

Anunta Technology Management Services Limited (Anunta)

System and Organization Controls (SOC 2) Type 2 Report

For the period January 1, 2024, to December 31, 2024

Report Issue Date: February 28, 2025

Panacea InfoSec (P) Ltd
New Delhi, India
<https://panaceainfosec.com>





Anunta Technology Management Services Limited

Independent Service Auditors' Report on Management's Description of a Service Organization's System Relevant to Security, Confidentiality, Availability and Processing Integrity and the Suitability of the Design and Operating Effectiveness of Controls

For the period, January 01, 2024 to December 31, 2024

(SSAE 21 - SOC 2 Type 2 Report)



Table of Contents

1. Independent Service Auditor's Report.....	5
2. Management of Anunta's Assertion.....	8
3. Description of Anunta's India & International DaaS/VDI, MES & Cloud/DC Operations and Support Function Services relevant to security, confidentiality, availability and processing integrity throughout the period of January 01, 2024 to December 31, 2024..	11
• Background and Overview of Services	11
• Significant Changes during the Review Period.....	11
• Subservice Organizations.....	11
• Components of the System.....	13
• Boundaries of the System.....	13
• Description of Control Environment, Control Activities, Risk Assessment, Monitoring and Information and Communication.....	14
• Applicable Trust Services Criteria and related Controls	32

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

Independent Service Auditor's Report

To: Management of Anunta Technology Management Services Limited (Anunta)

Scope

We have examined the attached Anunta Technology Management Services Limited (Anunta's) description of the system titled "India & International DaaS/VDI, MES & Cloud/DC Operations and Support Function Services" throughout the period January 01, 2024 to December 31, 2024 included in Section 3, based on the criteria set forth in the Description Criteria DC Section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (description criteria) and the suitability of the design and operating effectiveness of controls included in the description throughout the period January 01, 2024 to December 31, 2024 to provide reasonable assurance that Anunta's service commitments and system requirements would be achieved based on the trust service criteria for Security, Availability, Confidentiality and Processing Integrity set forth in TSP Section 100, 2017 Trust Services Principles and Criteria for Security *Availability, Processing Integrity, Confidentiality and Privacy* (applicable trust services criteria).

The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of Anunta's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

As indicated in the description, Anunta uses co-location data centre and cloud service providers as sub service organization to host its IT infrastructure and SaaS base applications. The description in Section 3 includes only the controls of Anunta and excludes controls of the various subservice organizations. The description also indicates that certain trust services criteria can be met only if the subservice organization's controls, contemplated in the design of Anunta's controls, are suitably designed and operating effectively along with related controls at the service organization. Our examination did not extend to controls of various subservice organizations for data center and cloud service provider services.

Service Organization's Responsibilities

Anunta is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the service commitments and system requirements were achieved.

Anunta has provided the accompanying assertion titled, Management of Anunta's Assertion (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirement would be achieved based on the applicable trust services criteria if operating effectively. Anunta is responsible for:

- 1) Preparing the description and assertion;
- 2) The completeness, accuracy, and method of presentation of the description and assertion;
- 3) Providing the services covered by the description;
- 4) Identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements and;
- 5) Designing, implementing, and documenting controls that are suitably designed and operating effectively to meet the applicable trust services criteria stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the presentation of the description based on the description criteria set forth in Anunta's assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects,

- 1) the description is presented in accordance with the description criteria and
- 2) the controls are suitably designed and operating effectively to meet the applicable trust services criteria stated in the description throughout the period January 01, 2023 to December 31, 2024.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide

reasonable assurance that the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion. Our examination also included performing such other procedures as we considered necessary in the circumstances. We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements related to the examination engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs. Because of their nature, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, conclusions about the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria are subject to the risks that the system may change or that controls at a service organization may become ineffective.

Opinion

In our opinion, in all material respects, based on the description criteria described in Anunta's assertion and the applicable trust services criteria:

- a. The description fairly presents the system that was designed and implemented throughout the period January 01, 2024 to December 31, 2024.
- b. The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period January 01, 2024 to December 31, 2024, and the subservice organization and user entities applied the controls contemplated in the design of Anunta's controls throughout the period January 01, 2024 to December 31, 2024.
- c. The controls operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period January 01, 2024 to December 31, 2024, and user entities and subservice organization applied the controls contemplated in the design of Anunta's controls, and those controls operated effectively throughout the period January 01, 2024 to December 31, 2024.

Description of Test of Controls

The specific controls we tested, and the nature, timing, and results of our tests are presented in the section 4 of our report titled "Independent Service Auditors' Description of Test of Controls and Results"

Restricted Use

This report, including the description of controls and results thereof in Section 4 of this report, is intended solely for the information and use of Anunta; user entities of Anunta's systems during some or all of the period January 01, 2024 to December 31, 2024; and those prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

The nature of the service provided by the service organization

- How the service organization's system interacts with user entities, subservice organizations or other parties
- Internal control and its limitations
- User entity responsibilities, Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

This report is not intended to be and should not be used by anyone other than these specified parties.

Shreyash Singwala

CPA Name/Signature: **Shreyash Singwala**

License Number: **PAC-CPAP-LIC-034059**

Date: **February 28, 2025**

SECTION 2

MANAGEMENT OF ANUNTA'S ASSERTION

Management of Anunta's Assertion

February 24, 2025

We have prepared the accompanying description of Anunta Technology Management Services Limited (Anunta) system titled "India and International DaaS/VDI, MES & Cloud/DC Operations and Support Function Services" throughout the period January 01, 2024 to December 31, 2024 (description), based on the criteria set forth in the Description Criteria DC Section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (description criteria).

The description is intended to provide users with information about the India and International DaaS/VDI, MES & Cloud/DC Operations and Support Function Services that may be useful when assessing the risks arising from interactions with Anunta's system, particularly information about the suitability of design and operating effectiveness of Anunta's controls to meet the criteria related to Security, Availability, Confidentiality and Processing integrity set forth in TSP Section 100, 2017 Trust Services Principles and Criteria for Security Availability, Processing Integrity, Confidentiality and Privacy (applicable trust services criteria).

