IT Security Policy

Document Control

Document #	IT Security Policy	**Approved By**	InfoSec Head
Version	1.4	**Reviewed By**	GRC Head
Approved on	10/07/2025	**Created By**	GRC Manager
Status	Approved		

Disclaimer

1. Do not forward or copy data in part or full without explicit permission of Infosec Team
2. At a minimum, this procedure will be reviewed/updated annually
3. Change history must be updated when any edits are made to the document
4. Please contact infosec@swiggy.in to request changes to the document

Revision History

Version	Date	Author	Reviewer	Approver	Change Description
1.4	10/07/2025	GRC Manager	GRC Head	InfoSec Head	Periodic review
1.3	10/07/2024	GRC Manager	GRC Head	InfoSec Head	Periodic review
1.2	29/05/2024	GRC Manager	GRC Head	InfoSec Head	Clear inputs added for IM communication
1.1	23/05/2024	GRC Manager	GRC Head	InfoSec Head	Entity Name change from Bundl Technologies Pvt Ltd. to Swiggy Ltd
1.0	18/07/2023	GRC Manager	GRC Head	InfoSec Head	Initial Document

Access List

List of Users	Access Type	Type of Media	Retention Period
Steering Committee	Read	Soft Copy	Default
INFOSEC Team	Read/Write/Modify	Soft Copy	Default
Employees	Read	Soft Copy	Default

Acronyms Used

Acronym	Expanded Form	Acronym	Expanded Form
IM	Instant Messaging		
Swiggy	Include Subsidiaries		

Review

This methodology document shall be reviewed on an annual basis or as per the need.

INDEX

Contents

1 Introduction

1.1. DOCUMENT OBJECTIVE

The objective of this policy is to enable end users to understand the security requirements and policies to be followed for the day-to-day computing activities. It is aimed at providing preventive / corrective measures to be taken in order to minimize the risks arising out of computing resources used by end users.

This policy provides guidelines for the protection and use of information technology assets and resources within the business to ensure integrity, confidentiality and availability of data and assets. “data” means any data or information that is proprietary to the SWIGGY, whether in tangible or intangible form, including, but not limited to: (i) any marketing strategies, plans, financial information, or projections, operations sales estimates, business plans and performance results relating to the past, present or future business activities; (ii) data related to products or services, and customer, merchants, delivery partners or vendors lists (iii) any scientific or technical information, invention, design, process, procedure, formula, improvement, technology or method; (iv) any concepts, reports, data, know-how, works-in-progress, designs, development tools, specifications, computer software, source code, object code, flow charts, databases, inventions, information and trade secrets; and (v) any other information that should reasonably be recognized as confidential information of SWIGGY. Confidential Information shall further include all information, processes, formulas, codes, etc. which may be developed as a result of any information supplied by SWIGGY or as a result of any work performed on behalf of SWIGGY.

1.2. SCOPE

This policy shall apply to all users of Swiggy Ltd. (the ‘company’) information systems i.e.

- Employees
- Contractors
- Outsourced Employees
- Others (if any)

All security and safety of all portable technology, such as laptop, notepads, handheld devises will be the responsibility of the user. Each user is required to use log in credentials and to ensure the asset is always kept safely to protect the security of the asset issued to them. In the event of loss or damage, SWIGGY IT Security Team will assess the security measures undertaken to determine if the user will be required to reimburse SWIGGY for the loss or damage.

1.3. RESPONSIBILITIES

SWIGGY employees’ security practices identified in this Policy govern all areas of information security applicable to SWIGGY employee and cover the governance and management of security for its internal operations, as well as the services provided to SWIGGY (as an organization) by its suppliers and partners. All SWIGGY employees (Full Time, Part Time, Contractors, Third-Party Vendors and Franchise Vendors) are responsible for information security. As such, they must understand their roles and responsibilities in mitigating security risks, reporting or escalating such risks, and implementing protective measures that are appropriate to their job function and in a manner consistent with SWIGGY information security policies, standards, and procedures.

