Information Security Policy

Objective:

The purpose 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 any and 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.

Scope:

This policy shall apply to all users of Bundl Technologies Private Limited (the 'company' or 'Swiggy') 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 kept safely at all times 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.

Code of Conduct (Important):

- USERS SHALL NOT PRINT, COPY, DISCLOSE, SHARE OR PROVIDE DATA RELATED TO SWIGGY, OR ITS PARTNER RESTAURANTS, DELIVERY PARTNERS OR ITS CUSTOMERS TO ANY PERSON EITHER IN SOFT OR IN PRINT FORM, WHO DOES NOT HAVE ANY AUTHORIZATION TO ACCESS

- THE SAME. USERS SHALL NOT ENCRYPT THE DATA USING ANY TECHNOLOGY AND TRANSFER, COPY TO PERSONAL STORAGE DEVISE/S.
- USERS SHALL NOT ENCRYPT THE DATA USING TECHNOLOGY OR TRANSFER, COPY TO PERSONAL STORAGE DEVISE/S, TAKE PICTURE OF THE DATA USING ANY KIND OF ELECTRONIC DEVISE OR IMAGERECORDING DEVICE

- USER SHALL NOT TAKE PICTURE OF THE DATA FROM COMPUTER RESOURCE OR HARD COPY WHNE IN POSSESSION, USING ANY KIND OF ELECTRONIC DEVISE OR IMAGE-RECORDING DEVICE BY ANY MEANS. THIS RESTRICTION EXCLUDES TAKING SCREENSHOT FOR DAYTODAY BUSINESS REQUIREMENT AND SHARING ONLY AMONG OTHER SWIGGY USERS.

- USERS SHALL TAKE UTMOST CARE TO PROTECT SWIGGY INFORMATION, ASSETS AND SHALL ACTIVELY PARTICIPATE AND CONTRIBUTE TO THE INFORMATION SECURITY INITIATIVES TAKEN UP BY SWIGGY.

- USERS MUST RESPECT THE RIGHTS OF OTHER USERS, INCLUDING THEIR RIGHTS AS SET FORTH IN OTHER POLICIES; THESE RIGHTS INCLUDE BUT ARE NOT LIMITED TO PRIVACY, FREEDOM FROM HARASSMENT, AND FREEDOM OF EXPRESSION.

- USERS SHALL NOT SAVE ANY PERSONAL DOCUMENTS LIKE RESUMES, PICTURES, OR SONGS, MEDIA ETC ON THE NETWORK FILE SERVER. IF ANY SUCH PERSONAL DOCUMENTS ARE FOUND ON THE SERVER, THE CONCERNED USER SHALL BE LIABLE FOR DISCIPLINARY ACTION. ANY SUCH INFORMATION DISCOVERED MAY BE DELETED IMMEDIATELY WITHOUT ANY INFORMATION TO THE USER.

- THE CONTENT OF ANY DATA OR INFORMATION MADE AVAILABLE TO OTHERS VIA SWIGGY NETWORK IS THE SOLE RESPONSIBILITY OF THE USER WHO CREATED THAT INFORMATION.

- USERS SHALL NOT USE SWIGGY RESOURCES FOR THEIR PERSONAL WORK AND ARE RESPONSIBLE FOR FOLLOWING POLICIES AND PROCEDURES DEVELOPED BY SWIGGY FOR THE USE OF THESE FACILITIES.

- IN THE COURSE OF NORMAL DAY-TO-DAY OPERATIONS, USERS SHOULD BE AWARE THAT SWIGGY MAY ON A REGULAR BASIS AUDIT, MONITOR AND LOG DESKTOP ACTIVITIES, WITH OR WITHOUT NOTICE. IF A SITUATION WARRANTS IMMEDIATE OR FURTHER INVESTIGATION, SWIGGY SHALL CONDUCT INVESTIGATION AND INITIATE APPROPRIATE LEGAL ACTION AGAINST SUCH USERS.

Internet, E-Mail, Applications and Computer Usage:

The use of Swiggy's electronic systems, including computers, Applications and all forms of Internet/intranet access, is for Swiggy's business and for authorized purposes only. Brief and occasional personal use of the electronic mail system or the Internet is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense or harm to Swiggy or otherwise violate this policy.

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:

- 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;
- 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;
- 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.

Ownership and Access of Electronic Mail, Internet Access, and Computer Files; No Expectation of Privacy

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.

Electronic Mail

Users shall not use internal and external E-mail systems to send confidential business or organization related information without prior permission from the department manager

Users shall not send chain letters, spam or unnecessary multiple forwarding such as holiday greetings

Users shall not send the virus alerts received on email to anyone other than the it-support@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

As noted above, electronic mail is subject at all times 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.

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.

Policy Statement for Internet/Intranet Browser(s)

The Internet is to be used to further Swiggy's mission, 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 any and 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 and install any programs or software themselves. They shall 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

Personal Electronic Equipment

Swiggy prohibits the use in the workplace of any type of camera phone, cell phone camera, digital camera, video camera, or other form of recording device to record the image or other personal information of another person, if such use would constitute a violation of a civil or criminal statute that protects the person's right to be free from harassment or from invasion of the person's right to privacy.

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 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.

