Version: 1.4
Updated on: Jun 2022

Physical and Environmental Security Procedure

1. Introduction

Swiggy has formulated information security policies specific to leading industry practices. This document details the security requirements pertaining to Physical Security.

The Physical & Environmental Security procedure outlines the various Physical Security Processes for effectively managing the premises of Swiggy.

This procedure is applicable to all the employees of Swiggy and support/third party staff who have physical access to Swiggy work areas and other information processing facilities e.g. server room, AHU room, Electrical room of Swiggy.

The procedure includes the following:

- Ensure that the premises and work areas of Swiggy are adequately protected against unauthorized physical access.
- Ensure that equipment owned and/or utilized by Swiggy is protected against unauthorized physical access.

2. Purpose

The objective of this policy is to educate end users and stakeholders on Physical & Environmental security of company information and information processing facilities. Swiggy shall ensure that all employees, contractors and third-party staff shall protect Swiggy information assets as defined by the policies, procedures and guidelines and only for business purposes.

Version: 1.4
Updated on: Jun 2022

3. Procedure Details for Physical Security

3.1 Business Requirement for Physical Access Control

Access to the information and information systems shall be controlled on the basis of business and security requirements. Physical access controls shall be deployed to protect information and systems of Swiggy from unauthorized access.

3.2 Physical Access Control

3.2.1 Perimeter Security

The following guidelines shall be followed to ensure that Swiggy premises are adequately protected against unauthorized access:

- The perimeter of the Swiggy premises shall be manned by security personnel on a 24X7 basis. In case of shared facilities, the Swiggy work area at each floor is treated as the premises to be secured.
- Security personnel shall be posted at entrance gates of facility. In case of shared facilities, the entrance to the work area is treated as the entrance gate.
- In case the facility is owned and /or maintained by Swiggy, security personnel shall be posted at the parking lot of the facility. Security personnel are instructed to check the identity of the occupants of a vehicle prior to granting entry to the vehicle.
- All security personnel are instructed to check the identity of any unidentified personnel entering the facility.
- Security personnel are instructed to check gate passes for all incoming and outgoing material to ensure that necessary approvals have been obtained for the material movement.

3.2.2 Physical Access

- Physical access rights shall be restricted to the employees of Swiggy. Personnel other than the employees of Swiggy shall be granted temporary entry rights.
- The main entry of Swiggy premises shall be secured using a manned reception.
- Other than the Swiggy employees, authorized person from the Swiggy administration and IT departments shall have access to Swiggy, for the maintenance of Swiggy work area.
- Swiggy Management team shall also be provided access to the Swiggy premises as per business requirements.
- For housekeeping purposes, authorized personnel shall be granted access to Swiggy premises. The housekeeping personnel will work under the supervision of security personnel.
- All visitors shall be guided to contact the reception to obtain the visitor pass.
- All visitors are to be restricted only to the reception area.
- The physical access to Swiggy premises shall follow Below Access Control Procedure.

3.3 Material Movement

Material movement, in and out of Swiggy premises shall be restricted and controlled by security personnel.

Material Movement Registers shall be used to monitor and regulate the movement of all incoming and outgoing material to and from Swiggy premises. The register shall be used to record the details of all materials moving into and outside the Swiggy premises.

Records of Material Movement Registers shall be maintained. Security personnel at the reception shall verify the identity and particulars of personnel moving material in and out of company premises make an entry.

3.3.1 Incoming Material

- On arrival of any incoming material, Security personnel shall check accompanying documentation and inform the concerned person who is the receiver of the material.
- Security personnel shall ensure that particulars of all incoming material are recorded in Incoming Material Register after physically verifying the item and its quantity and shall then endorse the security seal (date/time/number/signature) in the document.
- The authorized person who is receiving the material shall also enter their particulars in the register.
- Incoming materials shall be received only during business hours. Prior intimation and approval shall be given to security personnel in writing or by e-mail, in case of any incoming material arriving beyond business hours or holidays.

