceptions on next slide

Classification: Genpact Internal

Exceptions for Material In, Material Out and Mail Handling

Material In

All Sites

- Logistics signs on the MRN for all movement of goods. In addition IT also signs for all IT related material.

Imported Materials (SEZ):

- Bill of Entry for imported/B2B (bond to bond)ARE-1 form for indigenous goods.
- Invoice & Packing list.
- Airway bill or consignment note.
- Way bill for Kolkata (exception).
- Road Challan

Non Imported Materials (SEZ):

- Invoice
- Road Challan
- Way Bill for Kolkata (exception)

Material Out- SEZ's

Customs officer permission is required (which has TAT for 03 working days) before taking any goods out of SEZ unit. For obtaining this permission following documents needs to be provided to respective customs team – 1) Original Copy of Inward challan / Invoice etc. having stamp of Developer. 2) Vendor's request letter.

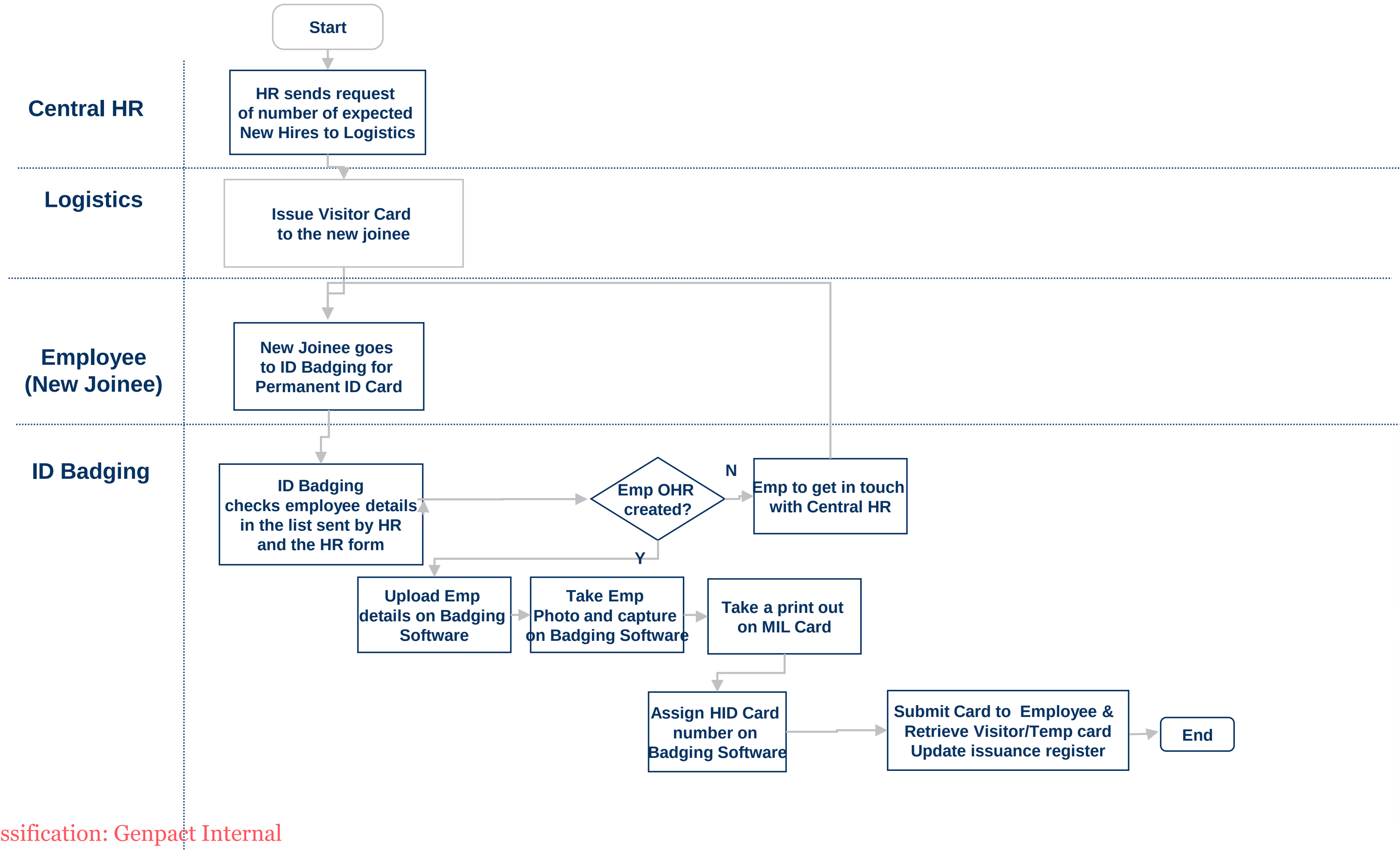
Goods belonging to process/functions – The Process owner / representative will sign on the MRN.

No Exceptions for Mail Handling

4.0 ID Badging

4.1 New ID Cards Issuance
4.2 Lost ID Card & Damaged ID card
4.3 Card Deactivation
4.4 Monthly Access Reconciliation Process
4.5 Access Grant Process
4.6 Access Card Inventory

4.1 New ID Card Issuance



Start
Central HR
HR sends request of number of expected New Hires to Logistics
Logistics
Issue Visitor Card to the new joinee
Employee (New Joinee)
New Joinee goes to ID Badging for Permanent ID Card
ID Badging
ID Badging checks employee details in the list sent by HR and the HR form
Emp OHR created?
N
Emp to get in touch with Central HR
Y
Upload Emp details on Badging Software
Take Emp Photo and capture on Badging Software
Take a print out on MIL Card
Assign HID Card number on Badging Software
Submit Card to Employee & Retrieve Visitor/Temp card Update issuance register
End

Escalation

- Trigger: Software issues or Site down
- Action: ID Badging Employee to inform Logistics
- Logistics inform Site Logistics Leader

Metric

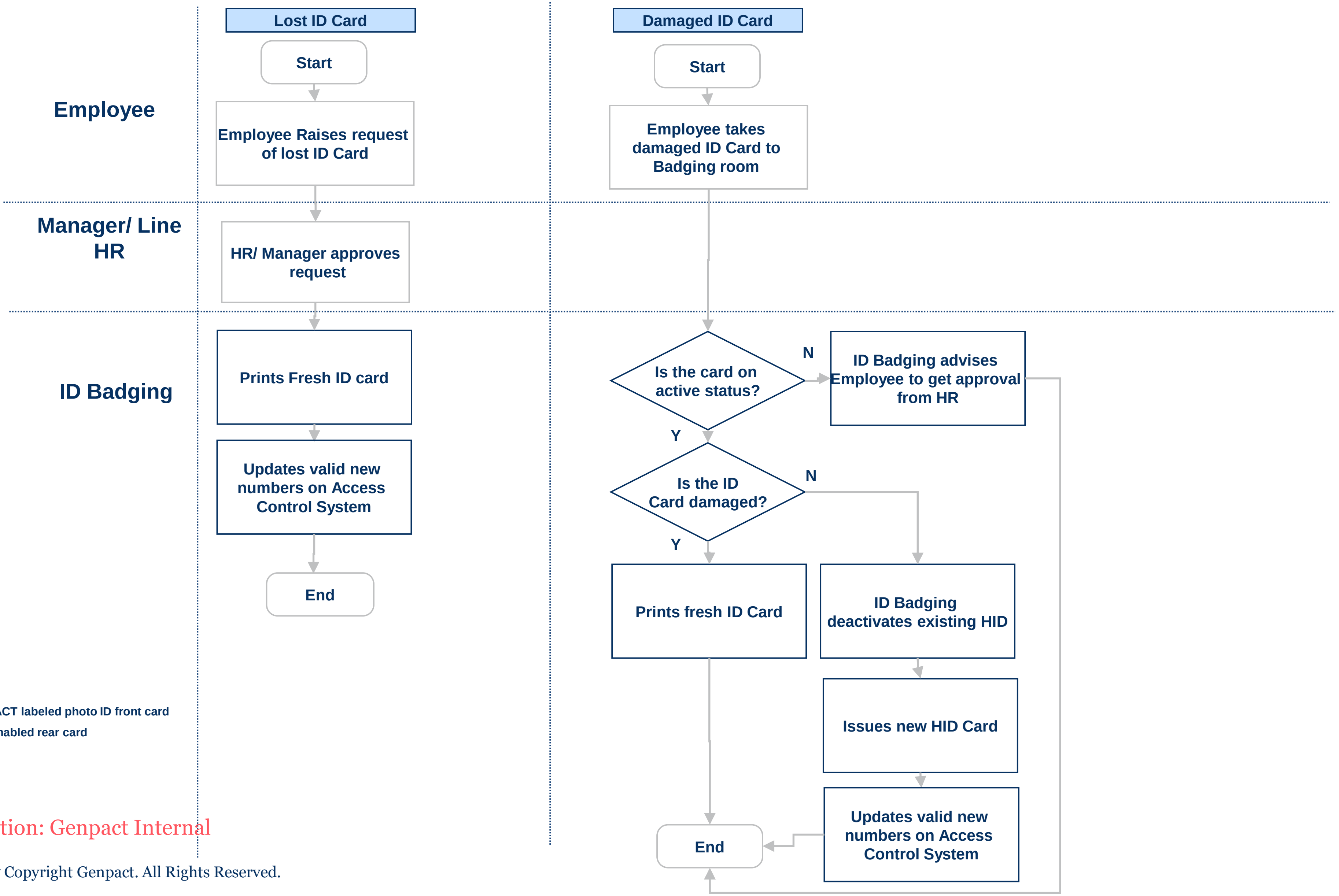
- # of New ID Cards issued vs Temporary Cards retrieved