The IT Security policy sets the minimum level of responsibility for the following individuals and/or groups:

1.3.1. Information Security Team

- Create, manage, and maintain the security controls framework for all of SWIGGY's information and data.
- Report incidents, breaches and ensure suspected information security weaknesses are reported to executive management.
- Defines and regularly reviews access restrictions (per Access Management Policy document), classifications and safeguards for information and data, in accordance with Data Classification policy.

1.3.2. Security Ops Team

- Provide application support and resolving incidents / problems for IT Security related to the respective applications.

1.3.3. User(s)

- Secure and protect information and data to which they have authorized access.
- Report all incidents to Infosec team at infosec@SWIGGY.in
- Refer to the clause 3 in this document to be adhered to by the user.

1.3.4. Application Owner

- Owns the information and data within the assigned application.
- Provide application support, resolving the ticket and ensuring the application is operational.

1.3.5. Business Ops

- Implement the business process successfully and own the information and data within that process.

1.4. REFERENCE DOCUMENT

1.4.1. ISO/ IEC 27002: 2022
1.4.2. ISO/IEC 27701: 2019

1.5. DEFINITIONS

Integrated Management System (IMS)	The Integrated Management System is • Aligned to global standards for Information Security Management – ISO/IEC 27001:2022 • Aligned to global standards for Privacy Information Management – ISO/IEC 27701:2019

2 Protecting Swiggy's Confidential Information

Information and data created, modified, maintained, transmitted, retrieved, destroyed or archived by Swiggy team members are viewed as company assets. It is vitally important to Swiggy's reputation, operational stability and financial assurance that controls are in place to ensure the confidentiality, integrity and availability of information and data owned and controlled by SWIGGY employees. These controls will therefore protect the business processes supported and enabled by this information and data. SWIGGY employee's information and data may be stored or processed in a variety of systems, each system posing a unique security risk to Swiggy (as an organization).

Application Owners will determine the data classification based on type, value, risk impact and sensitivity of the information. System Owners, Business Process Owners, Application Owners and Information Security personals will then leverage these categories/ classifications to provide appropriate protection and control.

3 In-scope modules for Information Security

3.1. Information Security

3.1.1. Access Control

SWIGGY employees will ensure that its information and data is protected in a manner that minimizes the risk of unauthorized disclosure, modification, or destruction. Individuals not explicitly granted access to SWIGGY's Information Systems are prohibited from using such systems.

Access should be provided only to information and data that is required to perform the activities associated with a role at SWIGGY. Measures to prevent unauthorized access shall be implemented.

Application Owners must partner with Business Process Owners to maintain internal controls of access, including:

- Users must be assigned unique accounts and credentials in accordance with the SWIGGY's Access Management policy.
- Generic or shared accounts must be assigned in accordance with the SWIGGY's Access Management policy.
- Only authorized and trained SWIGGY personnel can make changes or install network components on SWIGGY's networks as per Change Management policy.
- Access to information Systems must be controlled (authorized access).
- Application Owners / respective Business Ops Manager / Reporting manager/ Authorized approvers as per approval matrix are responsible for authorizing access.
- Application Owners and Infosec Team must review users' access rights at regular intervals.
- Privileged accounts must be reviewed by Infosec team periodically.
- User access to SWIGGY's Information Systems and information processing facilities must be revoked upon termination of employment or contract or adjusted upon role change.
- Password sharing should not be encouraged.
- Users shall not misuse provided access privilege for any personal benefits.
- If in case, due to technical glitch someone gets privilege/elevated to access company sensitive data/application or information from the system, user shall raise the incident to InfoSec@Swiggy.in and should not use that information or data for any use.

Refer to SWIGGY's User Access Management Policy for a more detailed set of instructions.