As indicated in the description, Anunta uses subservice organizations for data center and other services. The description in Section 3 includes only the controls of Anunta and excludes controls of the various subservice organizations. The description also indicates that certain trust services criteria can be met only if the subservice organization's controls, contemplated in the design of Anunta's controls, are suitably designed and operating effectively along with related controls at the service organization. Our examination did not extend to controls of various subservice organizations for data center and other services.

The description also indicates that certain trust services criteria specified in the description can be met only if complementary user entity controls contemplated in the design of Anunta's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of user entities.

We confirm, to the best of our knowledge and belief, that

- a. the description fairly presents the India and International DaaS/VDI, MES & Cloud/DC Operations and Support Function Services throughout the period January 01, 2024 to December 31, 2024, based on the following description criteria:
 - i. The description contains the following information:
 - 1) The types of services provided
 - 2) The components of the system used to provide the services, which are as follows:
 - a) Infrastructure. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks).
 - b) Software. The application programs and IT system software that support application programs (operating systems, middleware, and utilities).
 - c) People. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
 - d) Procedures. The automated and manual procedures.
 - e) Data. Transaction streams, files, databases, tables, and output used or processed by the system.
 - 3) The boundaries or aspects of the system covered by the description.
 - 4) For information provided to, or received from, subservice organizations or other parties,

- a) how such information is provided or received and the role of the subservice organization and other parties and
- b) the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.
- 5) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:
 - a) Complementary user entity controls contemplated in the design of the service organization's system.
 - b) When the inclusive method is used to present a subservice organization, controls at the subservice organization
- 6) If the service organization presents the subservice organization using the carveout method,
 - a) the nature of the services provided by the subservice organization and
 - b) each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.
- 7) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons.
- 8) In the case of a type 2 report, relevant details of changes to the service organization's system during the period covered by the description.

ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

- b. The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated as described and if user entities applied the complementary user entity controls, and the subservice organization applied the controls contemplated in the design of Anunta's controls throughout the period January 01, 2024 to December 31, 2024.
- c. The Anunta's controls stated in the description operated effectively throughout the period January 01, 2024 to December 31, 2024 to meet the applicable trust services criteria if user entities applied the complementary user entity controls, and the subservice organization applied the controls contemplated in the design of Anunta's controls throughout the period January 01, 2024 to December 31, 2024.

For Anunta Technology Management Services Limited (Anunta)

Name: Maneesh Raina

Designation: COO

Signature: **MANEESH
RAINA**

Digitally signed by MANEESH
RAINA
Date: 2025.02.25 16:57:40
+05'30'

SECTION 3

DESCRIPTION OF ANUNTA'S "INDIA & INTERNATIONAL DaaS/VDI, MES & Cloud/DC OPERATIONS AND SUPPORT FUNCTION SERVICES"

THROUGHOUT THE PERIOD

January 01, 2024 to December 31, 2024

Description of Anunta's India & International DaaS/VDI, MES & Cloud/DC Operations and Support Function Services relevant to security, confidentiality, availability and processing integrity throughout the period of January 01, 2024 to December 31, 2024

Background and Overview of Services

Background

Anunta Technology Management Services Limited (Anunta) is leading Managed Digital Workspace Solution Provider which enables organization to build a secure and scalable digital workspace on private, public, and hybrid clouds. Anunta's offerings are focused on Desktop-as-a-Service (DaaS), modern desktop management, BYOD and cloud transformation.

Anunta's Managed DaaS offering is a fully managed custom-built DaaS solution for global organization and provides on-demand virtual desktops hosted on any public cloud or customer's on-premises infrastructure using Virtual Desktop Infrastructure (VDI) technology. The DaaS offering covers the full DaaS lifecycle support and end-to-end design, onboarding, migration, and management of virtual desktops. Managed DaaS services are delivered from Anunta's Mumbai, Chennai, and Bangalore delivery centres and Data Centres hosted at Netmagic Solutions, Mumbai, and Chennai.

Anunta's has various product portfolio offering. Anunta's DesktopReady is a Packaged DaaS offering providing secured, pre-configured virtual desktops hosted on public cloud that is easy to deploy and use. EuVantage offers 24/7 infrastructure monitoring. Cloud Optimal helps organization with transparency and cost optimization of their cloud infra.

Anunta is partner to Top Tier technology OEMs and cloud provider and has successfully migrated over 600,000+ user desktops to cloud. Anunta optimizes the design phase to achieve the best TCO outcomes and provide seamless and uninterrupted migration of users.

Anunta's Mission is to empower end users with high-performing desktops on cloud that are secure, seamless, and are available from anywhere for business. Anunta's vision is to help customers maximize their business potential by providing user-centric digital workspace solutions.

Overview of Services Provided

DaaS Operations functions:

- Centralized Support Desk
- End User Support Services
- Server Support Services
- NOC Monitoring Services (EUEM)
- Network Services
- Telecom Services
- WAN Support Services
- Data Centre Services
- Solution Design Services
- Project Management Services

Software Function:

- Software Development & Maintenance

Support functions:

- HR & Training
- Admin & Physical Security
- InfoSec
- Finance
- Legal

Significant Changes during the Review Period

There are no significant changes during the review period.

Subservice Organizations

Anunta utilizes subservice organizations to perform certain key operating functions, specifically related to hosting of production servers, IT staffing, human resource background verification, payroll processing, equipment maintenance, technical scans, software and product licensing and certifications program. The accompanying description of the system includes only those policies, procedures, and controls and does not include policies, procedures and controls at the subservice organizations described below. The examination by the independent auditors did not extend to policies, procedures, and controls at the subservice organizations. Included below is a list of the subservice organizations.