Exception

- (*) See Site Exceptions on end section Exception list

Classification: Genpact Internal

4.2 Lost ID Card & Damaged Card



Employee

Manager/ Line HR

ID Badging

Lost ID Card

Start

Employee Raises request of lost ID Card

HR/ Manager approves request

Prints Fresh ID card

Updates valid new numbers on Access Control System

End

Damaged ID Card

Start

Employee takes damaged ID Card to Badging room

Is the card on active status?

N

ID Badging advises Employee to get approval from HR

Y

Is the ID Card damaged?

N

ID Badging deactivates existing HID

Issues new HID Card

Updates valid new numbers on Access Control System

Y

Prints fresh ID Card

End

*MIL Card are the GENPACT labeled photo ID front card

HID Cards are the chip enabled rear card

Escalation

- Trigger: No approval received from Manager
- Action:
- ID Badging Employee to inform Logistics
- Logistics inform Site Logistics Leader

Metric

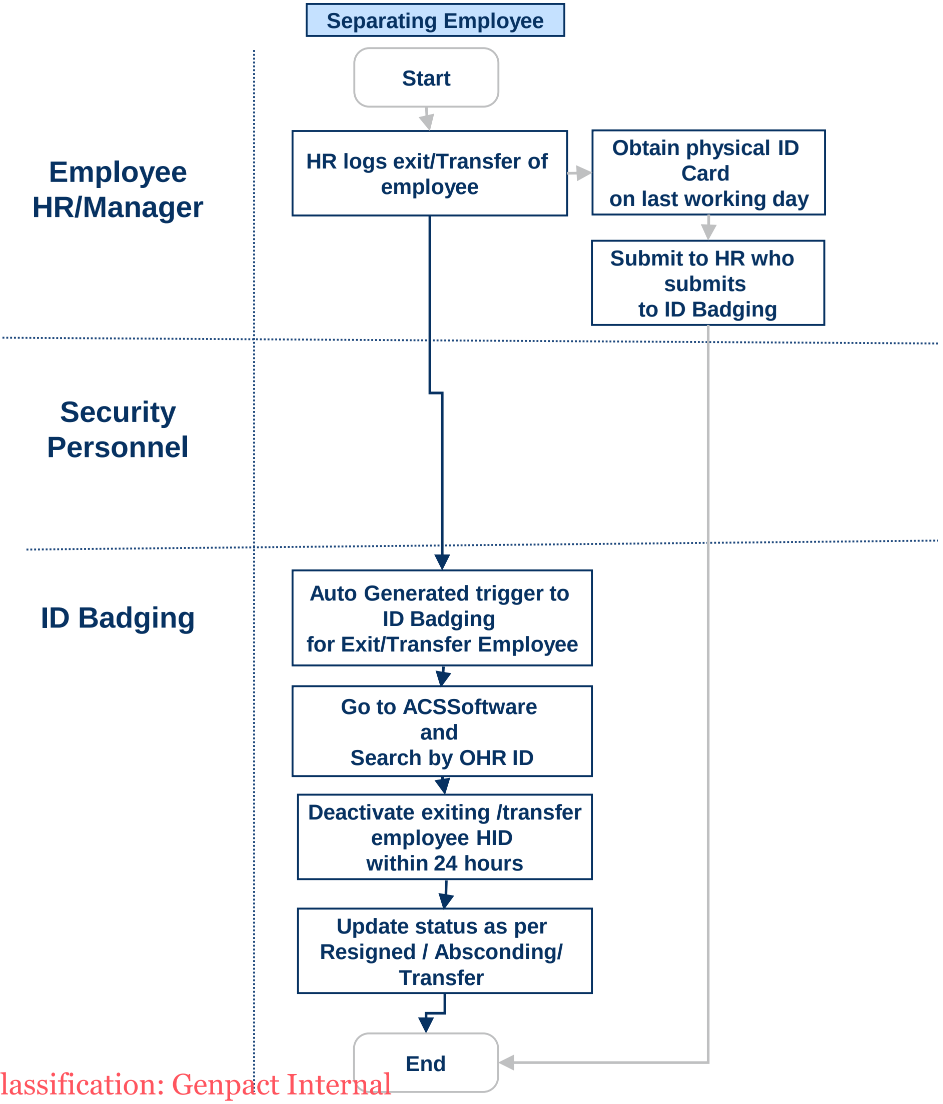
- # of New ID Cards issued

Exception

- (*) See Site Exceptions on end section Exception list

Classification: Genpact Internal

4.3 Card Deactivation


Separating Employee
Employee HR/Manager
Security Personnel
ID Badging
Start
HR logs exit/Transfer of employee
Obtain physical ID Card on last working day
Submit to HR who submits to ID Badging
Auto Generated trigger to ID Badging for Exit/Transfer Employee
Go to ACSSoftware and Search by OHR ID
Deactivate exiting /transfer employee HID within 24 hours
Update status as per Resigned / Absconding/ Transfer
End

Escalation

- Trigger:
- Software issues
- Action:
- ID Badging Employee to inform Logistics
- Logistics inform Site Logistics Leader