3.1.2. Physical Asset Protection

SWIGGY's information and data must be physically and electronically secured and should not be left unattended without suitable protective measures in place. In case a user is travelling out of India with SWIGGY IT assets, an approval is mandatory to impose from the respective Manager and H Team..

3.1.3. Clear Desk and Clear Screen Policy

- Adequate controls shall be built to reduce the risk of unauthorized access, loss of, and damage to the information available in the form of paper, stored on computer, removable media, etc. during and after the normal working hours.
- All users shall keep information assets such as printouts, notepads containing customer / vendor data, etc. in a secured place when not in use, especially after working hours.
- Users shall protect the allocated computers and terminals with adequate controls (workstation locks, passwords, etc.) when not in use and shall log off / shut down when leaving the office.
- Users must inform Infosec Team at infosec@SWIGGY.in when he / she is moving out of the country to ensure that appropriate actions are taken and information is not left unattended.

3.1.4. Privacy and Data Protection

All users are responsible for protecting the confidential information, which is available in their possession, including personal data belonging to customers, contractors, suppliers, and any other confidential business information. Failure to protect personal data could lead to financial penalties, legal or regulatory fines, and damage to SWIGGY's reputation. Users shall keep their system backup always on Google drive to protect their information from sudden breakdown/ crash of their system.

When Restricted/Confidential information is no longer needed, it must be disposed of using standard destruction methods and in accordance with the local laws. If any SWIGGY employee suspects that restricted/confidential information is being misused, or a security incident may have occurred, he/she should immediately contact Infosec team at infosec@SWIGGY.in

3.2. Information Systems Management

Business Process Owners and System Owners must partner to ensure the following controls are in place for their SWIGGY Information Systems and corresponding information and data.

3.2.1. Computer and Network Installations

- All users must only connect SWIGGY approved devices to the corporate network.
- Network devices (e.g., routers, switches, firewalls) must be securely configured to prevent unauthorized access, intrusions, or modifications.

3.2.2. Anti-Virus and Operating System Security

- Users shall follow all antivirus awareness guidance from the IT Department promptly and completely,
- Users shall contact the IT department for all virus management specific queries,
- The antivirus and Operating System on the system shall be checked to have the latest update installed. In case of any discrepancy IT team should be immediately informed at infosec@SWIGGY.in.
- Adequate controls must be implemented to properly detect and defend the firm against malicious software designed to disrupt computer operations.

3.2.3. Data Encryption

- Users shall ensure the proper and effective use of encryption to protect the confidentiality, authenticity and integrity of SWIGGY’s information and data. The levels of encryption shall be based on the data classification and information security risks involved.

- Users shall ensure that data encryption is enabled for their system. In case of any discrepancy found, user can reach out to InfoSec@SWIGGY.in
- Business critical sensitive data should be identified based on data classification and confidentiality requirements and must be protected with use of encryption where appropriate (e.g. at rest, during transmission) and consider compliance with local laws. Refer to SWIGGY's Data Classification policy for a more detailed set of instructions.

3.2.4. System Monitoring and Logging

- SWIGGY's Information Systems must be assessed for vulnerabilities and malicious code, and the use of these systems must be logged, monitored, and reviewed for unauthorized access.
- Logging facilities and log information should be protected against tampering and unauthorized access.
- System administrator and system operator activities should be logged, protected and periodically reviewed.

3.2.5. Server Configuration

Server configurations and operating system core files must be secured and protected from unauthorized access and compromise.

3.2.6. Asset Management

System Owners must ensure timely and accurate updates for their assets, both hardware and software, are reflected within applicable Asset Management processes and systems. Refer to the IT Asset Management policy for a more detailed set of instructions.

3.2.7. Reporting Loss of Restricted/Confidential Information

If a SWIGGY user suspects that restricted/confidential information is being misused, or a security incident may have occurred, he/she should immediately report the incident to the Infosec team at infosec@SWIGGY.in

3.2.8. Segregation of duties

Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

3.2.9. Segregation in Networks

Groups of information services, users and information systems should be segregated on networks. Refer to Network Device Management Policy for a more detailed set of instructions.