3.3.2 Outgoing Material

- Any material going out of the premises shall be accompanied with a valid returnable/non-returnable gate pass.
- Security shall physically check the outgoing material as per the contents described in gate pass and enter the particulars in the returnable /non-returnable Outgoing Material Register.
- The person taking the material shall also enter his particulars in Outgoing Material Register.
- The Administration and Facilities team shall be responsible for maintaining this register.
- All the columns must be filled in, legibly and clearly and include particulars such as date, time, and description of material and authorized signatory sign-off.

3.4 Classification of Areas

All Swiggy areas and facilities are classified into three broad zones, based on criticality to business and safety.

3.4.1 Zone A

Perimeter of the facility and all general access areas until reception/security checkpoints. There are no restrictions on accessing these areas. In case of shared facilities, access rights will be determined and controlled by building/facility management.

3.4.2 Zone B

General work and access areas beyond reception/security checkpoints. Access to these areas shall be restricted by access control systems. Personnel other than the employees of Swiggy shall be granted access after necessary approvals are obtained. Visitors to these areas shall be escorted by an employee of Swiggy at all times.

CCTVs shall be installed at prominent locations within Zone B areas.

3.4.3 Zone C

Comprises of areas where information and information processing facilities critical to business and production are handled and/or stored. This includes server rooms, hub rooms and other work areas where confidential information is processed, or critical assets such as DG sets, UPS, HVAC, cabling risers etc. Access to these areas shall be limited only to authorized employees, contract staff and other essential personnel.

Visitors to Zone C areas require approval specific to these areas, before being granted access.

All access points to Zone C areas shall be covered by CCTV surveillance.

3.5 Visitor Management

- All visitors to Swiggy premises shall register at the reception/security checkpoint.
- Security personnel shall verify the identity of visitors and particulars of the visit.
- Security personnel shall inform the employee being visited (Host).
- Visitors shall record their particulars(shall include assets like laptop, Camera, Pen drive, External HDD, etc.) in the visitor register. The host must also sign the register next to the visitor entry. Security personnel will be responsible for maintaining this register.
- Visitors shall be provided with a Visitors Badge, which should be displayed prominently, at all times within company premises and work areas.
- All the visitors shall be escorted by their respective hosts / Security or a designated employee, inside company premises, at all times.
- During exit, visitors shall return the Visitor Badge to security personnel, and record particulars of exit in the visitor register. Baggage check shall be carried out by security personnel.
- Records of visitor registers shall be maintained.

3.6 Register Maintenance Procedure

Physical security registers are of paramount importance, for capturing/recording information about movement of personals and materials at Swiggy. A list of physical security related procedures are listed below

3.6.1 Visitor Register

This register will monitor and regulate the movements of all the visitors entering the company premises. All the visitors who visit the company for business/ personal reasons must use the register. Visitor register must Include visitor's asset details (like: Laptop, Camera, etc.) also.

- Usage Guidelines:
- Visitors must display their badges at all times and shall register with the security office.
- All the visitors must be escorted by their respective hosts / Security at all the time. Under no circumstances will a visitor move unescorted. The host must also sign the register next to the visitor entry.
- The physical security personnel will be responsible for maintaining this register.
- All the columns must be filled legibly and clearly.

This register must be retained for auditing purpose.

3.6.2 Material Movement Register

This register will monitor and regulate the movements of all materials moving in and out of the office premises. This register records all materials that belong to Swiggy or its Vendors / Clients / Contractors moving 'in' and 'out' of the company premises. The custodian / owner of the material, who is making the movement of the material, must update the register.

Usage Guidelines:

Incoming Material

- On arrival of any incoming material, Security team should check the document and inform the concerned person who will in turn receive the material.
- Security team should ensure that all incoming material should be recorded in the incoming Material Register after physically verifying the item and quantity and endorse the security seal (date/time/no/signature) in the document.
- The authorized person who is receiving the material should sign the register.
- Incoming materials should be received between 0900 hrs. and 1800 hrs. Prior intimation should be given to Security in writing / mail, in case of any incoming material beyond 1800 hrs. or on weekends/holidays.