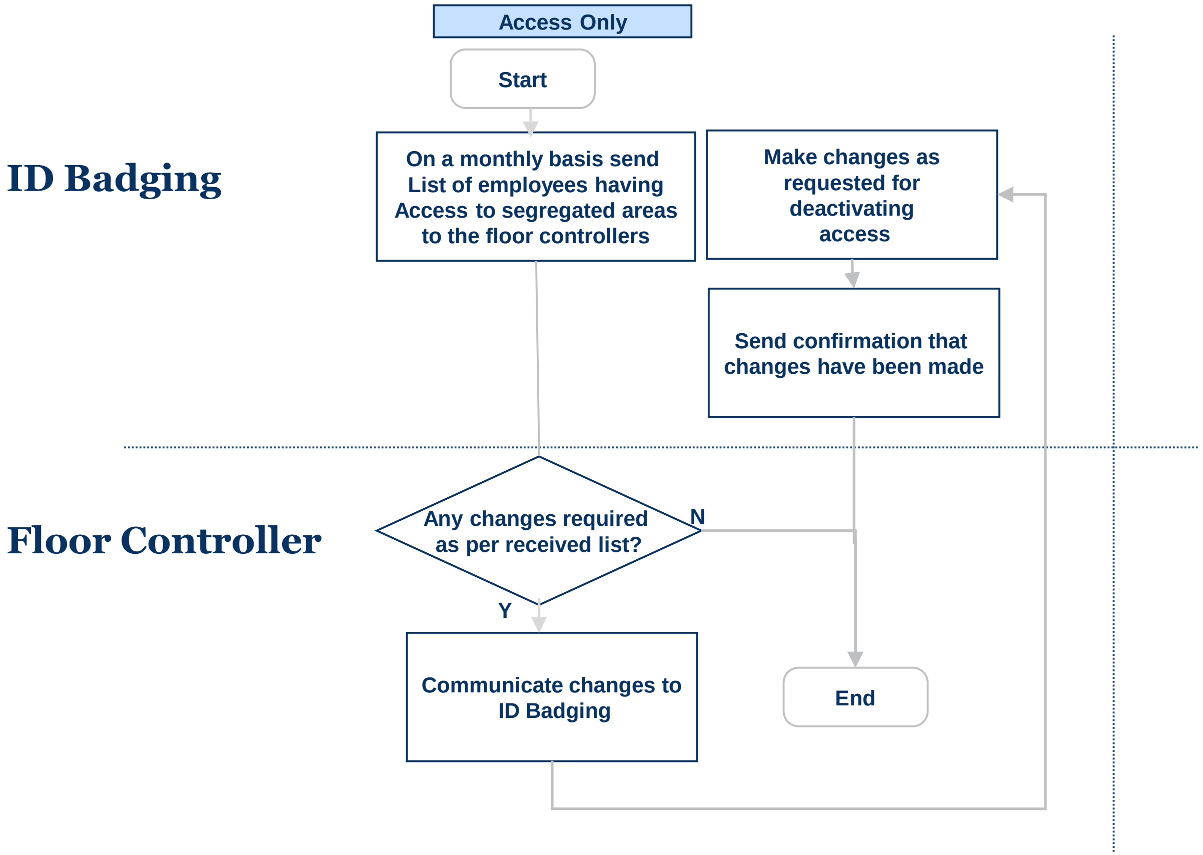
Metric

- # of Cards deactivated vs. to be deactivated

Exception

- (*) See Site Exceptions on end section Exception list

4.4 Monthly Access Reconciliation Process

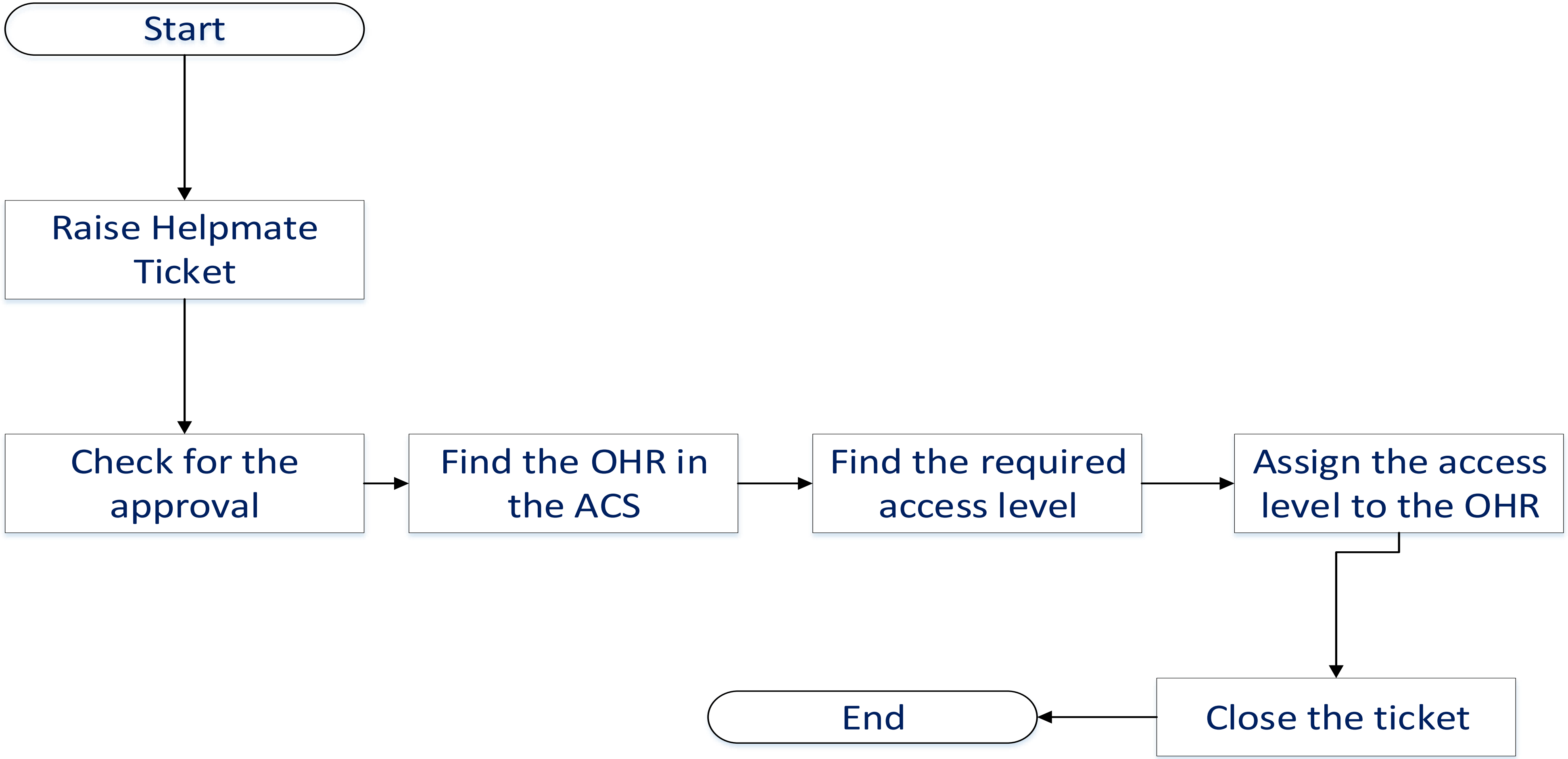

Access Only
ID Badging
Floor Controller
Start
On a monthly basis send List of employees having Access to segregated areas to the floor controllers
Make changes as requested for deactivating access
Send confirmation that changes have been made
Any changes required as per received list?
N
Y
Communicate changes to ID Badging
End

Metric

- List of access only sent to zone spocs/floor controllers.
- List to be shared by 25th of every month and the floor controller needs to validate and approve the same by the last working day
- If validation is not closed post 24 business hrs. of 3rd reminder it will be considered as auto approved with no changes required

Classification: Genpact Internal

4.5 Access Grant Process

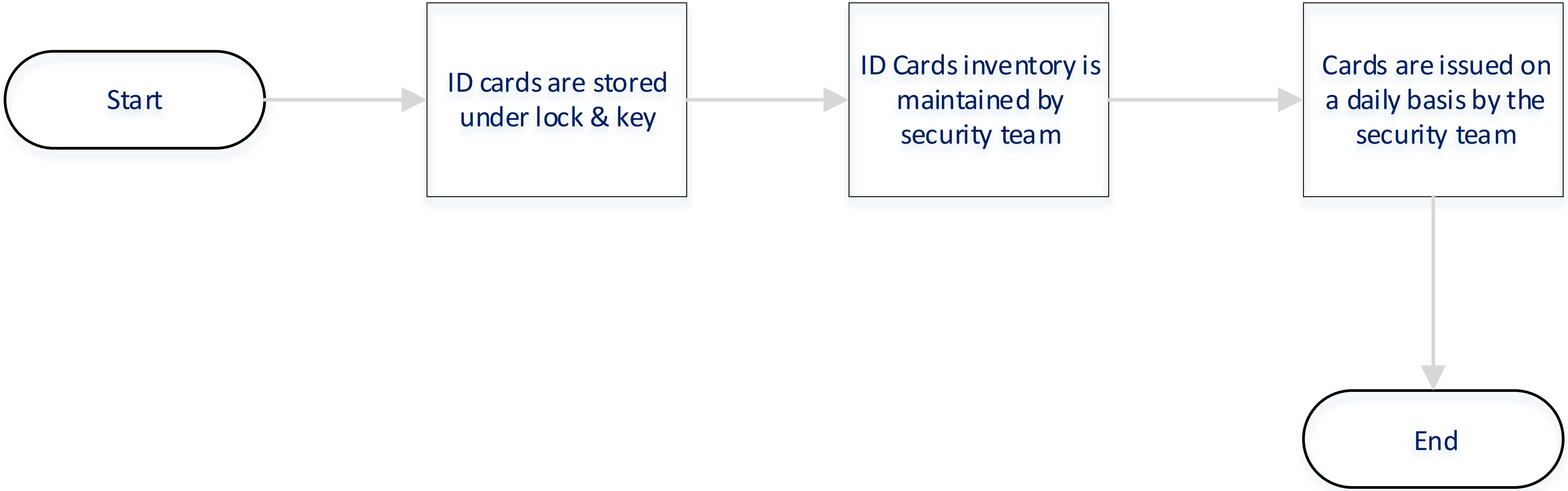


Metric

- Access granted post ticket approved on portal
- All requests to come from Helpmate

Classification: Genpact Internal

4.6 Access Card Inventory



Start
ID cards are stored under lock & key
ID Cards inventory is maintained by security team
Cards are issued on a daily basis by the security team
End

Classification: Genpact Internal

No Exceptions for Lost ID Card Damaged Card, Card Deactivation, Access Data

For all Sites :

In cases where the ID Badging is down due to software/hardware issues, stock out of MIL / HID cards a Temporary card with temp validity is issued.