3.2.10. Availability ((Information backup)

Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy. Refer to the Backup and Recovery Management policy for a more detailed set of instructions.

3.2.11. Information Security Continuity

- SWIGGY employees should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster (e.g. conducting Business Impact analysis).
- SWIGGY employees should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

- SWIGGY should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations (e.g. exercise and testing). Refer to the BCM policy for a more detailed set of instructions.

3.2.12. Theft or Loss of Hardware and Software/Data

In the event of theft or loss of IT equipment (hardware or software/data), user must report the incident in a timely manner to IT Support (it-support@swiggy.in) and Infosec team (InfoSec@Swiggy.in).

3.2.13. Unattended User Equipment

- Users shall be responsible for safeguarding the information assets installed in their areas.
- Active sessions shall be secured by an appropriate locking mechanism, such as locking the workstation, password protected screen saver, etc. In the absence of a locking mechanism, the active session shall be terminated after certain period of inactivity.
- Users shall log off from the terminals after the completion of session.
- Network printers shall be appropriately secured. Users shall ensure that any confidential information being printed on the printer is closely supervised and not left on the printers unattended. If required, the User shall use Secure Prints using secure passcode.

3.2.14. Password Management

Users having access to organizational computer systems must adhere to the Password Policy in addition to the following procedures:

- Users shall not disclose their user ID and password to anyone;
- Passwords must not be inserted into email messages or other forms of electronic communication;
- Always use a combination upper- and lower-case characters;
- Make your password easy for you to remember but hard for someone else to guess,
- Never write down your password; someone else might see it. Instead, commit it to memory;
- Users are responsible for the selection and maintenance of secure passwords adhering to SWIGGY password Management Policy;
- Users shall not enable auto logon options on the systems by saving the passwords. Refer to SWIGGY's Password Management policy for a more detailed set of instructions.

3.2.15. Internet, Applications and Computer Usage

The use of SWIGGY's electronic systems, including computers, Applications and all forms of Internet/intranet access, is for SWIGGY employee's business and for authorized purposes only. Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. Electronic communication should not be used to solicit or sell products or services that are unrelated to SWIGGY's business; distract, intimidate, or harass co-workers or third parties; or disrupt the workplace.

Use of SWIGGY computers, networks, Applications and Internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:

- Users shall use SWIGGY's Applications for business purposes only, and shall not use the applications for performing unauthorized or illegal acts;
- Assigned user accounts shall be used to work on the computing devices and the employees shall be held responsible for improper use of the assigned account;
- Users shall take reasonable steps to protect data and applications stored on their computing devices and Applications against unauthorized access;
- Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate SWIGGY business purposes;
- Engaging in private or personal business activities, including excessive use of instant messaging and chat rooms (see below);
- Accessing networks, servers, drives, folders, or files to which the employee has not been granted access or authorization from someone with the right to make such a grant;
- Making unauthorized copies of SWIGGY files or other SWIGGY data;