Subservice Organization	Description
NetMagic	Colocation data center services
Microsoft Azure	Cloud services
Impact InfoTech, Team Lease, Sevantis	IT staffing services (third party)
AuthBridge	Human resource background verification services
ADP	Payroll Processing and Time & Attendance management services
Dixit InfoTech	AMC for IT equipment and on-call support
Fortinet	Attack Surface, Brand Monitoring, Darknet Monitoring, please delete - External VAPT, Web Application, Secure Code Analysis, Firewall Rule Review
CrowdStrike Falcon EDR	Next-generation antivirus, endpoint detection and response, threat intelligence, and managed hunting solution
Manage Engine	Automated patch management solution for patch deployment on Windows, MacOS, and Linux systems.
Panacea InfoSec Pvt Ltd	External VAPT, Web Application, Secure Code Analysis, Firewall Rule Review
Microsoft	Enterprise agreement for Microsoft product licensing and support
Accops	A Server and Workspace virtualization solution for secure access
BSI	Management framework certifications (ISO 27001, ISO 27701, ISO 20000)

The Criteria that relate to controls at the subservice organizations included all criteria related to the Trust Service Principles of Security, Availability and Confidentiality. The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls include:

- The system is protected against unauthorized access (both physical and logical).
- Policies and procedures exist related to security and availability and are implemented and followed.

Anunta utilizes the following subservice providers for data centre and cloud services that are not included within the scope of this examination. However, Anunta's responsibilities for the applications and services run at these colocation data centre and cloud services are covered as part of the audit and in scope. Responsibility matrix is defined as part of the SLA and agreements with these sub service organizations.

Netmagic Solutions Pvt. Ltd.

Netmagic Solutions is used for co-location data centre service for hosting the products and is a SOC 2 attested data centre company. NetMagic Solutions has provided an Independent Service Auditors Report (SOC2).

The Criteria that relate to controls at the subservice organizations included all criteria related to the Trust Service Principles of Security, Availability and Confidentiality. The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls at Netmagic Solutions include:

- The system is protected against unauthorized access (both physical and logical).
- The system is available for operation and use and in the capacities as committed or agreed.
- Policies and procedures exist related to security and availability and are implemented and followed.

Microsoft Azure

Anunta is taking cloud services from Azure to host its applications to provide DaaS services and is a SOC2 attested cloud service provider. Azure has provided an Independent Service Auditors Report (SOC2).

The Criteria that relate to controls at the subservice organizations included all criteria related to the Trust Service Principles of Security, Availability and Confidentiality. The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls at Azure include:

- The system is protected against unauthorized access (both physical and logical).
- The system is available for operation and use and in the capacities as committed or agreed.
- Policies and procedures exist related to security and availability and are implemented and followed.

Principal Service Commitments and System Requirements

Anunta designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Anunta makes to user entities, the laws and regulations that govern the provision of services to its clients, and the financial, operational, and compliance requirements that Anunta has established for the services. Security

commitments to user entities are documented and communicated in customer agreements, as well as in the description of the service offering provided online.

Anunta establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Anunta's system policies and procedures, system design documentation, and contracts with customers.

Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the System.

The principal system requirements include:

- Logical access to programs, data and computer resources is restricted to authorized and appropriate users, and such users are restricted to performing authorized and appropriate actions.
- Physical access to computer and other resources is restricted to authorized and appropriate personnel.
- Changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented to result in complete, accurate and timely processing and reporting of transactions.
- Network infrastructure is configured as authorized to (a) support the effective functioning of application controls to results in valid, complete, accurate and timely processing and reporting of transactions; and (b) protect data from unauthorized changes.
- Application and system processing are authorized and executed in a complete, accurate and timely manner, and deviations, problems and errors are identified, tracked, recorded, and resolved in a complete, accurate and timely manner.
- Data is backed up regularly and is available for restoration in the event of processing errors or unexpected processing interruptions.

Components of the System

The System is comprised of the following components:

- Infrastructure including the physical structures, cloud setup, information technology (IT) and other hardware,
- Software including application programs and IT system software that support application programs,
- People including executives, sales and marketing, client services, product support, information processing, software development, IT,
- Procedures (automated and manual), and
- Data including transaction streams, files, databases, tables, and output used or processed by the system.

The System boundaries include the applications, databases and infrastructure required to directly support the services provided to Anunta's clients. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to Anunta's customers are not included within the boundaries of its system.

Boundaries of the System

The specific services and locations included at the organization level in the scope of the report are given below. All other products, services and locations are not included.

Products and Services in Scope
<p>The scope of this report is limited to India & International DaaS/VDI, MES & Cloud/DC Operations and Support Function Services.</p> <p>Services</p> <p>DaaS Operations functions:</p> <ul style="list-style-type: none"> • Centralized Support Desk • End User Support Services • Server Support Services • NOC Monitoring Services (EUEM) • Network Services • Telecom Services • WAN Support Services • Data Centre Services • Solution Design Services • Project Management Services <p>Software Function:</p> <ul style="list-style-type: none"> • Software Development & Maintenance

Support functions:

- HR & Training
- Admin & Physical Security
- InfoSec
- Finance
- Legal

Geographic Locations in Scope

Country	City	Location Address
India	Mumbai	Level 2, Block 6, Nirlon Knowledge Park, Off Western Express Highway, Goregaon (East), Mumbai – 400063, Maharashtra
	Chennai	4 th Floor, Block B, Futura Tech Park, 334, Old Mahabalipuram Road, Sholinganallur, Chennai – 600119, Tamil Nadu
		Prestige Polygon, 9th floor, Anna Salai, Rathna Nagar, Teynampet, Chennai - 600035, Tamil Nadu
	Bengaluru	Level 2, API Bhavan, 16F, Miller Tank Bed Area, Vasantha Nagar, Bengaluru – 560052, Karnataka

The report excludes all processes and activities that are executed outside above locations. Unless otherwise mentioned, the description and related controls apply to locations covered by the report.

Description of Control Environment, Control Activities, Risk Assessment, Monitoring and Information and Communication

Control Environment

Anunta’s internal control environment reflects the overall attitude, awareness, and actions of management concerning the importance of controls, and the emphasis given to controls in the Company’s policies, procedures, methods, and organizational structure.