Virtual Onboarding – Profile is created at the time of receipt of onboarding trigger, however card is issue to employee at the time of visiting office

*Level 1: Premises Level Access

Level 2: Building Level Access

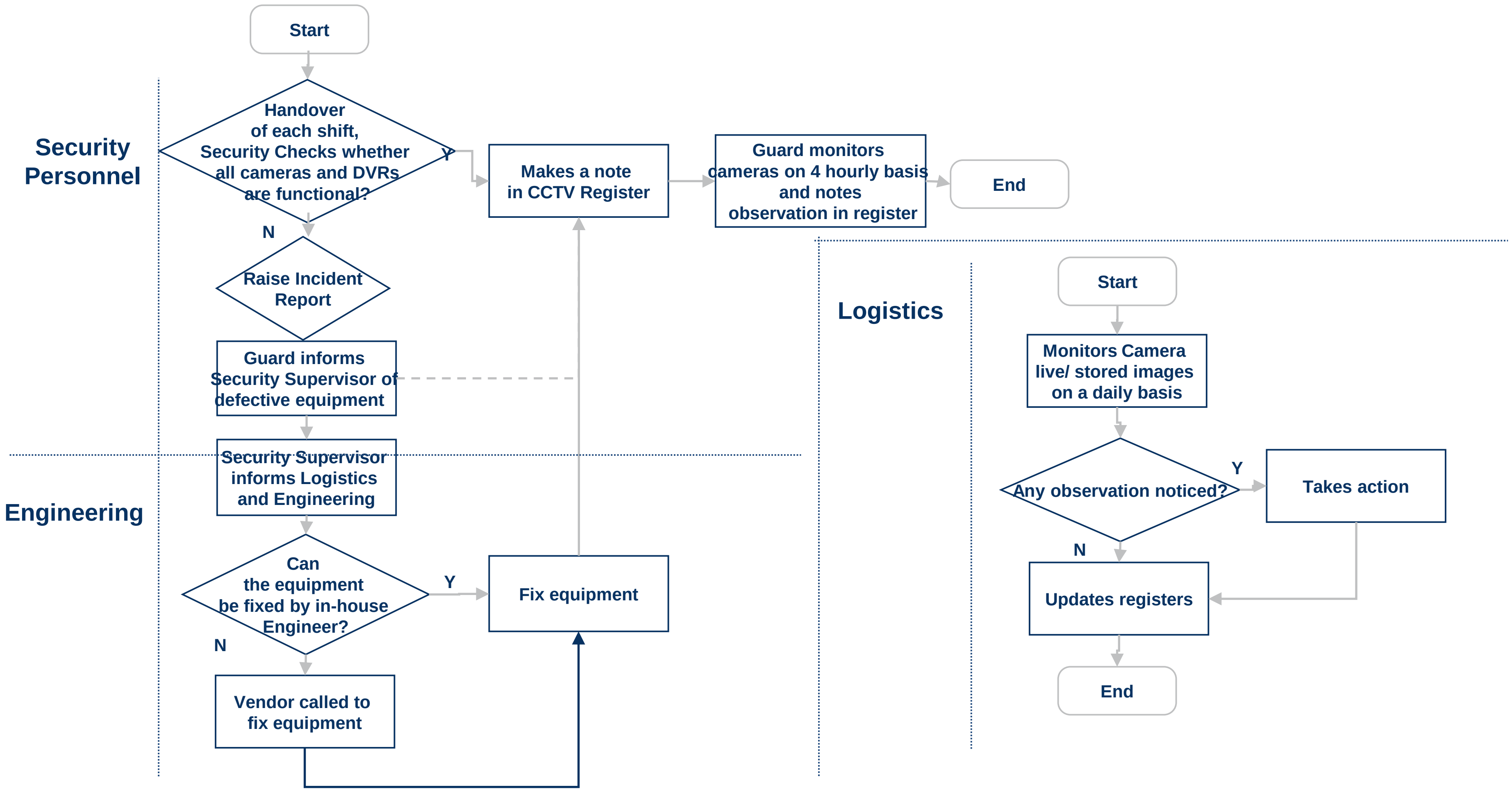
Level 3: Floor/ Process Level Access

Classification: Genpact Internal

5.0 CCTV

5.1 CCTV Equipment & Monitoring

5.1 CCTV Equipment & Monitoring


Security Personnel
Start
Handover of each shift, Security Checks whether all cameras and DVRs are functional?
Y
Makes a note in CCTV Register
Guard monitors cameras on 4 hourly basis and notes observation in register
End
N
Raise Incident Report
Guard informs Security Supervisor of defective equipment
Security Supervisor informs Logistics and Engineering
Engineering
Can the equipment be fixed by in-house Engineer?
Y
Fix equipment
N
Vendor called to fix equipment
Logistics
Start
Monitors Camera live/ stored images on a daily basis
Any observation noticed?
Y
Takes action
N
Updates registers
End

Metric

- Details noted at an interval of 4 hours by Security Guard and daily random check by Logistics
- Logistics/Security manager reviewing Live/ stored images on a daily basis.
- CCTV footage retention will be 30 days for all Entry and Exit cameras and for client areas as per MSA requirements,

Escalation

- Trigger: Any suspicious activity observed
- Action: Security Guard to inform Security Supervisor
- Security Supervisor to inform Logistics
- Logistics to inform Site Logistics Leader