- Destroying, deleting, erasing, or concealing SWIGGY files or other SWIGGY data, or otherwise making such files or data unavailable or inaccessible to SWIGGY or to other authorized users of SWIGGY systems;
- Misrepresenting oneself or SWIGGY;
- Violating the laws & regulations and engaging in unlawful or malicious activities;
- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either SWIGGY's networks or systems or those of any other individual or entity;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- Sending, receiving, or accessing pornographic materials;
- Becoming involved in partisan politics;
- Causing congestion, disruption, disablement, alteration, or impairment of SWIGGY networks or systems;
- Maintaining, organizing, or participating in non-work-related Web logs ("blogs"), Web journals, "chat rooms", or private/personal/instant messaging;
- Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned, if you leave such computer or system unattended;
- Using recreational games; and/or
- Defeating or attempting to defeat security restrictions on SWIGGY systems and applications;
- Employees shall use SWIGGY Applications for business purposes only, and shall not use the Applications for performing unauthorized or illegal acts;
- Employees shall take reasonable steps to protect data & applications stored on their computing devices and Applications against unauthorized access;
- All internet access shall be processed through a content filter and only appropriate categories that are required for the business shall be allowed; content not related to business shall be blocked by the content filter;
- Users shall not introduce malicious programs into the network or server (e.g., viruses, worms, etc.);
- Users shall not execute any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is part of the employee's normal job/duty;
- Users shall not override user authentication or security of any host, network or account;
- Using SWIGGY electronic systems to access, create, view, transmit, or receive racist, obscene, sexist, threatening, or otherwise objectionable or illegal material, defined as any visual, textual, or auditory entity, file, or data, is strictly prohibited; such material violates SWIGGY policies and subjects the responsible employee to disciplinary action; SWIGGY's electronic mail system, Internet access, and computer systems must not be used to harm others; use of SWIGGY resources for illegal activity can lead to disciplinary action, up to and including dismissal and initiation of criminal prosecution;
- SWIGGY will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities, e-mail use, and/or computer use;
- Unless specifically granted in this policy, any non-business use of SWIGGY's electronic systems is expressly forbidden;
- If you violate these policies, you could be subject to disciplinary action, up to and including dismissal;

SWIGGY owns the rights to all data and files in any computer, network, or other information system used in SWIGGY and to all data and files sent or received using any SWIGGY system or using SWIGGY's access to any computer network, to the extent that such rights are not superseded by applicable laws relating to intellectual property; SWIGGY also reserves the right to monitor electronic mail messages (including personal/private/instant messaging systems) and their content, as well as any and all use by employees of the Internet and of computer equipment used to create, view, or access e-mail and Internet content; Employees must be aware that the electronic mail messages sent and received using SWIGGY equipment or SWIGGY-provided Internet access, including web-based messaging systems used with such systems or access, are not private and are subject to viewing, downloading, inspection, release, and archiving by SWIGGY officials at all times; SWIGGY has the right to inspect any and all files stored in private areas of the network or on individual computers or

storage media in order to assure compliance with SWIGGY policies and relevant laws; No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the employee or an appropriate SWIGGY official.

SWIGGY uses software in its electronic information systems that allows monitoring by authorized personnel and that creates and stores copies of any messages, files, or other information that is entered into, received by, sent, or viewed on such systems; There is no expectation of privacy in any information or activity conducted, sent, performed, or viewed on or with SWIGGY equipment or Internet access; Accordingly, employees should assume that whatever they do, type, enter, send, receive, and view on SWIGGY electronic information systems is electronically stored and subject to inspection, monitoring, evaluation, and SWIGGY use at any time; Further, employees who use SWIGGY systems and Internet access to send or receive files or other data that would otherwise be subject to any kind of confidentiality or disclosure privilege thereby waive whatever right they may have to assert such confidentiality or privilege from disclosure; Employees who wish to maintain their right to confidentiality or a disclosure privilege must send or receive such information using some means other than SWIGGY systems or SWIGGY-provided Internet access.

SWIGGY has licensed the use of certain commercial software application programs for business purposes; Third parties retain the ownership and distribution rights to such software; No employee may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software; Violation of this policy can lead to disciplinary action, up to and including dismissal.

3.2.16. Electronic mail

- Users shall not use internal and external E-mail systems to send confidential business or organization related information;
- Users shall not send chain letters, spam or unnecessary multiple forwarding such as holiday greetings.
- Users shall forward the virus alerts received to IT Support team at it-support@SWIGGY.in , infosec@SWIGGY.in
- Users shall not send any messages, regardless of their validity, that may cause damage or degrade anyone;
- All users of SWIGGY emailing system are responsible for appropriate use and proper dissemination of information;
- Communication outside organization shall be blocked for everyone and exceptions to be documented with timelines for the requirements which would be no more than 6 months.
- Domain whitelisting to be audited periodically to ensure unwanted domains are blocked in case missed from the user request

As noted above, electronic mail is always subjected to monitoring, and the release of specific information is subject to applicable laws and SWIGGY rules, policies, and procedures on confidentiality. Existing rules, policies, and procedures governing the sharing of confidential information also apply to the sharing of information via commercial software.