The Chief Executive Officer, the Senior Management Team and all employees are committed to establishing and operating an effective Information Security Management System in accordance with its strategic business objectives. The Management at Anunta is committed to the Information Security Management System, data protection and ensures that IT policies are communicated, understood, implemented and maintained at all levels of the organization and regularly reviewed for continual suitability.

Integrity and Ethical Values

Anunta requires directors, officers, and employees to observe high standards of business and personal ethics in conducting their duties and responsibilities. Honesty and integrity are core principles of the company, and all employees are expected to fulfill their responsibilities based on these principles and comply with all applicable laws and regulations. Anunta promotes an environment of open communication and has created an environment where employees are protected from any kind of retaliation should a good faith report of an ethics violation occur. Executive management has the exclusive responsibility to investigate all reported violations and to take corrective action when warranted.

Board of Directors

Business activities at Anunta are under the direction of the Board of Directors. The company is governed by its Board of Directors headed by its founder Ananda Mukerji as the Founder & Executive Chairman. Sivakumar Ramamurthy is the CEO and Deputy Managing Director is in charge of the company’s Global operations playing a key role in strategy and client management.

Management’s Philosophy and Operating Style

The Executive Management team at Anunta assesses risks prior to venturing into business ventures and relationships. The size of Anunta enables the executive management team to interact with operating management on a daily basis. The key functions of Board of Directors (BoD) include:

- Monitoring the external environment;
- Understanding the strategies and capabilities of the company’s major competitors;
- Assessing strategic implications of opportunities and business risks;
- Analysing strengths and weaknesses relative to the company’s goals;
- Formulating implementation strategies;
- Allocating resources (capital, people, and facilities);

- Measuring and monitoring organizational and business unit performance via internal controls; and
- Identifying and evaluating functions, which are key to executing company strategies.

Anunta's Vision and Mission

Vision

To help customers maximize their business potential by providing user centric digital workspace solutions.

Mission

To empower end users with high performing desktops on cloud that are secure, seamless and are available from anywhere for business.

Values

Honesty and Reliability

The consciousness that they have put in the centre on every stage of their workings and reliability, honesty, and mutual trust.

Risk Management and Risk Assessment

The application of protection measures is based on the risk associated with information assets and the importance of those assets to the organization. As part of this process, threats to security are identified and the risk from these threats is formally assessed.

Anunta has placed into operation a risk assessment process to identify and manage risks that could adversely affect their ability to provide reliable processing for User Organizations. This process consists of management identifying significant risks in their areas of responsibility and implementing appropriate measures to address those risks. Senior Management team are members of forums and core working groups in industry forums that discuss recent developments.

Pandemic /COVID 2019 Risks

Anunta has reassessed its risk with respect to Pandemic risk / COVID risks. Appropriate short term and long-term changes have been made to impacted controls.

Information Security Policies

Anunta has developed an organization-wide Information Security Policies. Relevant and important Security Policies (IS Policies) are made available to all employees via Company Intranet to new employees. Changes to the Information Security Policies are reviewed and approved prior to implementation.

Following is the key list of policies by the organization:

- **Anunta ISMS Scope Document**
This document provides the scope of the information security management systems of the organization.
- **Information Security and Privacy Management Manual**
This document provides the consolidated view of all information security and privacy policies including organization structure and roles and responsibilities at different levels.
- **Service Management System Manual**
This document provides guidance and direction for the implementation and continual improvement of service management framework.
- **PL-Acceptable Use**
The policy specifies acceptable uses of systems and user responsibilities for the security and confidentiality of data. It provides guidelines to employees of how to protect company data.
- **PL-Access and Identity Management**
This policy outlines the rules governing user IDs, system authentication, new-hire and termination procedures, and password management.
- **PL-Account Management**
This policy sets forth the requirements and controls for account management to protect the confidentiality, integrity and availability of information assets.

- **PL-Anunta Management System Policy**

This policy specifies the requirements, applicability and guidelines to users of all management systems such as ISO 27001, ISO 27701, and ISO 20000.

- **PL-Anunta Privacy Policy**

This policy specifies the privacy information management system and guidelines to handle personal data.

- **PL-Anunta Website Privacy Policy**

This policy aims to tell users how and why Anunta collect their information, use that data, and if it shares with others.

- **PL-Anunta Whistleblower Policy**

- This policy aims to encourage employees and others to report any serious concerns, misconduct or illegal acts.

- **PL-Asset and Information Management**

This policy defines the handling of the assets during its lifecycle starting from procurement to disposal.

- **PL-Business Continuity and Availability Management**

It is the intent to ensure that each client line of business implements a BC management plan. Anunta recognizes that BC management increases the client program's resilience to business disruption arising from internal and external events and reduces the impact on the accounts and eventually business operations, reputation, profitability, policy owners and stake holders.

BC Plans are designed to assist in ensuring an effective response to incidents that may occur and that would threaten normal operations. In smaller organizations, one BC plan may be sufficient to cover all operations and processes, whereas in a larger organization a number of plans may be required in the interests of practicality and maintainability to cover different sites or office locations and/or different organizational functions.

- **PL-Capacity Management**

This policy defines to maximize the production output and to keep an eye on how much can be achieved from existing resources and be prepared to meet any future requirements.

- **PL-Change Management**

This document defines the change management guidelines.

- **PL-Compliance**

- This policy defines the applicable compliance requirements are identified and governed to ensure they are met.

- **PL-Cryptography Controls**

This policy aims to establish the standards and responsibilities for the encryption of digital assets and is managed in a consistent and appropriate manner.

- **PL-Data Retention and Disposal Policy**

This policy defines the requirement to identify the data to be retained as per any legal, regulatory, contractual and business requirements and to ensure data is securely disposed post its retention period.

- **PL-Email and Internet Security**

This policy defines the standard for the use of organization email and internet and set guidelines to the users.

- **PL-Human Resource Security**

This policy aims to establish the process for human resource security during talent acquisition, onboarding, background check, offboarding, training and performance management.