Classification: Genpact Internal

No Exceptions in CCTV Monitoring

*Level 1: Premises Level Access

Level 2: Building Level Access

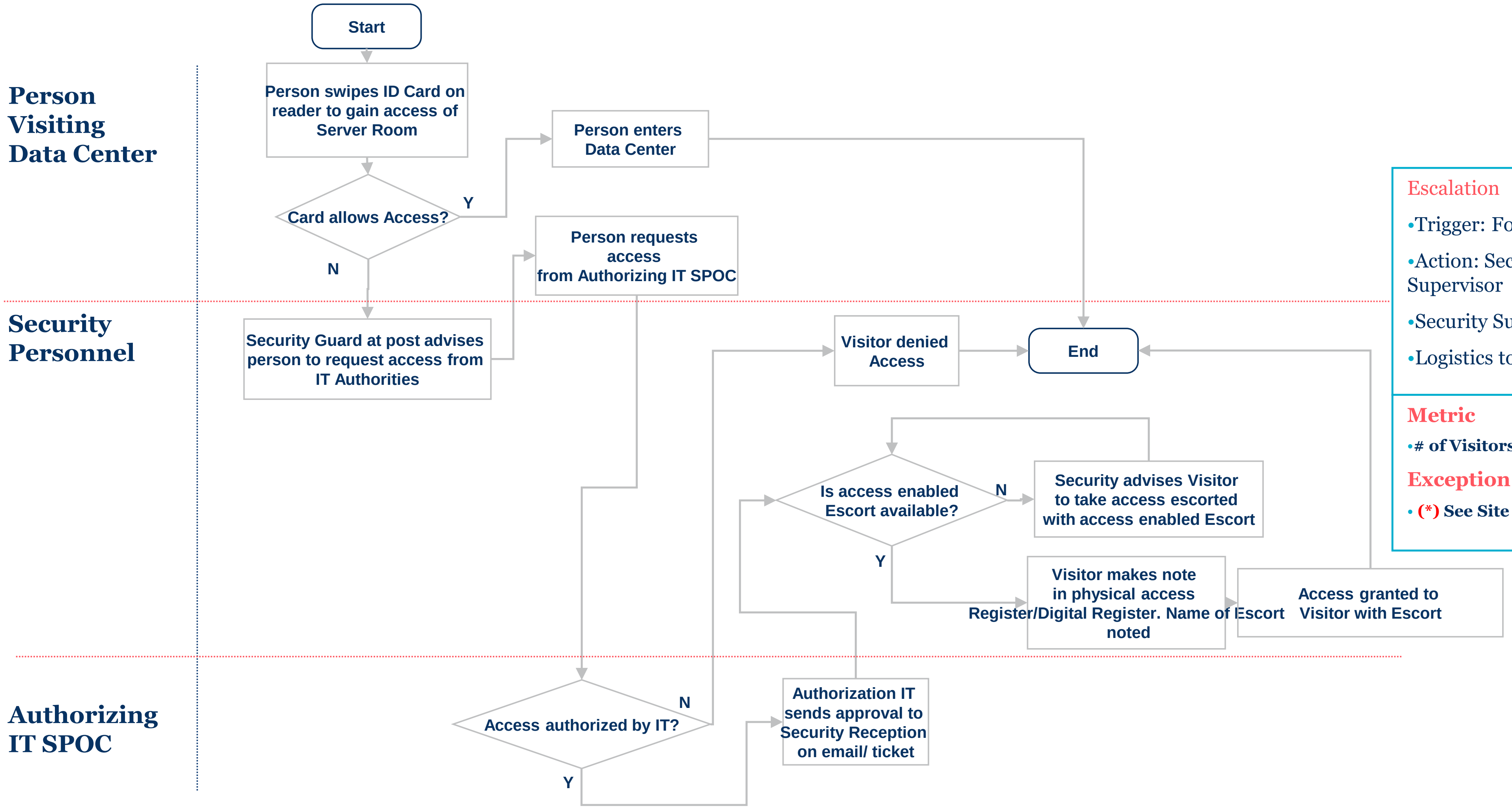
Level 3: Floor/ Process Level Access

Classification: Genpact Internal

6.0 Customized Access

6.1 Data Server Security
6.2 ODC/ Carve Outs Access

6.1 Data Server Security


Start
Person Visiting Data Center
Person swipes ID Card on reader to gain access of Server Room
Card allows Access?
Y
N
Person enters Data Center
Person requests access from Authorizing IT SPOC
Security Personnel
Security Guard at post advises person to request access from IT Authorities
Visitor denied Access
End
Is access enabled Escort available?
N
Y
Security advises Visitor to take access escorted with access enabled Escort
Visitor makes note in physical access Register/Digital Register. Name of Escort noted
Access granted to Visitor with Escort
Authorizing IT SPOC
Access authorized by IT?
N
Y
Authorization IT sends approval to Security Reception on email/ ticket

Escalation

- Trigger: Force entry to data Center
- Action: Security Guard to inform Security Supervisor
- Security Supervisor to inform Logistics
- Logistics to inform Site Logistics Leader

Metric

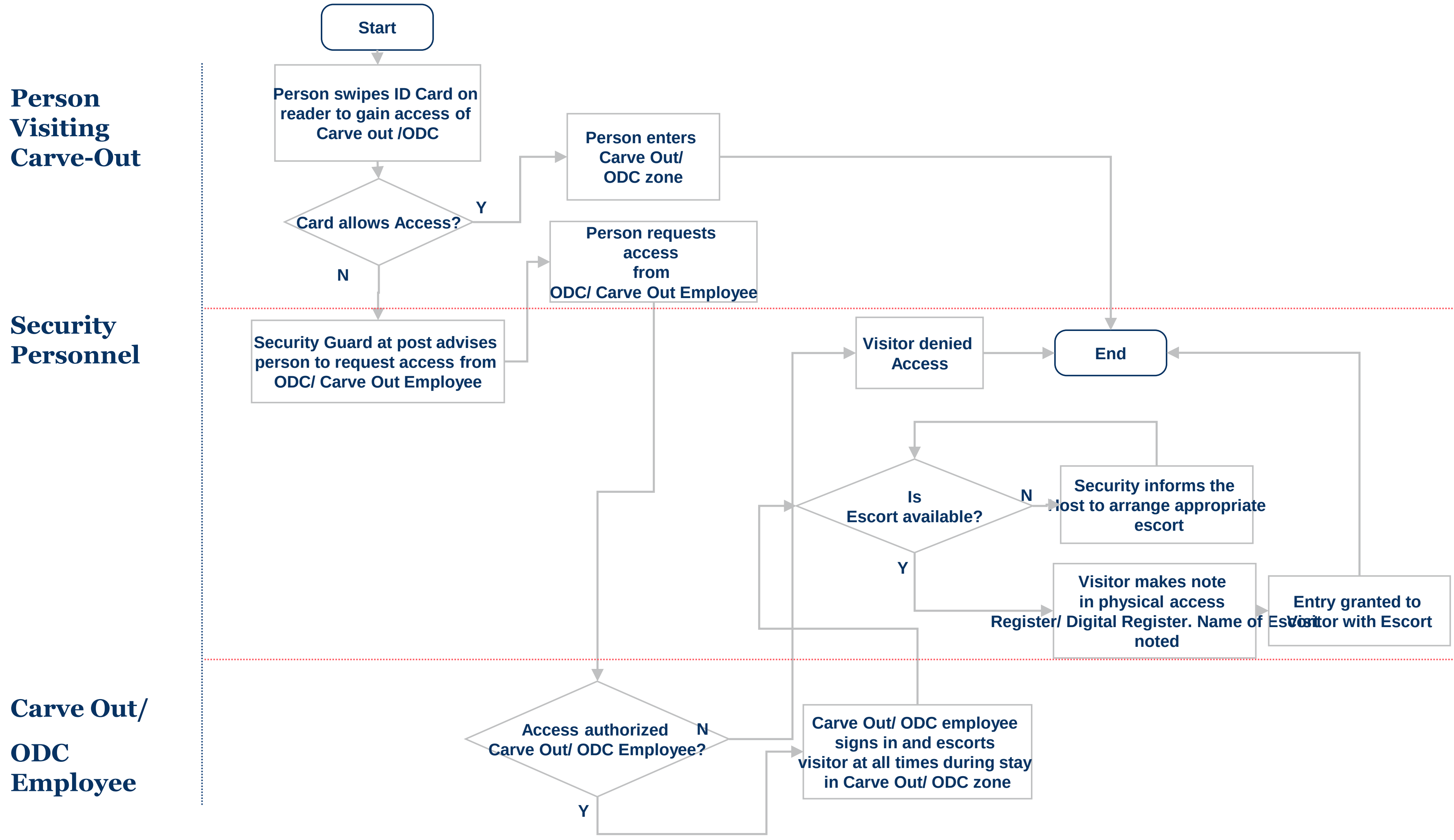
- **# of Visitors arrived**

Exception

- **(*) See Site Exceptions on end section Exception list**

Classification: Genpact Internal

6.2 Client Restricted/Segregated Areas



Person Visiting Carve-Out

Security Personnel

Carve Out/ ODC Employee

Start

Person swipes ID Card on reader to gain access of Carve out /ODC

Card allows Access?

Y

Person enters Carve Out/ ODC zone

N

Person requests access from ODC/ Carve Out Employee

Security Guard at post advises person to request access from ODC/ Carve Out Employee

Visitor denied Access

End

Is Escort available?

N

Security informs the Host to arrange appropriate escort

Y

Visitor makes note in physical access Register/ Digital Register. Name of Escort noted

Entry granted to Visitor with Escort

Access authorized Carve Out/ ODC Employee?