Outgoing Material

- Any material going out of the premises should be accompanied with a valid returnable/non-returnable gate pass duly signed by the authorized signatory.
- Security should physically check the outgoing material as per the contents in Gate pass and enter the details in the returnable /non-returnable material register.
- The person taking the material should sign the outgoing material register.
- The security team will be responsible for maintaining this register.
- All the columns must be filled in, legibly and clearly.
- This register must be retained for audit purpose.

3.6.3 Key Register

This register shall track the movement of keys for restricted rooms/cabins issued to employees. The employees who are owners of the restricted rooms or have a need to use, must use this register.

Usage Guidelines:

- Owners of the restricted rooms shall make entry in the register for obtaining keys to common rooms/cabins/desk cabinets and cupboards.
- Security needs to provide the keys only to the owner of the restricted rooms or on appropriate authorization from the owner for any other employee.
- Keys shall be returned to the security after the intended use and no keys other than employee desk cabinets shall be taken out of the facility.
- Visitors/Contractors shall not be given the keys without appropriate authorization from the owners.
- All the columns must be filled legibly and clearly.

This register must be retained for a period of one year.

3.7 CCTV Monitoring

Introduction:

Swiggy uses closed circuit television (CCTV) images to provide a safe and secure environment for employees and for visitors to the Company's business premises, such as clients, customers, contractors and suppliers, and to protect the Company's property.

This policy sets out the use and management of the CCTV equipment and images in compliance with the Data Protection Act 1998 and the CCTV Code of Practice.

Purposes of CCTV

The purposes of the Company installing and using CCTV systems include:

- To assist in the prevention or detection of crime or equivalent malpractice
- To monitor the security of the Company's business premises
- To ensure that health and safety rules and Company procedures are being complied with.
- To assist with the identification of unauthorized actions or unsafe working practices that might result in disciplinary proceedings being instituted against employees and to assist in providing relevant evidence

Location of cameras

CCTVs shall be installed at prominent locations within company premises. In addition, all entry/exit points and at least Zone C areas shall be covered by CCTV surveillance. No camera focuses, or will focus, on toilets, shower facilities, changing rooms, staff kitchen areas.

Version: 1.4
Updated on: Jun 2022

Following are the key considerations for CCTV monitoring at Swiggy premises:

- CCTV recording shall be retained for a period of 30 days.
- CCTV cameras shall be positioned such that they are not vulnerable to theft, vandalism or tampering.
- Access to CCTV images shall be restricted to authorized members (approval should come from Admin head) of the Administration team.
- Only viewing rights shall be assign to all regional authorized personnels of Admin team.
- Disclosure of CCTV images/recordings to third parties is prohibited unless required by the law enforcement agencies for investigations or for purpose of audit, and only under explicit approval.
- Administration and Facilities shall ensure that CCTV cameras capture clear images to ensure effective monitoring.

Access to and disclosure of images

Access to, and disclosure of, images recorded on CCTV is restricted. This ensures that the rights of individuals are retained.

The images that are recorded are stored centrally. Access to recorded images is restricted to the operators of the CCTV system i.e. Admin team line managers who are authorized to view them upon request as detailed below.

Disclosure of images-will only be made in accordance with the purposes:

- The police and other law enforcement agencies, where the images recorded could assist in an investigation.
- Courts and other quasi-judicial authority.
- Line managers involved with Company disciplinary and performance management processes.
- Individuals whose images have been recorded and retained (unless disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders).
- Internal Complaint Committee and/or Enquiry committee constituted

and are approved by the Legal Head of the Company. Admin team shall ensure the approval from Legal Head is in place before disclosure of images of recording.

All requests for disclosure and access to images will be documented, including the date and time of the disclosure, to whom the images have been provided and the reasons why they are required. If disclosure is denied, the reason will be recorded.