- **PL-Incident Management**

This policy defines the process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, ensuring that agreed levels of service quality are maintained.

- **PL-Information Classification**

This policy defines the classification of data/information based on its level of sensitivity and impact should it be disclosed, altered, or destroyed without authorization.

- **PL-Malware Protection**

This policy aims to protect information and information asset from all security threats to safeguard information to minimize the risk of information leakage or compromises.

- **PL-User End Point Device Security**
This policy aims to set guidelines to safeguard information on mobile devices and to users while they own or handle any mobile devices.
- **PL-Network Security**
This policy provides an overview of the network security protocols in place.
- **PL-Operational Technology Security**
This policy aims to identify potential vulnerabilities and address them to prevent sensitive information from being lost, stolen, or compromised.
- **PL-Organization of Information Security**
This document defines the structure of information security organization and governance.
- **PL-Password Management**
This document sets the user account management criteria and password requirements for users and systems.
- **PL-Physical and Environmental Security**
This policy describes the methodology by which access to sensitive areas or building that house information is controlled and monitored.
- **PL-Data Masking, Anonymization and Pseudonymization Policy**
This policy aims to define guidelines to make personal data anonymize and pseudonymize to intact user privacy.
- **PL- Social Media Policy**
This policy aims to set expectations for appropriate behavior and ensure that an employee's social media posts will not expose the company to legal problems or public embarrassment.
- **PL- Software License Management**
This policy aims to identify the list of licensed software used in the organization and to ensure enterprise-wide license management to avoid any copyright infringement.
- **PL-Supplier Relationship**
This policy aims to identify list of subservice organizations and to have necessary contracts and agreements.
- **PL-System Acquisition, Development and Maintenance**
This policy defines the requirements of secure software development lifecycle.
- **PL-Release and Deployment Management**
This document defines release and deployment management.
- **PL-Remote Working Policy**
This policy aims to provides clarity on remote work procedures, ensures productivity, and offers flexibility to employees while safeguarding company interests.
- **PL-Training and Professional Development**
This policy defines the needs and strategy for employees training, awareness and education related to their job responsibilities and information security and data privacy.
- **PL-Budgeting and Accounting**
This document defines budgeting and accounting for service components.
- **PL-Continual Improvement**
This document aims to improve the suitability, adequacy, effectiveness and efficiency of information security, privacy and service management system.
- **PL-HIPAA Breach Notification Policy**
The aim of this policy is to ensure compliance with applicable status of HIPAA, HITECH and applicable regulations.
- **PL-Threat Intelligence**
This document defines ways to protect information assets from a variety of threats.

- **PL-Use of Cloud Services**
This document provides guidance on acquisition, use, management and exit of cloud services.
- **PL-Service Catalogue**
This document provides the details of service catalogue – existing and potential services.
- **PR-Human Resource Procedure**
This document defines the various activities performed by the Human Resource function.
- **PR-Onboarding Process**
This document defines the requirements for onboarding process for human resource.
- **PR-Training Process**
This document establishes a governance structure to drive end to end training programs for the employees.
- **PR-Employee Exit Process**
This document defines the requirements for offboarding process for human resource.
- **PR- Physical Security and Administration**
This document defines the various activities performed by the physical security and administration function.
- **PR-Access Control**
This policy aims to minimize the security risk of unauthorized access to physical and logical systems.
- **PR-Privilege Access Management**
This document describes the management of privilege users and PAM.
- **PR-Problem Management**
This document aims to identify problems and minimize or avoid the impact of incidents and issues.
- **PR-PII Principal Rights Management**
This document aims to effectively manage requests from PII principal or data subjects or their representatives.
- **PR-Access Card Management**
This document provides guidelines for access card control – permanent and temporary card.
- **PR-Account Management, Password Reset and Account Unlock**
This document defines the guidelines for user account unlock and password reset.
- **PR-Account Management**
This document defines the account ID, email ID creation and deletion process.
- **PR-User Addition, Deletion and Modification**
This document defines procedure for adding, deleting and modifying a user in the application.
- **PR-Anti Virus Management**
This policy aims to protect information and information asset from all security threats to safeguard information to minimize the risk of information leakage or compromises.
- **PR-Anunta Infra Monitoring**
This document aims to ensure the monitoring of network, servers, applications and IT infrastructure for its continued availability.
- **PR-Background Verification**
This document sets the requirement of background check during onboarding for human resource security.
- **PR-BitLocker Drive Encryption**
This policy provides guidance on the use of encryption to protect information resources that process or transmit confidential information.
- **PR-Change Management**
This policy ensures that all changes to IT services and infrastructure are planned, approved, communicated, recorded, and implemented successfully.

- **PR-Customer Experience Poll**

This document defines to take input and feedback from customer basis on their experience for the services offered to them.

- **PR-Business Relationship Management**

This document is to establish and maintain a working relationship between Anunta and its clients.

- **PR-Data Centre Service Management**

This document aims to set the guidelines for the service management of data center.

- **PR-Disciplinary Action**

This policy aims to make users aware of the consequences of the noncompliance to organization information security guidelines.

- **PR-Backup and Recovery**

This policy sets the strategy and guidelines of information backup and restoration.

- **PR-Software License Management**

This document defines the guidelines of software asset lifecycle and its management.

- **PR-Stale Computer Object Cleanup**

This document sets the guidelines for efficient management and clean up of stale computer objects in active directory.

- **PR-Software Team Exception and Deviation Handling**

This document outlines the procedure for managing exceptions and deviations related to software acquisition, development, and maintenance.

- **PR-System Testing**

This document defines the procedure for carrying out system testing.

- **PR-Event Logging**

This document defines the requirements and guidelines for capturing and review of security events, audit trails and to report security incident to take appropriate action when required.

- **PR-Information Security Incident Management**

The policy provides a general overview of the incident management and response process. It outlines classification, priorities, notification and reporting of incidents.

- **PR-Risk Management**

This policy describes the process by which risks to protected and confidential information are assessed and managed. The Incident Management Policy directs personnel to respond to any actual or suspected security incidents relating to information systems and data.