N

Carve Out/ ODC employee signs in and escorts visitor at all times during stay in Carve Out/ ODC zone

Y

Escalation

- Trigger: Force entry to Carve Out
- Action: Security Guard to inform Security Supervisor
- Security Supervisor to inform Logistics
- Logistics to inform Site Logistics Leader

Metric

- # of Visitors arrived

Exception

- (*) See Site Exceptions on end section Exception list

Classification: Genpact Internal

genpact

No Exceptions on Invalid access alarm, Data Server Security

Exceptions for Client Restricted/Segregated Areas

- All Business specific MSA’s have to be signed off by the Genpact CSO.
- In case of Access Control System failure/outage, all Access controlled entry and exit points will be manned by Security guards and all movement logged in a register.

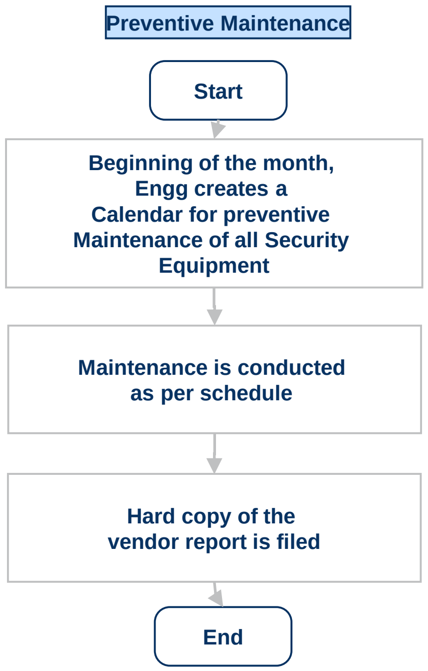
Classification: Genpact Internal

7.0 Security Equipment Maintenance

7.1 Preventive Maintenance
7.2 Corrective Maintenance

7.1 Preventive Maintenance & 7.2 Corrective Maintenance

Engineering



Preventive Maintenance

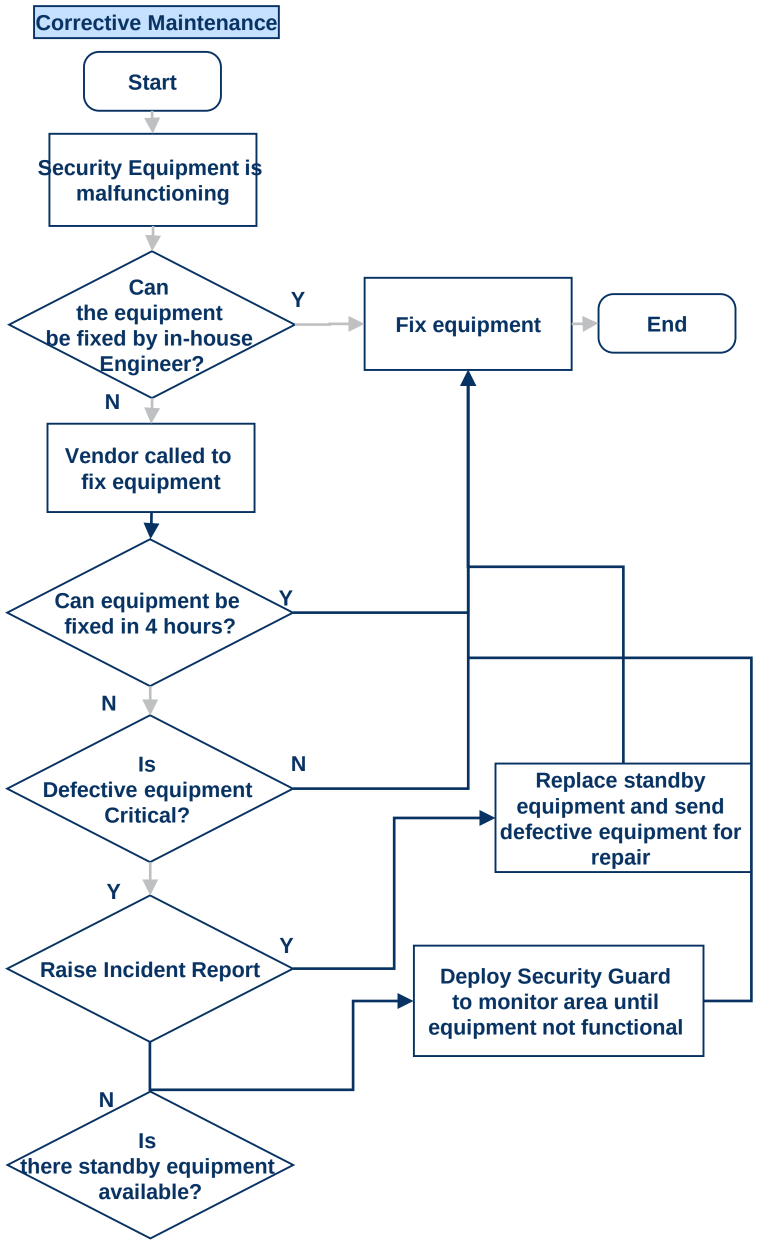
Start

Beginning of the month, Engg creates a Calendar for preventive Maintenance of all Security Equipment

Maintenance is conducted as per schedule

Hard copy of the vendor report is filed

End



Corrective Maintenance

Start

Security Equipment is malfunctioning

Can the equipment be fixed by in-house Engineer?

Y

Fix equipment

End

N

Vendor called to fix equipment

Can equipment be fixed in 4 hours?

Y

N

Is Defective equipment Critical?

N

Y

Raise Incident Report

Y

Replace standby equipment and send defective equipment for repair

N

Deploy Security Guard to monitor area until equipment not functional

Is there standby equipment available?

Metric

- No. of Preventive Maintenance Scheduled vs. conducted
- No. of Corrective Maintenance conducted

Exception

- (*) See Site Exceptions on end section Exception list

Escalation

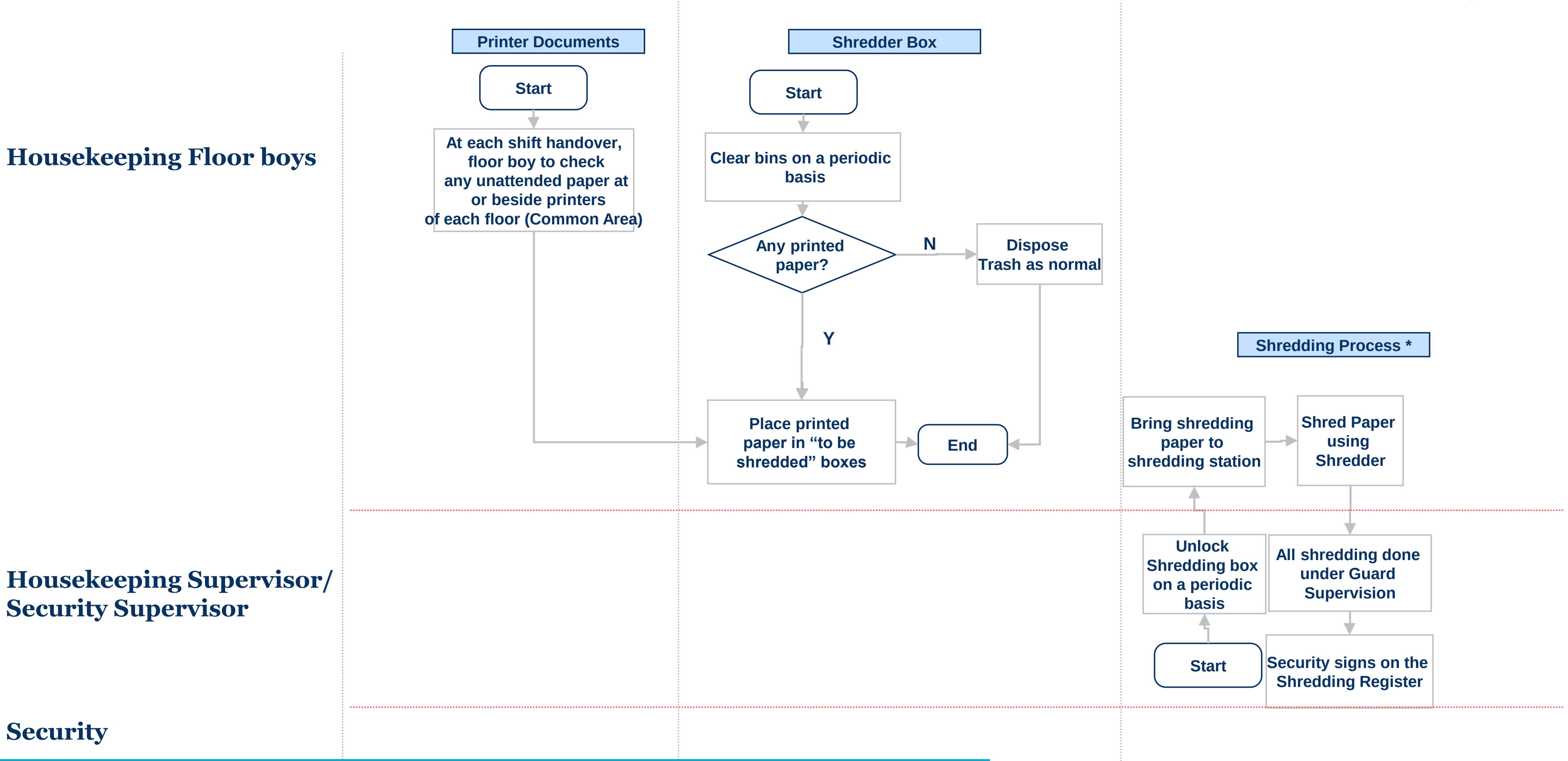
•Trigger: Maintenance not conducted as per schedule

