Tirupati

Tirupati Group

(Tirupati Medicare Limited, Tirupati Lifesciences Private Limited, Tirupati Wellness Private Limited & Newtramax Healthcare Private Limited)

Information Security Policy

Policy Number: TG/P/ITD/001-00

Authored By	Reviewed By	Approved By	Version	W.E.F.
Nasim Akram Deputy Manager- IT	Nipun Dang General Manager - IT	Ashok Goyal CEO	1.0	1st February 2024
				

Information Security Policy

Introduction

At Tirupati Group, we prioritize the protection of critical information pertaining to our organization, employees, customers, and stakeholders. We remain vigilant against all potential threats, whether they arise from internal sources or external factors, and whether they are deliberate or accidental in nature.

Our Commitment

Tirupati Group holds the privacy and security of information concerning individuals, organizations, and stakeholders in high regard. We are dedicated to implementing reasonable measures to safeguard this information, including sensitive and critical data. Our company adheres to all applicable legal, regulatory, and contractual obligations regarding data privacy. We have established comprehensive information security controls to uphold the protection and privacy of information within our organization.

Scope

This policy lays down the governance structure for information security and risk management, outlines mechanisms for monitoring and processing data stored in the company's database and establishes procedures for addressing breaches.

Applicable to Tirupati Group and its subsidiaries, this policy extends to individuals or organizations accessing or providing Personal Data to the company. This encompasses the Board, employees, shareholders, customers, suppliers, statutory authorities, local communities, and service providers. Irrespective of the mode or location of data recording, breach protocols are uniformly enforced.

Objectives

Aligned with applicable laws and milestones, our objectives ensure the responsible handling of information:

- All forms of information, whether electronic or physical, will be exchanged ethically and transparently, with consent sought from information providers.
- Information will be reliable and processed only for lawful purposes, distinguishing between general and personal/sensitive data, with the latter requiring explicit stakeholder consent.
- **Access Control:** Establish strong role-based access control systems in internally to maintain the confidentiality of the documents.
- **Records retention:** Sensitive Information will be retained in the systems for as long as it is required. Once the legitimate purpose for retaining such information has been served, it shall be erased from the company database.
- **Disclosures:** Adequate safety measures will be in place while transferring information to third-parties or external associations under contracts.

- Robust security controls will be implemented to safeguard against breaches or leaks, data loss and data theft, minimizing the risk of compromising stakeholder security.
- Confidential Information will be restricted to relevant departments internally, and when shared externally, non-disclosure agreements will be executed to mitigate breach risks.
- Regular training and awareness programs will be conducted to instill confidence among employees and stakeholders, ensuring adherence to relevant information security regulations.
- Employees will also receive basic technical training to take timely remedial steps in case an information breach occurs.

Targets & Actions:

To actualize our objectives, we have set the following targets:

Targets

To achieve these objectives, the following target actions are defined:

- Implement robust access control measures to restrict unauthorized access to IT systems and data.
- Deploy comprehensive cybersecurity solutions, including firewalls, Endpoint Security, Email Security, and intrusion detection systems, to detect and prevent cyber threats.
- Conduct regular audits and risk assessments to identify vulnerabilities and gaps in IT security controls.
- Provide ongoing training and awareness programs to educate employees about IT security best practices and policies.

Actions

Data Security: The company takes data security seriously and is committed to protecting confidential information. Employees must:

- Use strong passwords and keep them confidential.
- Change password at regular intervals.
- Use multi-factor authentication.
- Report any suspected data breaches or security incidents immediately.
- Not allowed storing sensitive data on personal devices

Privacy: The company respects the privacy of its employees and customers. Employees must:

- Respect the privacy of others and avoid collecting or using personal information without authorization.
- Only access data necessary for their job duties
- Comply with all applicable privacy laws and regulations.

Prohibited Use: The following uses are strictly prohibited:

- Installing or using unauthorized software.
- Accessing or sharing confidential information without authorization.
- Downloading or copying copyrighted material without permission.
- Engaging in illegal or unethical activities.
- Sending or receiving offensive or discriminatory content.
- Using unauthorized Portable Media. (e.g. Pen drive etc.)
- Wasting company resources.
- Engaging in any activity that could compromise the security or integrity of IT resources.

Do's & Don'ts: General Do's & Don'ts to be followed by all stakeholders.

- **Do's**

- Be accountable for your IT assets and data.
- Adhere to Policies on Use of IT Services and Resources.
- Use good judgment to protect your data.
- Always keep important data in a secure path/ folder.
- Protect your laptop during the trip.
- Ensure sensitive information on the computer screen is not visible to others.
- Protect your user ID and password.
- Do lock your computer/laptop when not in use.
- Physically secure your laptop /Desktop.
- Lock the Computer system before leaving your work desk.
- Always shut down your computer system properly before leaving the office.
- Always follow password policy for creating passwords to avoid risks involved.
- Do use hard-to-guess passwords or passphrases.
- Do change passwords at regular intervals.
- Do use different passwords for different accounts.
- Do keep your passwords or passphrases confidential.
- Be careful while entering a password when someone is sitting beside you.
- Do check the URL before clicking any link sent via email.
- Do report all suspicious activity and cyber incidents to the IT Department.