- **PR-ISO Internal Audit**

This policy provides the process for org wide internal information security audit coverage, frequency, and action on reported findings.

- **PR-Asset Management**

This document defines the guideline for asset management.

- **PR-IT Asset Disposal**

This policy describes the guidelines for asset disposal and to track the disposed asset.

- **PR-Patch Management**

This document describes the process of applying updates to software, drivers, and firmware to protect against vulnerabilities.

- **PR-Vulnerability Management**

This policy aims to establish the rules for the review, evaluation, application, and verification of system updates to mitigate vulnerabilities in the IT environment and the risks associated with them.

- **PR-Configuration Management**

This document ensures that selected components of a complete IT service, system or product are identified, baseline and maintained in a controlled manner.

- **PR-WAN Service Management**

This policy describes the process of monitoring the WAN for health, performance, and availability.

- **PR-Capacity Management**

This document defines the capacity management process for human, technical, information and financial resources.

- **PR-Communication Management**

The objective of this document is to establish a procedure for internal and external communication needs.

- **PR-Business Continuity and Availability Management**

This document objective is to define procedures for business continuity.

- **PR-Server Support Service**

This document describes various activities performed to provide support to operating systems.

- **PR-IT Service Request Management**

This document sets guidelines to enable effective and efficient management of service requests.

- **PR-Service Design and Transition**

This document establishes and implement plans to control the delivery of new services or changes to the services.

- **PR-Service Level Management**

This document ensures that services are provide in line with the agreed service level.

- **PR-Budgeting and Accounting**

The document is to define a process for budgeting and accounting for services.

- **PR-Key Management**

This document is to define the key management process.

- **PR-Anunta Management System Performance Evaluation**

This document aims to define procedure for evaluating the performance of Anunta management systems namely ISMS, PIMS and ITSM.

- **PR-Compliance**

The objective of this document is to ensure that compliance with technical, legal, regulatory, contractual and procedural requirements.

- **PR-Document Control**

This document describes creating, storing, revising, updating, retaining and securely disposing of documents.

- **PR-HIPAA Breach Notification**

This document is to define the procedure for breach notification and response.

- **PR-Continual Improvement**

This document aims to elaborate on ways to improve the effectiveness and efficiency of management systems framework.

Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changes in business conditions. Anunta management and Information Security personnel monitor the quality of internal control performance as a routine part of their activities.

Production systems and infrastructure are monitored through service level monitoring tools which monitor compliance with service level commitments and agreements. Reports are shared with applicable personnel and customers, and actions are taken and communicated to relevant parties, including customers, when such commitments and agreements are not met. In addition, a self-assessment scan of vulnerabilities is performed. Vulnerabilities are evaluated and remediation actions monitored and completed. Results and recommendations for improvement are reported to management.

Information and Communication

Anunta has documented procedures covering significant functions and operations for each major work group. Policies and procedures are reviewed and updated based upon changes and approval by management. Departmental managers monitor adherence to Anunta policies and procedures as part of their daily activities.

Anunta management holds departmental status meetings, along with strategic planning meetings, to identify and address service issues, customer problems, and project management concerns. For each service, there is a selected service manager who is the focal point for communication regarding the service activity. Additionally, there are personnel that have been designated to interface with the customer if processing or systems development issues affect customer organizations. Electronic messaging has been incorporated into many of Anunta’s processes to provide timely information to employees regarding daily operating activities and to expedite management’s ability to communicate with Anunta employees.

Electronic Mail (e-Mail)

Communication to Customer Organizations and project teams through e-Mail. Important corporate events, employee news, and cultural updates are some of the messages communicated using e-Mail. e-Mail is also a means to draw attention of employees towards adherence to specific procedural requirements.

Components of the System

Infrastructure

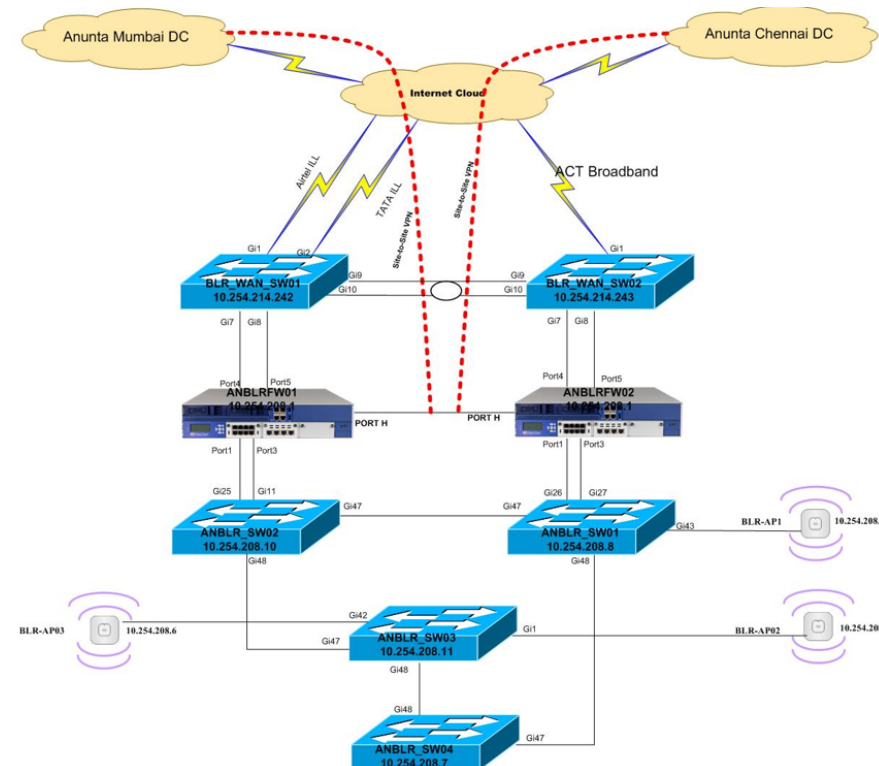
The infrastructure comprises physical and hardware components of the System including facilities, equipment, networks, cloud services, laptops and software. Offices are connected to internet using high speed leased lines and broadband connections.


