zomato

INFORMATION SECURITY POLICY

Table of Contents

1. OBJECTIVE

The purpose of this Information Security Policy ("**Policy**") is to protect Zomato's information resources from accidental or intentional unauthorized access, modification, or damage, either via internal or external threats by enforcing appropriate controls. The Policy supports the overall objective of Zomato to protect the Confidentiality, Integrity and Availability (CIA) of the Information systems, Information Assets and the Information.

2. SCOPE

This Policy applies to all Zomato office locations and users worldwide, including employees. Within the scope of applicability of this policy all the assets/resources such as, but not limited to, information systems, hardware, software, data, media, and paper files at Zomato and approved third-party facilities are covered.

3. RESPONSIBILITY

The Information Security team shall be primarily responsible for ensuring adherence to this Policy.

4. DEFINITIONS

- **Information:** Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual
- **Information Systems**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information
- **Information Assets:** Data or other knowledge that has value to an organization
- **Information Security**: Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide Confidentiality, Integrity and Availability.
- **Risk**: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
- **Confidentiality:** Confidentiality means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information
- **Integrity**: Integrity means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity
- **Availability**: Availability means ensuring timely and reliable access to and use of information
- **Functional requirements**: Functional requirements specify the functioning of the systems when certain conditions are met
- **Incident**: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
- **Mobile Device**: A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smartphones, tablets, and E-readers.

5. POLICY DESCRIPTION

a) Asset Management

Assets associated with Zomato's information, information systems and information processing facilities shall be identified and documented. Asset management shall indicate the ownership and importance which shall be used and protected in accordance with their importance to Zomato. Refer 'IT Asset Management Process' for further details.

b) User Access Management

Access to Zomato's information, information systems (Infrastructure, applications, source code repositories) and information processing facilities shall be controlled to prevent unauthorized access. Only authorized individuals shall be granted access to the information systems and those individuals' accountability shall be assured. Access to information on systems and applications should be based on well-defined user roles in the application/platform. Team responsible to manage the platform needs to ensure strict adherence to the Logical Access Management Process. There will be clear delegation of authority for the right to upgrade/change user profiles and permissions, and also key business parameters which should be documented. Privileges are allocated on a need-to-use and event-by-event basis; the request for allocation of a privilege is initiated from the user concerned to the platform owner which reviews the reasons for higher privileges. Strong password policy shall be implemented for system login. Refer 'User Access Management Process' for further details.

c) Change Management

Changes to applications and infrastructure systems shall be performed through defined processes and requisite approvals to ensure security during change management activities. Only approved, tested and authorized changes shall be made to the applications, infrastructure and systems. Changes shall be reviewed periodically by the respective department head to ascertain whether appropriate change management processes were followed or not. Refer 'Change Management Process' for further details.

d) Mobile devices and Teleworking

Zomato shall establish secure procedures for safeguarding and preventing leakage of information through laptops, mobile devices etc. The policies shall enable safe and secure access to the ecosystem by identifying various guidelines for remote access and by defining various controls for the usage of the devices pertaining to both the policy scenarios. Refer 'Remote Working Policy' for further details.

e) Network Security

The network infrastructure of Zomato shall be secured to protect information from unauthorized access and enable effective usage of various networking, communications, and computing facilities. Refer 'Network Security Policy' for further details.

f) System Acquisition, Development and Maintenance

Zomato shall ensure that adequate controls are deployed in the software development process to address risks in meeting functional and information security requirements. Refer 'Software Development Lifecycle Process' for further details.

g) Third Party Risk Management

Zomato shall require all third parties who have access to Zomato's information/ information assets to adhere to Zomato's Third Party Risk Management process. Third party's access to Zomato's information/ information assets shall be restricted. Refer 'Third Party Risk Management process' for further details.

h) Incident Management

- **Management of information security incidents** - An event will be an incident when it is analyzed and classified to be adverse by the incident response team. An incident response plan is expected to be defined and implemented that denotes the roles and responsibilities (and contact information) of key leaders tasked with managing data incidents broadly, and security incidents specifically. At a minimum, it is expected that businesses should be able to restore their operations and have plans for incident and crisis management.

