

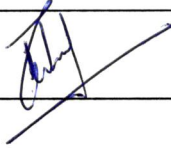
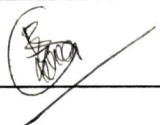
Policy name- IT and data security policy

Version number – SIL/2025/08.001

Approval Date - 15/10/2025

With Effective From – 01/11/2025

Revision Date – 02/05/2026

Maker	Checker	Approval L1
Subrahmanya Gupta Boda VP-IT	Rahul K Director - Finance	Giridhar Kumar COO
		

IT AND DATA SECURITY POLICY

1. PURPOSE

The purpose of this policy is to establish a framework for protecting Sumadhura's information technology assets and data resources. It outlines the responsibilities, acceptable usage, and security protocols necessary to ensure confidentiality, integrity, and availability of organizational data and systems.

2. SCOPE

This policy applies to all employees, contractors, consultants, interns, and third-party service providers who access or use Sumadhura's IT infrastructure, systems, applications, or data.

3. APPLICABILITY

The policy is applicable across all departments and locations of Sumadhura Infracon Pvt Ltd. It governs the use of hardware, software, networks, cloud services, and data handling practices.

4. RESPONSIBILITY AND MANAGEMENT

The IT Department is responsible for implementing and maintaining security controls, monitoring systems, and responding to incidents. The HCM Department ensures employees are informed of this policy during onboarding and exit processes. All employees are responsible for adhering to the guidelines and reporting any suspicious activity or breaches.

5. ACCEPTABLE USE

Company-provided IT resources must be used solely for business purposes. Personal use of devices and the internet such as use of office assets during office time for trading, gaming use of social media is strictly prohibited and must not interfere with work responsibilities. Sharing of login credentials or access rights is not permitted under any circumstances.

5. Software Asset / Subscription Management

Installation of unauthorized software or hardware is strictly prohibited.

Employees **must only** use company-approved softwares and/or Cloud Apps for storing, processing, or transmitting Company Data. Users may request for entitled software through it.support@sumadhuragroup.com

Prior approval from appropriate authority for requesting installation of licensed software or provision of access to subscription based software or entitled software is mandatory.

Any software services or SaaS software subscribed for company purposes shall be procured through company email id. Any subscriptions or SaaS software subscribed through credit cards issued by company or reimbursed shall be declared to the IT Department for maintaining compliances.

Any request to use a new Cloud App must be submitted to the IT Department through the official service portal for a security and compliance review.

The review process will assess the application's data security controls, privacy policy, compliance certifications (e.g., SOC 2, ISO 27001), and business necessity.

No employee may sign up for or use a new Cloud App for business purposes until it has received formal written approval from the IT Department.

Access to Cloud Apps shall be granted based on the principle of least privilege, ensuring users only have the access rights necessary to perform their job functions.

6. DATA PROTECTION

All sensitive and confidential data must be stored securely and accessed only by authorized personnel. Data must be encrypted during transmission and storage where applicable. Employees must not copy, transfer, or disclose company data to external parties without prior approval.

Users are responsible for understanding the classification level of the data they handle (e.g., Public, Internal, Confidential, Restricted, PII).

SUMADHURA INFRACON PRIVATE LIMITED

Uploading or storing Personally Identifiable Information (PII) [Customer Related], Protected Health Information (PHI) [Employee related], or other regulated data into unapproved Cloud Apps is strictly prohibited.

Restricted or Confidential Company Data may only be stored in Cloud Apps and local storage specifically approved by IT for that level of data sensitivity.

Downloading Company Data from approved Cloud Apps to personal or non-company devices is forbidden unless explicitly authorized by management and any such authorization may be submitted to IT.

7. PASSWORD AND ACCESS CONTROL

Passwords must be complex, changed periodically, and kept confidential. Access to systems and data will be granted based on role and business need.

- Password length - Minimum 8 Characters
- Password composition - Alpha Numeric and Special Charters
- Password management - Passwords not to be stored in documents / books / papers etc.
- Multi-factor authentication - Wherever available must use multi-factor for critical systems
- Frequency of password changes - 90 Days (Normal Systems) / 45 Days (Systems with Sensitive Data)

8. INCIDENT REPORTING

Any suspected data breach, unauthorized access, or IT security incident must be reported immediately to the IT Helpdesk at it.support@sumadhuragroup.com. The IT team will investigate and take appropriate corrective actions.

9. DEVICE AND NETWORK SECURITY

Employees shall be allocated a desktop/laptop as per Resource allocation sheet received from the HR department. Laptops and Desktops shall be procured as per approved standard. Any deviation shall be approved by Directors of respective departments.