Network Segmentation Overview

Anunta offices are equipped with the latest hardware, software and networking infrastructure. Offices are linked using high speed communication links, backed up by redundant networks.

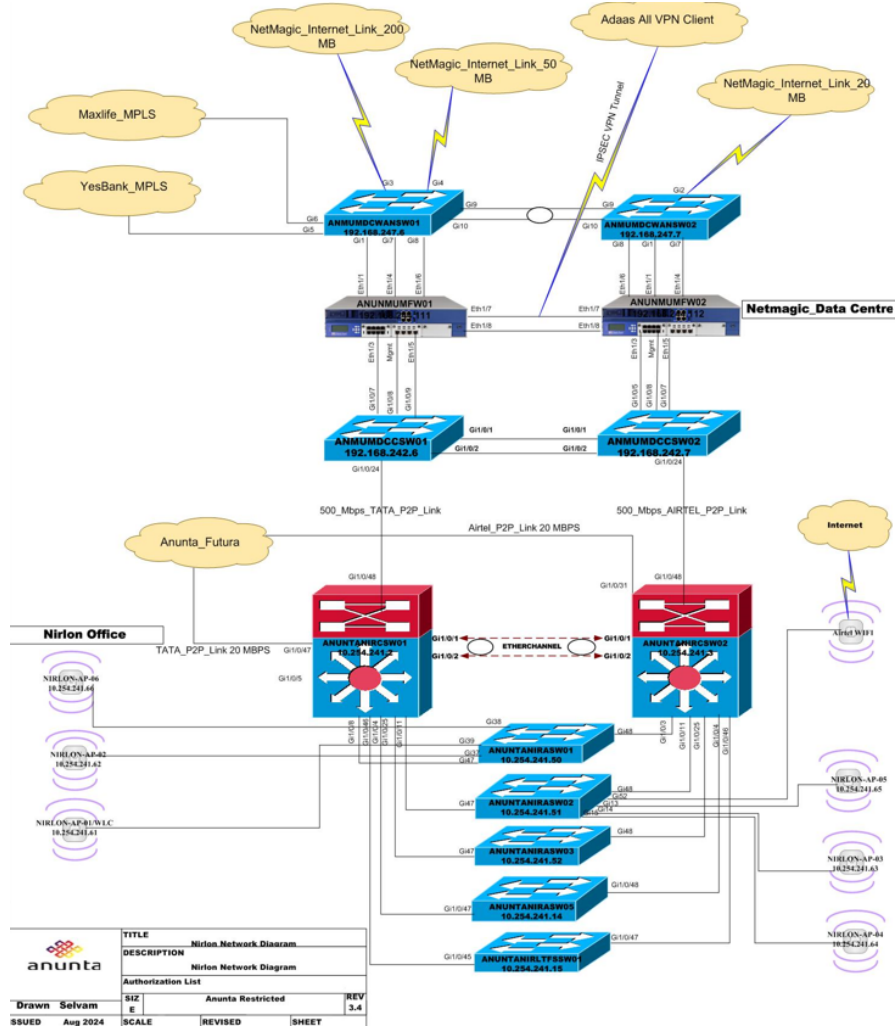
NETWORK DIAGRAMS

Anunta Network Architecture Diagram – Bengaluru

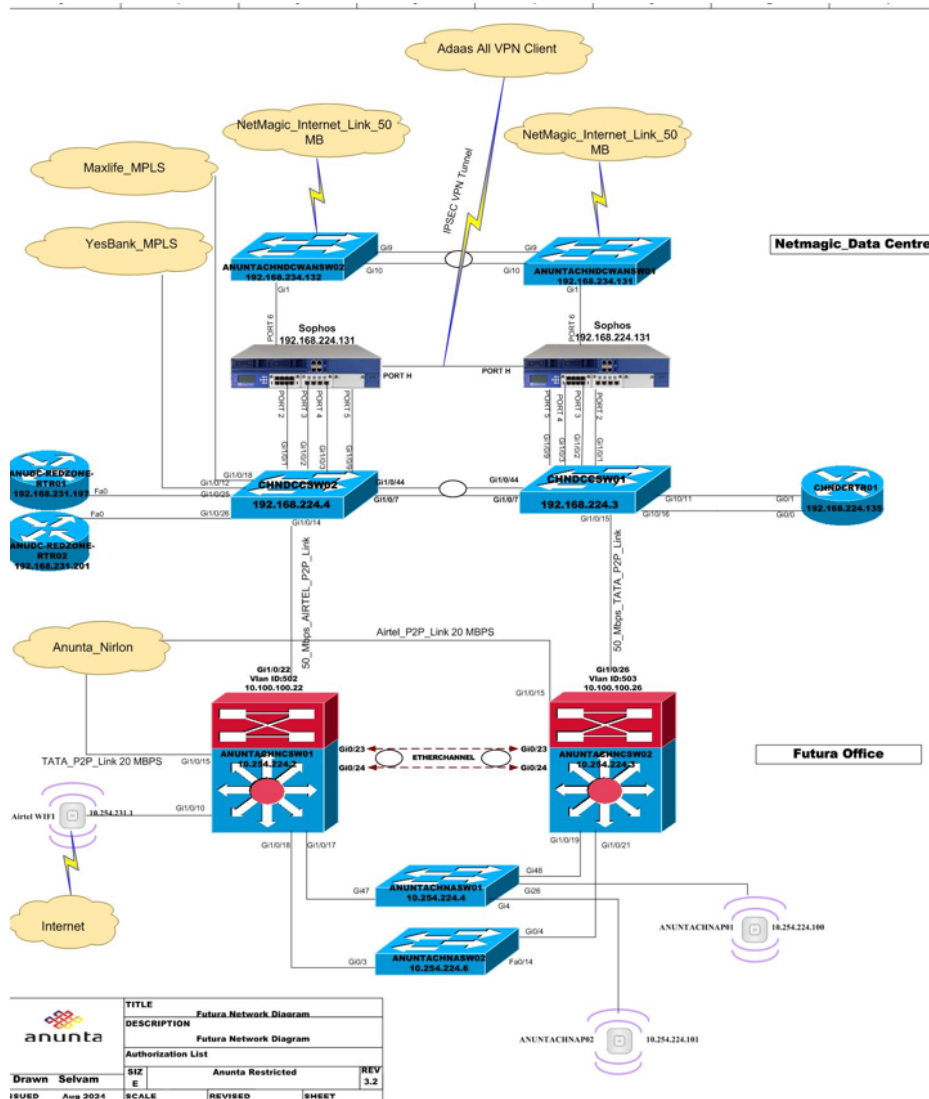


	TITLE: Bangalore Network Diagram		
	Description: Bangalore Network Diagram		
Authorization List			
Drawn : Selvam	SIZE	ANUNTA Restricted	VER. 2.0
Issued : Aug 2024	SCALE	REVISED	SHEET

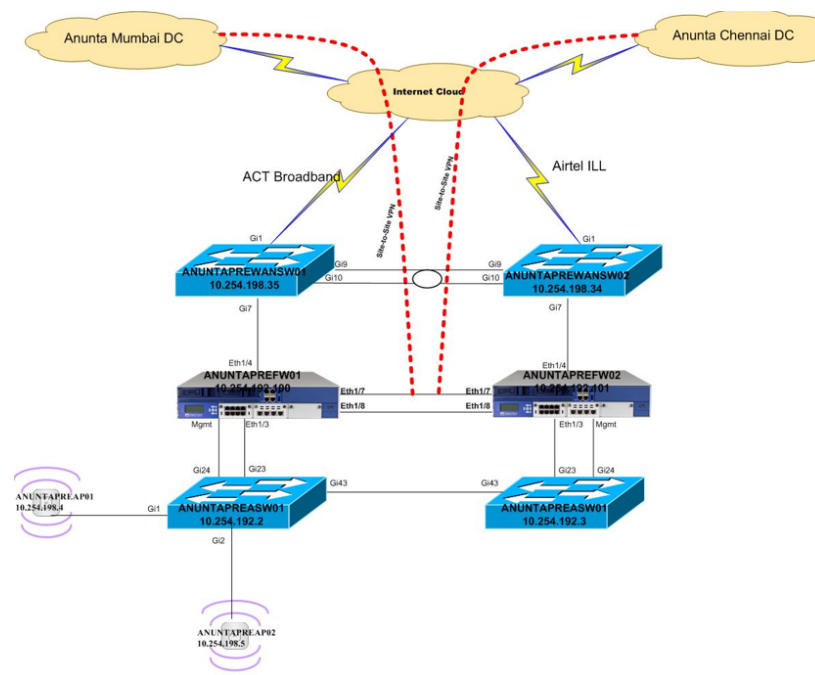
Anunta Network Architecture Diagram – Mumbai




Anunta Network Architecture Diagram – Chennai (Futura Tech Park)



Anunta Network Architecture Diagram – Chennai (Prestige Polygon)



		TITLE: Prestige Network Diagram	
		Description: Prestige Network Diagram	
Authorization List			
Drawn : Selvam	SIZE	ANUNTA Restricted	VER. 1.1
Issued : Aug 2024	SCALE	REVISED	SHEET

Network Connection to Client Sites

“Anunta connects to the client network and systems via secured tunnel. The access is limited to infrastructure for which Anunta is responsible to manage. Client application login ID and password is shared on need to have basis with Anunta’s authorized employees for delivering the services.

Physical Structure Overview

Anunta’s power systems are designed to provide uninterrupted power, regardless of the availability of power from the local public utilities supplying the office premises, UPS units and backup generators supply power to the center in the event of a power failure. All components are covered by maintenance contracts and tested regularly. Generators are tested periodically.

Fire Extinguishers and smoke detectors are installed at all sensitive points. Regular check on the working condition is done, warranty is checked and AMC is entered on completion of Warranty. Yearly fire drills are conducted in coordination with Admin and HR personnel. The fire drills reports are collected and analysis made upon them.

Media Disposal process ensures that the disposal of unwanted media etc., are disposed timely to protect and maintain the security of the information and data.

Physical Access

Anunta has its operations and delivery centers at multiple locations across the country. The entrances are secured with physical access controls and in many places by a security person and CCTV surveillance. Physical and Environmental Security of Anunta is controlled and governed by Anunta ISMS Policy.