The Admin team shall respond promptly and in any case within 10 working days considering following criticality of the request:

P0 - The request has to come within 5 hrs of the incident and same shall be taken care in 12 to 24 working Hrs.
P1 - The request has to come to admin team within 5 to 24 Hrs of the Incident and the same shall be investigated/resolved in 24 to 72 working Hrs.
P2 - The request has to come to admin team within 32 to 48 Hrs of Incident and same shall be Investigated / resolved in 10 working days. This time boundaries excludes any technical exigencies and may get delay in investigation / resolution.

All P0, P1, P2 request should come with 3 levels of email(online if any) approval and then only considered for the investigation.
Level of three approvals is as below:

1st level of approval - city head/ process head(Corporate)
2nd level of approval - HR (AVP)
3rd level of approval - Legal(only for P0 Incidents)

Staff training

The Company will ensure that all employees handling CCTV images or recordings are trained in the operation and administration of the CCTV system and on the impact of the Data Protection Act 1998 with regard to that system.

Implementation

The Company's Administration team shall be responsible for the implementation of and compliance with this procedure and the operation of the CCTV system and they will conduct a regular review of the Company's use of CCTV. Any complaints or enquiries about the operation of the Company's CCTV system should be addressed to Admin team.

3.8 Physical Security

- Swiggy must ensure that a admin team exists to take care of the physical infrastructure.
- Swiggy must ensure that different zones are identified based on the sensitivity of the data contained in the zone and the information technology components in the zone.
- It is recommended that the zones have different physical security requirements based on the data contained in the zone, sensitivity, confidentiality and availability of the information.
- Swiggy should ensure that the requirements for each zone is determined through risk assessment.
- It is recommended that the risk assessment must consider the factors such as, threats like aircraft crashes, chemical effects, dust, electrical supply interference, electromagnetic radiation, explosives, fire, smoke, theft/destruction, vibration/earthquake, water, criminals, terrorism, political issues (e.g. strikes, disruptions) and other threats based on the entity's unique geographical location, building configuration, neighboring environment/entities, etc.

3.9 Zone 'C' access control procedure

- Request should receive from user with department Head email approval with below details:
    - Employee Name
    - Employee ID
    - Email ID
    - Area to get access (e.g. Server/ HUB room) details
    - Location

- IT Compliance / Admin team will provide the access for the User accordingly
- Access control review for Server/ HUB room shall be done on quarterly basis by IT team
- IT Compliance team shall be responsible for IT Server & HUB room access control
- Admin team shall be responsible for rest access control

Version: 1.4
Updated on: Jun 2022

4. Procedure for Environmental Security

4.1 Equipment Maintenance

4.1.1 Equipment Protection

All critical equipment of Swiggy including the servers, firewall, network switch, file servers and the computing device hosting the access control application have been stored within the network/ server room. Access shall be restricted to only the IT team, authorized administration staff and network room owner. The access shall be controlled through the use of proximity cards and/or biometric scanners

Equipment shall be appropriately sited and protected from security threats and environmental hazards. Access controls and posting of security guards shall be considered where necessary.

In case of facility owned and/or maintained by Swiggy, security personnel shall be responsible for safeguarding equipment and assets located externally such as DG sets, UPS, etc.

Security personnel shall ensure that equipment is protected from unauthorized access. In case of shared facilities, Swiggy shall ensure that adequate protection of the utilities is provided by the facility/ building management.

Portable equipment taken out of Swiggy premises shall not be left unattended in public places if portable equipment is not used or is unattended within the office, it shall be stored in lockable cabinets with proper key control.

Controls shall be implemented to minimize the risk arising from potential threats to include:

- Theft
- Fire
- Explosion
- Water
- Dust and other particulate contamination
- Electrical supply interference

The Administration & Facilities Team shall monitor environmental conditions. Conditions that could adversely impact information and information processing facilities shall be immediately reported to concerned stakeholders.

Temperature and Humidity monitoring shall be carried out for all server rooms, hub rooms, UPS storage areas etc.