Only one IT Asset shall be provisioned per employee and any additional shall be provisioned post procurement with approval of Directors of respective departments

As a one-time measure, Any additional assets with employees shall be duly returned to the IT department before 30th Oct 2025.

All company devices must have updated antivirus and security patches.

Only approved devices shall be allowed to connect to the corporate network.

SUMADHURA INFRACON PRIVATE LIMITED

Use of public Wi-Fi for accessing company systems is discouraged. USB drives and external devices are by default blocked from usage. When they must be used, they must be scanned for malware before use. VPN Shall be used to connect to sensitive systems from outside company network.

The network shall be built to provide seamless connectivity across the Sumadhura offices, Project sites, Customer Experience Centers and any other relevant sites using homogeneous networking standards to provide foundation and security.

10. EXIT PROCEDURE

Upon separation, employees must return all IT assets to IT Department and ensure deletion of company data from personal devices. Access rights will be revoked immediately upon exit notification. A no-dues clearance from the IT department is mandatory for final settlement. In case the department head determines that an IT asset is needed for a specific purpose and duration, it may be reissued to the head of department as a temporary issue of asset.

11. VIOLATIONS AND CONSEQUENCES

Non-compliance with this policy may result in disciplinary action, including termination of employment. Legal action may be initiated in cases of data theft, breach of confidentiality, or damage to IT infrastructure.