- **Reporting IT information security Events and Weaknesses** - Zomato shall implement procedures for detecting & reporting incidents and responding to incidents related to exceptional situations in day-to-day administration of the IT and information security related areas. The incidents shall be reported in time to the appropriate regulatory authorities and corrective actions shall be taken immediately to avoid the recurrence of such events in future. All reported incidents shall be logged, analyzed and classified according to predefined criteria. Escalations and actions shall be as per the classification of incidents.

- **Reporting Non-IT information security incidents** - An Incident is an occurrence of any exceptional situation that could compromise the Confidentiality, Integrity or Availability of Information of Zomato. It is related to exceptional situations or a situation that warrants intervention of senior management, which has the potential to cause injury or significant property damage;

All events shall be reported in a timely manner as per procedures for event reporting and corrective actions shall be taken immediately as per procedures to avoid the recurrence of such events in future. Refer 'Information Security Incident Management Process' for further details.

i) Information Security for Operational Management

- **Protection from malware** - All servers, desktops, workstations, handheld devices, gateways and any other access points to Zomato network shall be protected against malicious code. Information security team is responsible for updating and scanning of these systems and taking necessary actions on the infected systems. Action taken on infected systems would be logged in Antivirus Reports on a regular basis. Refer to 'Malware Protection Process' for detail.

- **Logging and Monitoring** - User activities, exceptions, and security events shall be logged and monitored the activities of users with high levels of access (privileged users such as system administrators and system operators) shall be logged and independently reviewed on a requirement basis. The audit logs shall be retained based on the record retention requirements. Log information shall be protected against unauthorized access, alterations and operational problems. Access to logs shall be provided on 'need-to-know' and 'need-to-have' basis. Refer to 'Logs Management Process' for details.

- **Control of operational software** - Users shall only use authorized software and unauthorized installation of software shall be restricted. The access to install software on operational systems shall be restricted to authorized personnel only. All upgrades and applications of service packs shall be carried out after appropriate testing and evaluating the additional security measures provided by the vendor. In case of any exceptions due to technical limitations, approval shall be taken from the Information security team for acceptance of tests conducted by the vendor.

j) Business Continuity

Zomato shall plan for and implement the controls to mitigate the impact of disaster and timely resumption of business activities and information security.

- Zomato shall provide direction and support for business continuity
- Set the organizational requirements and expectations for business continuity
- Guide the implementation of appropriate policies, standards, processes, procedures, plans and controls necessary to recover functions within Zomato
- Define the roles and responsibilities of employees towards business continuity
- Perform annual mock drills of the business function to keep the Business Continuity measures up to date

k) BCP & DR

BCP & DR forms a significant part of Zomato's overall business continuity management plan, which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes. DR shall be designed to minimize the operational, financial, legal, reputational and other material consequences arising from a disaster. BCP & DR Technical plans with documentation shall be prepared by platform owners in consultation with Information Security team to ensure that maximum possible service levels are maintained during unexpected events so that departments and critical operations recover from interruptions as quickly as possible and identify mitigation strategies for minimum interruptions with clearly defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

l) Backup Management

Backup copies of information are essential to recover and restore original data in the event of data loss. Data which has been backed up should be secured from unauthorized access, should be available when required and its restoration should be tested periodically to ensure its validity. A backup schedule providing the details and frequency shall be prepared to ensure that business requirements are addressed including the retention period of backup. Backup records (including backup software logs) shall be kept up-to-date when the backup process starts and ends. Backup software logs shall be monitored and they shall also be stored securely for possible future reference. Monitoring of backup shall be performed by authorized personnel on a periodic basis. Restoration testing of backed up data shall be performed on a periodic basis based on the criticality of data to ensure that organization's data availability requirements can be met. Refer to "Backup Management Process" for details

m) Information Security Awareness Program

Zomato shall implement a formal security awareness program to:

- Make all employees aware of the importance of Information Security and Data Privacy
- Encourage employees to understand the importance of information security and data privacy risks and procedures in place to mitigate such risks
- Educate employees upon hire and at least annually (for example, by emails, posters, memos, meetings, and promotions).

The Security awareness training should be made as an annual mandatory program for all the employees to be compliant with HR policies. The training material related to information security and information technology shall be periodically reviewed by the security team.

n) Compliance

Zomato shall comply with relevant laws, regulations, industry standards and contractual agreements which may impact its business and information security activities. Zomato's processes and infrastructure are certified with ISO 27001: 2013 standard. Refer 'Compliance Management Policy' for further details.

o) Review mechanisms

Zomato has established several review mechanisms for monitoring and responding to data breaches and cyberattacks such as:

- Vulnerability Assessment and Penetration Testing (VAPT), internally and externally on an annual basis
- Performing internal and external audits, periodically

p) Information Security Governance team

Zomato has established the Information Security Governance team with representatives from cross-functional teams including Technology, Security and GRC (Governance, Risk and Compliance) teams.The Board of Directors oversees the Information Security Governance team and has approved the Information Security Policy.