It is a violation of SWIGGY policy for any employee, including system administrators and supervisors, to access electronic mail and computer systems files to satisfy curiosity about the affairs of others, unless such access is directly related to that employee's job duties. Employees found to have engaged in such activities will be subject to disciplinary action.

3.2.16. IM Communication:

Employees and contractors of Swiggy Ltd. (whether on Swiggy payroll or the third party payroll, associated with Swiggy directly or indirectly) are prohibited from using non-approved instant messaging clients or applications for business communications.

Only approved and authorized applications/platforms shall be used for official communications. Failure to comply may result in serious disciplinary action.

Exceptions may be granted for matters specifically approved by management.

3.3. Electronic mail Tampering

Electronic mail messages received should not be altered without the sender's permission; nor should electronic mail be altered and forwarded to another user and/or unauthorized attachments be placed on another's electronic mail message.

3.3.1. Internet / Intranet Browser(s)

Electronic mail messages received should not be altered without the sender's permission; nor should electronic mail be altered and forwarded to another user and/or unauthorized attachments be placed on another's electronic mail message.
The Internet is to provide effective service of the highest quality to SWIGGY's customers and staff, and to support other direct job-related purposes. Managers should work with employees to determine the appropriateness of using the Internet for professional activities and career development. The various modes of Internet/Intranet access are SWIGGY resources and are provided as business tools to employees who may use them for research, professional development, and work-related communications. Limited personal use of Internet resources is a special exception to the general prohibition against the personal use of computer equipment and software.

Employees are individually liable for all damages incurred as a result of violating SWIGGY security policy, copyright, and licensing agreements.
All SWIGGY policies and procedures apply to all employees' conduct on the Internet, especially, but not exclusively, relating to intellectual property, confidentiality, SWIGGY information dissemination, standards of conduct, misuse of SWIGGY resources, anti-harassment, and information and data security.
Data and/ or programs should be downloaded from the Internet to SWIGGY network only under the following conditions:

- Downloaded data and programs should be checked for viruses using an approved methodology and tools before it is stored on the network;
- Data and/ or programs should be business-relevant and appropriate, and shall be acquired and used in compliance with all the legal requirements;
- Users shall not download / install any programs or software by themselves; They shall raise a ticket with necessary approvals and request the IT department to do so on their behalf;
- Downloaded programs or executable applications should be checked for suitability, compatibility, and security before they are installed on the network;

3.3.2. Legal use of Software

- In view of licensing concerns and the need for standard desktop configurations, no personal software/Licenses may be loaded on SWIGGY resources, unless expressly permitted by SWIGGY;
- The terms of all software licensing agreements and copyright laws should be abided by SWIGGY employees as applicable to them;
- Users should not make software available for others to use or copy in violation of the software's license agreement(s)/;
- Unlicensed and unauthorized software from any third party should not be accepted for installation and use at SWIGGY;
- Copyright materials are the Intellectual Property (IP) of their creators; Therefore, the posting, copying, redistribution or uploading of copyrighted material without the permission of the owner of such material is prohibited;
- If software media is delivered to the user, it may be used only on the computing resources for which the license was purchase;

- Installation of Pirated/Cracked/Illegal software/s on SWIGGY resources is expressly forbidden;
- Downloading and Installing torrents from illegal websites on SWIGGY assets or sharing such files on the network file servers are strictly forbidden;