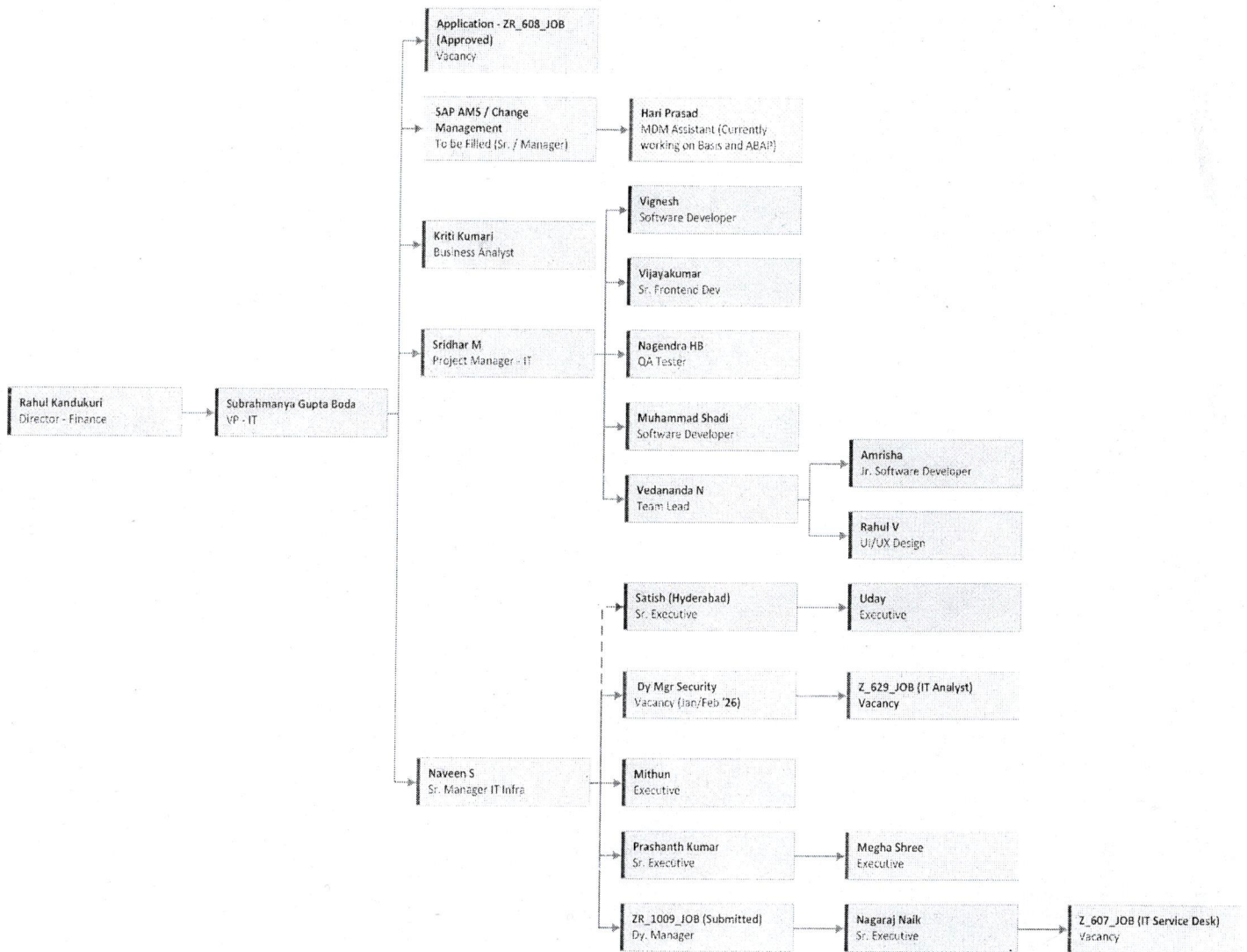


SUMADHURA INFRACON PRIVATE LIMITED

SUMADHURA

FOUNDATION OF HAPPINESS

IT Organogram
Oct 2025

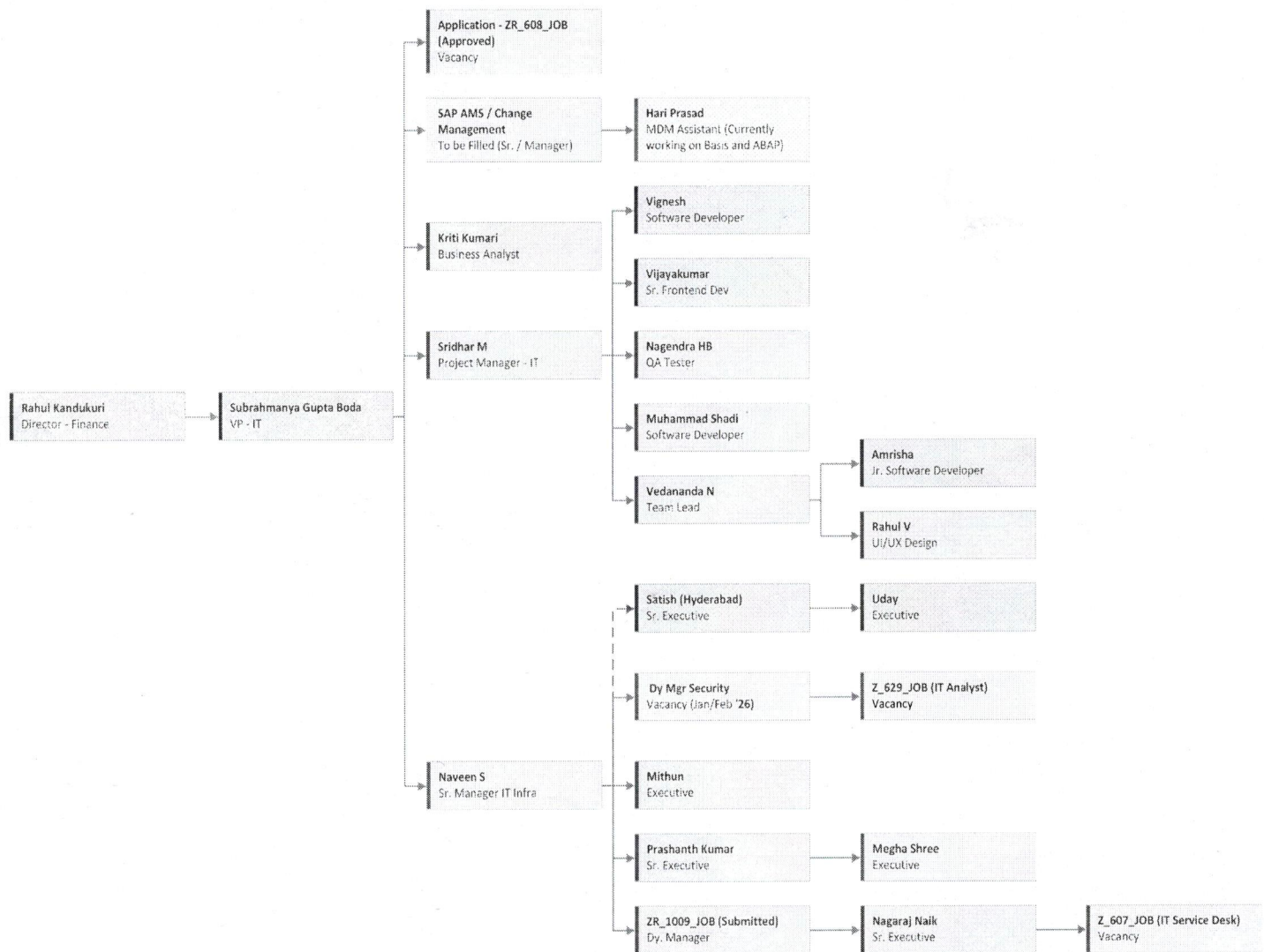


[Signature]
9/04/2025

IT Organogram
Oct 2025

SUMADHURA

FOUNDATION OF HAPPINESS



[Signature]
9/04/2025