•Action: Maintenance Engineer to inform Maintenance Supervisor, Maintenance Supervisor to Chief Engineer, Chief Engineer to inform Site Logistics Leader

8.0 Document Security

8.1 Printer Documents
8.2 Bin Documents
8.3 Shredding Process

8.1 Printer Documents, 8.2 Bin Documents & 8.3 Shredding Process


Printer Documents
Shredder Box
Shredding Process *
Housekeeping Floor boys
Housekeeping Supervisor/ Security Supervisor
Security
Start
At each shift handover, floor boy to check any unattended paper at or beside printers of each floor (Common Area)
Start
Clear bins on a periodic basis
Any printed paper?
N
Dispose Trash as normal
Y
Place printed paper in “to be shredded” boxes
End
Bring shredding paper to shredding station
Shred Paper using Shredder
Unlock Shredding box on a periodic basis
All shredding done under Guard Supervision
Start
Security signs on the Shredding Register

Escalation

- Trigger: Unshredded printed documents found in disposing trash
- No shredding done due to machine malfunction
- Action: Security Guard to inform Security Supervisor, HK/ Security Supervisor to inform Logistics, Logistics to inform Site Logistics Leader

Metric

- Shredding conducted on a weekly basis

9.0 Reporting & Monitoring

9.1 Daily Security Report
9.2 Reconciliation of VMS Cards
9.3 Inventory Kit
9.4 Facilities Audit Process
9.5 Incident Management
9.6 Document Reviewing

9.1 Daily Security Report

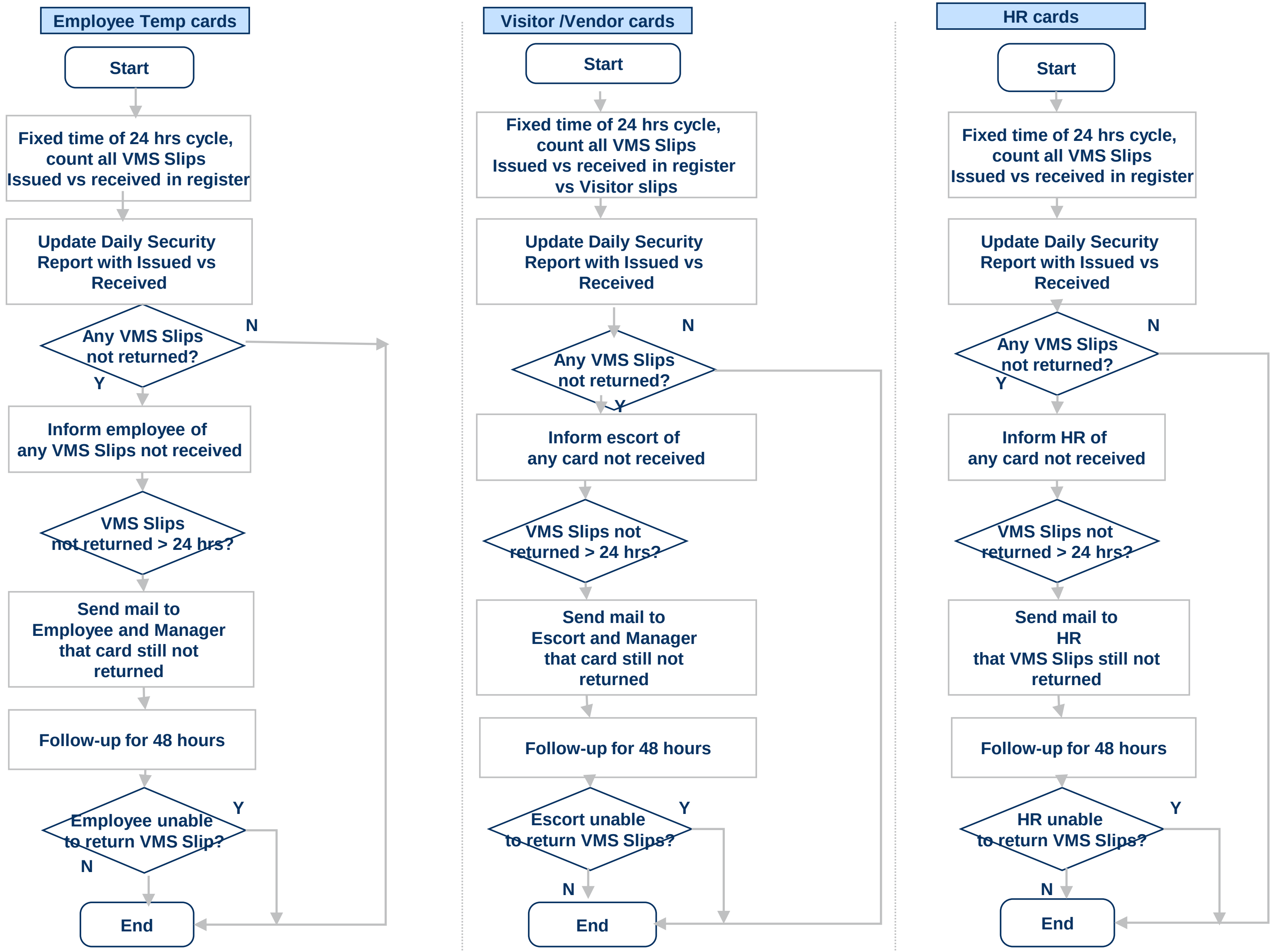
Security Assignment Manager to update following in a Daily Security Report and send to Logistics

1. Any Incidents on/ around premises
2. Security Equipment Functioning
3. Cards Reconciliation Summary
4. Guard Attendance
5. Any Lost/ Found Cases

Classification: Genpact Internal

9.2 Reconciliation of VMS Cards

Security Personnel



Employee Temp cards

Start

Fixed time of 24 hrs cycle, count all VMS Slips Issued vs received in register

Update Daily Security Report with Issued vs Received

Any VMS Slips not returned?

N

Y

Inform employee of any VMS Slips not received

VMS Slips not returned > 24 hrs?

Send mail to Employee and Manager that card still not returned

Follow-up for 48 hours

Employee unable to return VMS Slip?

Y

N

End

Visitor /Vendor cards

Start

Fixed time of 24 hrs cycle, count all VMS Slips Issued vs received in register vs Visitor slips

Update Daily Security Report with Issued vs Received

Any VMS Slips not returned?

N

Y

Inform escort of any card not received

VMS Slips not returned > 24 hrs?

Send mail to Escort and Manager that card still not returned

Follow-up for 48 hours

Escort unable to return VMS Slips?