3.3.3. Personal Electronic Equipment

- Users are not authorized to use personal devices for official usage, approval is to be obtained from Infosec team if personal devices are to be used for official usage.
- Due to the significant risk of harm to SWIGGY's electronic resources, or loss of data, from any unauthorized access that causes data loss or disruption, employees should not bring personal computers or data storage devices (such as floppy disks, CDs/DVDs, external hard drives, USB / flash drives, iPods/iPads/iTouch or similar devices, laptops or other mobile computing devices, or other data storage media) to the workplace and connect them to SWIGGY electronic systems unless expressly permitted to do so by SWIGGY;
- To minimize the risk of unauthorized copying of confidential SWIGGY business records and proprietary information that is not available to the general public, any employee connecting a personal computing device, data storage device, or image-recording device to SWIGGY networks or information systems thereby gives permission to SWIGGY to inspect the personal computer, data storage device, or image-recording device to SWIGGY networks or information systems thereby gives permission to SWIGGY to inspect the personal computer, data storage device, or image-recording device at any time with personnel and/or electronic resources of SWIGGY's choosing and to analyze any files, other data, or data storage devices or media that may be within or connectable to the data-storage device in question in order to ensure that confidential SWIGGY business records and proprietary information have not been taken without authorization.
- Employees who do not wish such inspections to be done on their personal computers, data storage devices, or imaging devices should not connect them to SWIGGY computers or networks;
- Violation of this policy, or failure to permit an inspection of any device under the circumstances covered by this policy, shall result in disciplinary action, up to and possibly including immediate termination of employment, depending upon the severity and repeat nature of the offense. In addition, the employee may face both civil and criminal liability from SWIGGY, from law enforcement officials, or from individuals whose rights are harmed by the violation.

3.3.4. Mobile Device Management

- Users shall take special care of the mobile computing resources, such as laptops, mobile phones, palmtops, etc.; to prevent the compromise of business information;
- Such resources shall not be left unattended at any time unless the information has been properly safeguarded;
- Users shall take special care while using the mobile computing resources in public places to protect the information from unauthorized access;
- Personal mobile devices can only be used for the email access, business internet access;
- Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away
- Mobile devices should be carried as hand luggage when traveling by aircraft;
- On Loss of mobile devices, immediately register a complaint with the jurisdictional police station and also inform to infosec@SWIGGY.in;

Each employee who utilizes personal mobile devices agrees and undertakes:

- Not to download or transfer data or sensitive information to the device. Not to use the mobile device as the sole repository for SWIGGY's information. All business information stored on mobile devices should be backed up.
- To make every reasonable effort to ensure that SWIGGY's data or information is not compromised using mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by or shown to unauthorized persons and all mobile devices should be password protected.
- Not to share the device with other individuals to protect the business data access through the device.
- To abide by SWIGGY's Internet, E-Mail, and IT Security policy, as applicable for appropriate use and access of internet sites etc.
- To notify SWIGGY immediately in the event of loss or theft of the registered device
- Not to connect USB memory sticks or external storage devices to the mobile phone to copy or transfer SWIGGY Data.
- Will delete all data held on the device upon changing the mobile phone or termination of the employee. The terminated employee can request personal data be reinstated from back up data.
- Has the right to deregister the device for business use at any time.

3.3.5. Printing, Copying and Scanning

- Documents must be printed only if it is necessary;
- Printed documents must be attended to immediately, i.e., they should be filed if required or shredded(disposed) if not required;
- IT department has all rights to get printing logs for unauthorized access or misuse of the printing facility;
- In the event that the printer has a fault and does not print the document, it is required that the print command be cancelled immediately; Under no circumstances should Confidential or Highly Confidential documents be printed unless the individual is present at the printer to receive the same;

3.3.6. Disclaimer and Signature format

All outgoing emails to external parties shall a have Signature and disclaimer inserted as follows; Refer to Annexure B for disclaimer and signature format;

4 Disciplinary action

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

5 Exception

SWIGGY reserves unconditional right to amend, abrogate, modify and / or rescind any of the provisions of this policy at any time; Exceptions to the policy will be handled on a case-to-case basis by the Management and HR Department.