When selecting a site for new facility, a risk assessment exercise shall be carried out and its results taken under consideration.

All network, telecommunication and power cables shall be enclosed within dedicated conduits to prevent interference. All cabling activities shall be monitored by Swiggy personnel to ensure that information and information assets are not compromised.

In shared facilities where cabling security is the responsibility of facility/building management, Swiggy shall monitor steps taken to safeguard cabling equipment. An agreement shall be signed with facility/building management, with regard to cabling security and maintenance.

4.1.2 Cabling Security

All cabling activities are carried out by authorized vendors and the vendor agreements address the security requirements to be adhered to by the vendors. The Swiggy IT team shall work with the vendors and ensure that Swiggy information assets are not compromised.

4.1.3 Off-Premises Security of Equipment

Any equipment moved out of the Swiggy facility shall follow the material movement process outlined in this procedure.

An entry shall be made in the Material Movement register and the necessary approvals shall be obtained and recorded in the Material Movement register.

4.1.4 Secure Removal of Equipment

The equipment containing licensed software and Swiggy internal information shall be securely overwritten by the IT team prior to removal of the equipment from the Swiggy premises.

4.2 Fire Suppression and Detection Systems

Swiggy premises shall be equipped with smoke detectors. In case of a fire, the smoke detectors raises an alarm to alert security stationed at the entrance of the office premises and the smoke indicators alert the building security. Fire extinguishers should be present on all floors and the network room of Swiggy. Water sprinklers shall be present in the facility other than in the Server Room.

4.2.1 Fire Drill – Mock Testing

Mock fire drills need to be performed twice a year to maintain the preparedness for emergency evacuation at all times. A checklist will be used to evaluate the effectiveness and efficiency of the evacuation process. The evacuation procedure in case of emergency has been documented in the Incident Management Plan.

4.3 Data Centre – Physical Infrastructure Management

Administration and Facilities team shall ensure the following controls in the data center & network equipment room

- On line UPS of appropriate load capacity to provide constant power during faults, blackouts and degraded power supply
- Glass windows shall not be allowed in the Data Centre and network equipment room
- Data center shall not be located in close proximity to high probability environmental risks (like munition dumps, explosives, chemical storage or processing facility, military base etc.)

- Fire Suppression systems shall be installed to prevent fire
- Smoke detectors above ceiling shall be installed
- Emergency lighting, powered by a supply other than the main power, shall be implemented
- Temperature within the data center shall be periodically monitored and controlled.
- Air conditioning systems shall have a dust filtering system installed
- All scheduled testing and maintenance of equipments within the data center shall be performed with proper approvals from the Director/Head of Administration and Facilities.
- Server rooms shall not be used for storage and will be clear of all unnecessary equipment and materials not in use

Glossary of terms:

1. **P0 -** Incidents which are called for any emergency requiring urgent attendance by police, fire or ambulance. If the incident is of a criminal nature, it shall be immediately referred to the Victorian Police for further investigation. These procedures do not override any State or Commonwealth Act in relation to unlawful activity.
2. **P1 -** Incidents which directly affect on company operations
3. **P3 -** Incidents related to company owned personal assets**.**

Revision History:

Version	Version Date	Effective from	Prepared by	Reviewed By	Approved by
1.4	28th Jun 2022	28th Jun 2022	IT Compliance	IT, HR, Admin & Legal Team	Sriharsha Majety CEO
1.3	28th Jun 2021	28th Jun 2021	IT Compliance	IT, HR, Admin & Legal Team	Sriharsha Majety CEO
1.2	28th Jun 2020	28th Jun 2020	IT Compliance	IT, HR, Admin & Legal Team	Sriharsha Majety CEO
1.1	28th Jun 2019	28th Jun 2019	IT Compliance	IT, HR, Admin & Legal Team	Sriharsha Majety CEO
1.0	29th Jan 2018	5th Feb 2018	IT Compliance	IT, HR, Admin & Legal Team	Sriharsha Majety CEO

Version: 1.4
Updated on: Jun 2022