Y

N

End

HR cards

Start

Fixed time of 24 hrs cycle, count all VMS Slips Issued vs received in register

Update Daily Security Report with Issued vs Received

Any VMS Slips not returned?

N

Y

Inform HR of any card not received

VMS Slips not returned > 24 hrs?

Send mail to HR that VMS Slips still not returned

Follow-up for 48 hours

HR unable to return VMS Slips?

Y

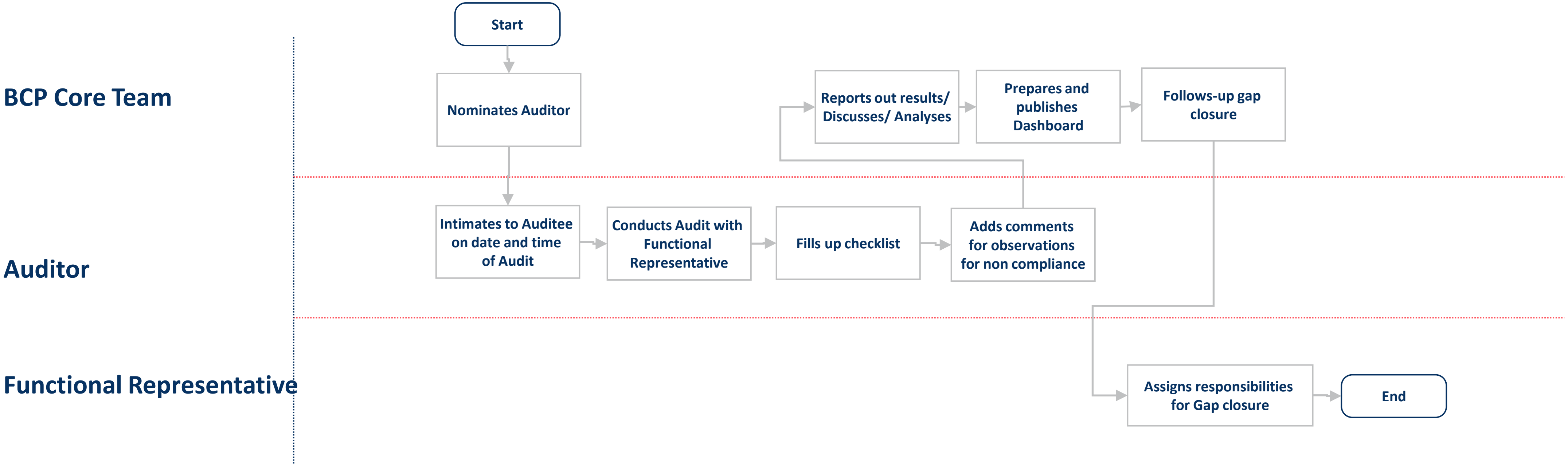
N

End

9.3 Inventory Kit

All the temporary cards that are issued at the reception that includes visitor, vendor and forgot ID cases to be reconciled from the VMS report and tracked in the register

9.4 Facilities Audit Process



BCP Core Team

Auditor

Functional Representative

Start

Nominates Auditor

Intimates to Auditee on date and time of Audit

Conducts Audit with Functional Representative

Fills up checklist

Adds comments for observations for non compliance

Reports out results/ Discusses/ Analyses

Prepares and publishes Dashboard

Follows-up gap closure

Assigns responsibilities for Gap closure

End

Escalation

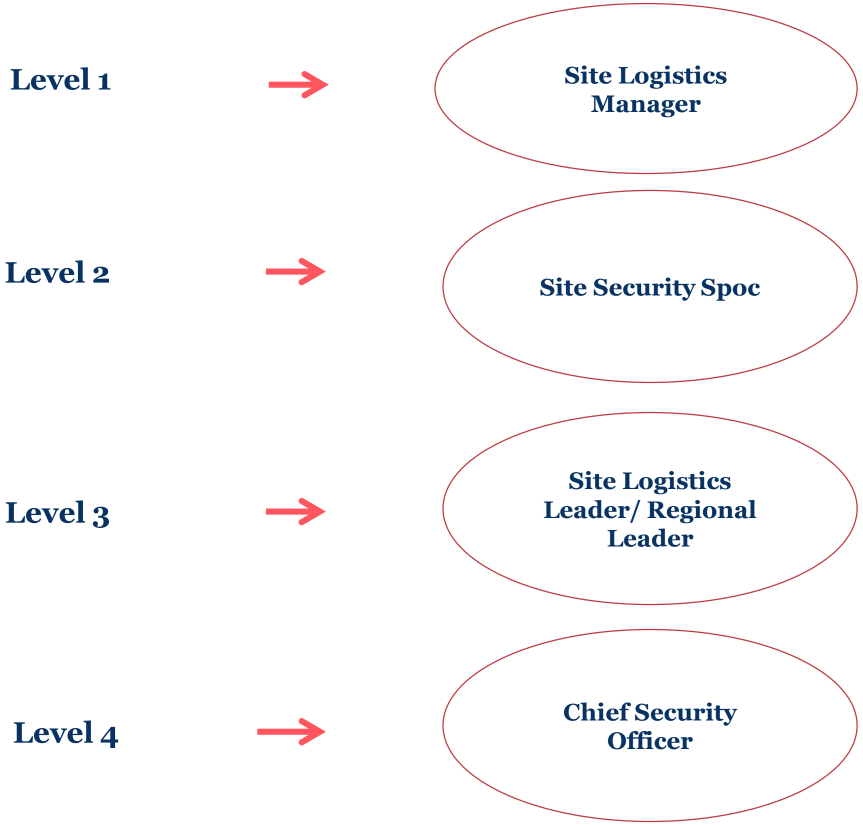
- Trigger: No auditor available to conduct audit on scheduled date
- No Functional Representative to accompany Auditor
- No input received from SLL
- Action: BCP Core Team Member to inform CML
- CML to inform SLL
- CML to inform Logistics Leader

Classification: Genpact Internal

9.5 Incident Management

Any Physical Security Incident Observed by Employee/ Floor Controllers/Logistics/Weekly checks and Audits that shall include ACS outage /failure, CCTV outage/Failure, Door not closing, Alarm ringing without reason etc. (Indicative list only)

SECURITY ESCALATION MATRIX



Level 1 → Site Logistics Manager

Level 2 → Site Security Spoc

Level 3 → Site Logistics Leader/ Regional Leader

Level 4 → Chief Security Officer

Metrics

- All reportable incidents will be documented and RCA to be carried out

Classification: Genpact Internal

9.6 Document Reviewing

		Respective Supervisor	Logistics	Security Manager	Site Logistics Leader
1	Daily Security Report	Daily		Weekly	Daily
2	Security Attendance Register	Daily	Weekly	Weekly	Monthly
3	Security Handover Register	Daily	Weekly	Weekly	
4	Housekeeping Attendance Register	Daily	Weekly	Weekly	
5	Maintenance Register	Daily	Weekly	Weekly	
9	VMS cards reconciliation registers	Daily	Weekly	Weekly	Monthly
10	Vehicle Register	Daily	Fortnightly	Weekly	Monthly
11	CCTV Register (Monitoring & Equipment)	Daily	Daily	Weekly	Monthly
12	Material In Register	Daily	Weekly	Weekly	
13	Material Out Register	Daily	Weekly	Weekly	
14	Sticker Issue File	Daily	Weekly	Weekly	
15	ID Card Issuance Register	Daily	Weekly	Weekly	Monthly
16	Shredding Process Register	Daily	Weekly	Weekly	Monthly
17	Maintenance Report	Daily	Weekly	Weekly	Monthly
18	Facilities Audit Score Card			Weekly	Monthly

Register reviewed would be countersigned with date of Review

Classification: Genpact Internal

No Exceptions on :

7.1 Preventive Maintenance

7.2 Corrective Maintenance

8.1 Printer Documents

8.2 Bin Documents

8.3 Shredding Process

9.1 Daily Security Report

9.2 Reconciliation of Cards

9.3 Inventory Kit

9.4 Facilities Audit Process

9.5 Incident Management

9.6 Document Reviewing

**** All security documents have to be maintained for a period of 18 months(under lock and key), post which they can be shredded post approvals from Site Logistics Leader.

Thank You.

genpact

Transformation
Happens Here