Key responsibilities of the Information Security Governance team include:

- Align Information Security with business objectives
- Provide IT governance and Organisational structure that constantly works to improve Data Protection
- Define and implement Information Security Frameworks and Tools

- Assess and monitor Information Security Risks
- Monitor Information Risk incidents
- Security compliance management
- Drive firm-wide training and communications on Information Security
- Providing insights and recommendations on Information Security Risk Management to the executive team
- GRC communicates the updates to the Audit Committee on a periodic basis.

Quarterly meetings are conducted to review and discuss the Information Security strategy. In addition, the Information Security team interacts on a case basis to discuss the security risks, incident response, implementation status, etc.

6. EXCEPTION MANAGEMENT

All exceptions to this Policy will be directed to the Information Security team. The Information Security team shall ensure that the exception request is formally recorded (in the exception management form) with substitute controls which will be put in place. The exception will be reviewed by the Information Security team and they will take a decision to formally approve/reject the exception request. The validity of the exception shall be defined and shall not exceed one year. An annual review of all accepted exceptions shall be carried out by the Information Security team to identify any changes to the risk posed by the exception or to identify any alternate controls that may be implemented to reduce the risk.

7. COMPLYING TO THE POLICY

All employees shall comply with this Policy. Any employee found to be abusing the privilege of Zomato's access to business systems, or not in compliance with any of these policies, may be subject to disciplinary action, up to and including termination of employment. Any such disciplinary action shall only be taken to the extent permissible by local law. Federal, state, and/or local law enforcement agencies may also be notified if evidence of criminal actions exists. All employees are to check security and compliance obligations mentioned in contracts and/or master services agreements with their respective managers (or business process equivalent) to ensure that they adhere to those security and compliance commitments agreed with the customer.

Employees are encouraged to consult with the Technology and Security team to seek clarification on any queries they may have pertaining to Information Security. Moreover, if employees notice any suspicious activities which breaches the Information Security Policy, they are encouraged to report it to the Technology and Security team in order to minimize the impact and exposure on Zomato.

8. DOCUMENT REVIEW AND CONTROL

The Policy will continue to be in force unless superseded by a fresh policy. This Policy will continue to be in force unless superseded by a fresh policy. Zomato management reserves the right to amend, abrogate, modify, rescind / reinstate the entire Policy or any part of it at any time. This Policy will be reviewed at least once in a year or in case of any significant changes

9. REFERENCES

- Remote Working Policy
- IT Asset Management Process
- Logical Access Management Process
- Change Management Process
- Log management Process
- Backup Process
- Secure development lifecycle process
- Third party cyber risk management process
- Incident Management process
- Malware Protection Process
- Compliance Management Policy

- Network Security Policy

10. DISCLOSURES

This Policy shall be disclosed on the website of the Company.

11. CONFLICT OF POLICY

In the event of any conflict between this Policy and the provisions contained in the Applicable Laws, the provisions of Applicable Laws shall prevail.

12. AMENDMENT

Any change in this Policy shall be approved by the Information Security Team. The Technology and Security Team shall have the right to withdraw and/or amend any part of this Policy or the entire Policy, at any time, as it deems fit, or from time to time, and the decision of the Board in this respect shall be final and binding.

13. COMPLIANCE

The Information Security Governance team is responsible for implementing this Policy.

Any queries regarding this Policy shall be referred to the Information Security Governance team at security@zomato.com, who is in charge of administering, enforcing and updating this Policy.

14. INTERPRETATION

In any circumstance where the terms of this Policy are inconsistent with any existing or newly enacted law, rule, regulation or standard governing the Company, the said law, rule, regulation or standard will take precedence over this Policy.

15. VERSION HISTORY

Version	**Approved in**	**Description**
Version 1	December, 2021	Original Policy
Version 2	November, 2022	Addition of section on Information Security Governance team
Version 3	May 2023	No change
Version 4	May 2024	Addition of review mechanism para,other minor changes in line with best practices