- Official E-mail accounts should be used for official purposes only.
- Official E-mail should not be forwarded to a personal E-mail account.
- Do remember that wireless is inherently insecure. Avoid using public Wi-Fi hotspots.
- Do lock printouts containing sensitive information in a drawer to reduce the risk of unauthorized disclosure.
- Do be aware of your surroundings when printing or faxing sensitive information.
- Do pick up information from printers, copiers, or faxes in a timely manner.

  - **Don'ts**

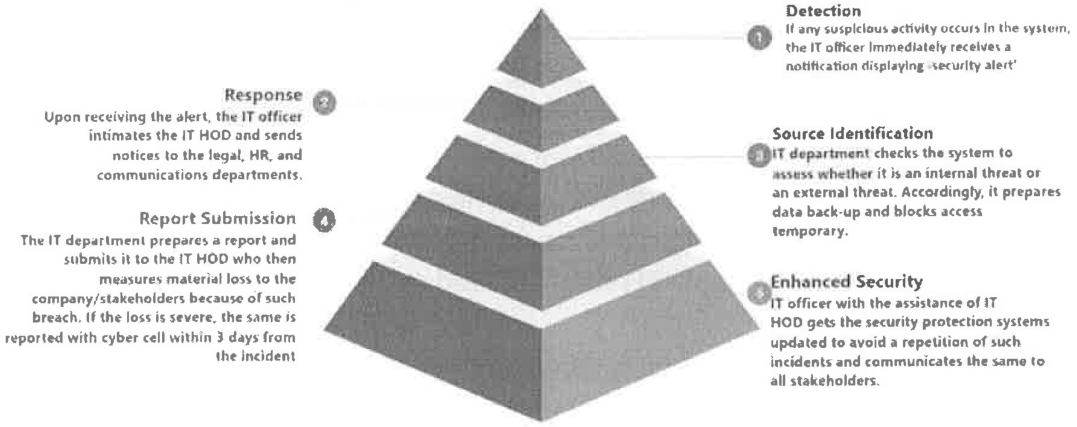
- Don't leave your computer / sensitive documents unlocked.
- Don't discuss something sensitive in public places. People around you may be listening to your conversation.
- Don't leave devices unattended.
- Don't share company electronic data through any channel, such as email, Pen drive, share drive without any authorization/permission.
- Don't share passwords with anyone or write them down.
- Don't use a password that was used earlier.
- Don't use the name of things located around you as passwords for your account.
- Don't respond to emails received from strangers.
- Don't click on links from an unknown or untrusted source.
- Don't share company electronic data via email Pen drive, share drive without any Authorization/Permission.
- Don't use an unauthorized and unprotected computer system.
- Never write down your password in the notebook and do not stick the written password on the Desktop/ Laptop.
- Do not leave your laptop unattended, even for a few minutes.
- Never reply to email(s) requesting financial or confidential information without verifying.
- Avoid opening e-mail(s) or e-mail attachments from an unknown sender.
- Don't leave printouts or portable media containing private information on your desk.
- Don't power off your computer system directly from the power button.
- Don't transfer/move computer systems without IT Admin knowledge and Permission.

Incident Response Procedure:

In the event of security breaches or data vulnerabilities, Tirupati Group employs a structured escalation process to swiftly address and mitigate risks, ensuring the integrity and confidentiality of sensitive information.

In case of any security breach, write to the below email address and contact your IT department.

- Tirupati Medicare: itcare@tirupatimedicare.com
- Tirupati Wellness: itcare@tirupatiwellness.in
- Tirupati Lifesciences: itcare@tirupatilifesciences.com



Collaboration and Engagement:

Effective communication with both internal and external stakeholders is integral to upholding our information security standards:

- The policy shall be readily accessible on Tirupati Group's website, ensuring transparency and visibility to all stakeholders.
- Our department heads shall disseminate the policy to relevant stakeholders, facilitating awareness and understanding across the organization and its external partners.

Implementation and Accountability:

a. This policy applies to all employees, management, and contractors of the Tirupati Group.
b. The management is responsible for implementing this policy.
c. Business Unit Leads will be held accountable for the associated performance of the policy.
d. IT heads/Designee will take the lead in all training and monitoring-related activities.

Allied policies and procedures:

Below is a list of relevant policies and SOPs that have already been put in place by Tirupati Group. These shall be seen as additional documents to supplement this Information Security policy:

- Data Integrity Policy
- IT SOP's
- IT Dos and Don'ts

Monitoring and Compliance:

a. We will measure and report on performance annually effectiveness of IT controls to ensure ongoing compliance with this policy.
b. The IT HOD will review this policy annually and recommend necessary revisions to reflect changes in technology, regulations, and company practices.

By adhering to these guiding principles, we aim to provide a safe & secure IT environment & resources within our organization.