Password Management

- 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- & 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,
- Users having access to organizational computer systems must adhere to the Swiggy Password Policy Click here to view Swiggy IT Password Policy.

Disclaimer and Signature format

All outgoing emails to external parties shall a have Signature and disclaimer inserted as follows:

- Employee Full Name
- Designation with Department
- Office address with landline and official mobile number

Disclaimer format

"This e-mail, including any attachments, may contain confidential information and is intended only for the addressee(s) named above. If you are not the intended recipient(s), you should not disseminate, distribute, or copy this e-mail. Please notify the sender by reply e-mail immediately if you have received this e-mail in error and permanently delete all copies of the original message from your system. E-mail transmission cannot be guaranteed to be secure as it could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. Company accepts no liability for any damage or loss of confidential information caused by this email or due to any virus transmitted by this email or otherwise."

Logical Access Practices

Logical Access Practice shall follow the Swiggy Logical Access policy, Click here to view Access Control Policy

Antivirus & 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 intimated.

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 purchased
- No programs that could result in damage to a file or computer system and/ or the reproduction of it may be loaded on Swiggy computing resources
- 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.

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 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

Mobile Resources

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
- Users shall be responsible for backing up the project related data on a regular basis from the mobile computing devices to the network file servers
- Personal mobile devices can only be used for the email access, business internet access.

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 through the use of 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 Computer Usage 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.

Keeping mobile devices secure

The following must be observed when handling mobile computing devices (such as notebooks and iPads):

- 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.

Printing Coping & Scanning:

- Documents must be printed only if it is absolutely 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.

Clear desk and clear screen

- 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.

- Employees shall keep information assets like printouts of client deliverables, notepads containing client data, etc. in a secured place when not in use, especially after working hours.

- Users shall protect the personal computers and terminals with adequate controls (workstation locks, passwords, etc.) when not in use and shall log off / shut down when leaving the office.

Disciplinary Action

Swiggy has the right to ensure that IT equipment is used properly and in accordance with this Policy terms. Accordingly, to the extent allowed by applicable law, Swiggy may monitor any and all use of its equipment at any and all times, as determined within its sole discretion. This includes monitoring or recording telephonic conversations or any electronic communication. Swiggy may take other steps to protect its equipment, such as build exception reports to flag potential misuse of equipment, such as mobile phones, as well as access, copy, use, modify or disclose any information obtained from monitoring or recording. Personal use of Swiggy equipment is also subject to such monitoring and recording, and even deleted items may be retrieved. Swiggy equipment should never be used for any messages or materials that a user may wish to keep personally private. There cannot be any expectation of privacy when using any Swiggy equipment at any time.

All the users should report any observed (or suspected) security weaknesses in IT systems or services to the IT department. Serious security incidents should be informed to IT Helpdesk. Such activities include, but are not limited to the following:

- Violation of Information Security Policies

- Breach of confidentiality/ access control
- Software malfunction
- Virus activity
- SPAM / JUNK mails in Emails services
- Non-Production data communication through mails, File transfer
- System failure
- Degradation of the information processing services

USERS SHALL STRICTLY ADHERE TO THESE POLICIES AND IF FOUND VIOLATING THE SAME, MAY HAVE THEIR PRIVILEGES, SUCH AS USER ACCOUNTS ACCESS, REVOKED WITHOUT NOTICE WHEN IT IS DEEMED NECESSARY FOR THE SECURITY OF SWIGGY'S COMPUTING RESOURCES, WHILE SWIGGY DECIDE ON THE DISCIPLINARY ACTION INCLUDING TERMINATION OF EMPLOYMENT.

SWIGGY SHALL ALSO RESERVE THE RIGHT TO INITIATE APPROPRIATE LEGAL ACTION INCLUDING CRIMINAL PROSECUTION UNDER APPROPRIATE PROVISIONS OF INFORMATION TECHNOLOGY ACT, 2006 AND INDIAN PENAL CODE, 1860. SWIGGY SHALL RESERVE ITS RIGHT TO INITIATE CIVIL PROCEEDINGS AS WELL FOR RECOVERY OF DAMAGES AGAINST SUCH USERS.

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.

Version: 2.5

Updated on: June 2022

Revision History:

V.No	Version Date	Effective from	Prepared by	Reviewed by	Approved by
2.5	09th June 2022	11th June 2022	Compliance Department	Legal & IT Department	Rajeev Kumar (AVP IT & InfoSec)
2.4	10th June 2021	11th June 2021	Compliance Department	Legal & IT Department	Rajeev Kumar (AVP IT & InfoSec)
2.3	10th June 2020	11th June 2020	Compliance Department	Legal & IT Department	Rajeev Kumar (Head of InfoSec)
2.1	11th June 2019	14th June 2019	Legal & IT Department	Rajeev Kumar (IT Director)	Rahul Jaimini (CTO)
2.0	12th June 2018	14th June 2018	Legal & IT Department	Rajeev Kumar (IT Sr Manager)	Rahul Jaimini (CTO)
1.1	12th June 2017	14th June 2017	Legal & IT Department	Darshan KB (IT Manager)	Rahul Jaimini (CTO)
1.0	10th March 2016	11th March 2016	HR Department	Darshan KB (IT Manager)	Rahul Jaimini (CTO)