Entry to the Anunta offices is restricted to authorized personnel by an electronic access badge control system. All employees are provided with electronic access card which helps to open the door of designated areas to authorized individuals. All visitors have to sign the visitors register and not provided any access to the door and escorted by the designated employees.

Employees are subjected to show their ID cards at the Security entrance and use electronic access card to access authorized area. Employees are granted access only to those areas which they require to access. Some members of the IT Support Team & Administration team have access to the entire facility. The management team has access to all areas except the server rooms. Employees are required to always wear their employee identification cards while within the facility.

CCTV is implemented to monitor the activities in server room and main entrance and other secure zones. Admin Team monitors the CCTV recordings. Logs are generated and communicated to the management periodically. Backup of recordings are retained.

ID cards are issued to new employees based on an access requisition initiated by the Human Resource (HR) group. The HR group sends an email requesting the IT team and Administration / Facilities team to issue an access card to the new employee. The IT / Administration team ensures that the access controls are configured with the appropriate access rights, and then issues the same to the employee.

On separation of an employee from the organization, the HR group initiates the 'Exit Process' and circulates it to all the concerned groups. Based on this, the employee's privileges in the access control system are revoked.

Access by visitors, contractors and/or third-party support service personnel's both entry and exit are monitored by security personnel. Photography, video, audio, or other recording equipment, are not allowed inside secure premises, unless specifically authorized. Such accesses are recorded, authorized, and monitored. Visitor, contract and/or third-party service personnel to sensitive areas such as data centers are strictly on "need to have" basis and subject to the principle of least privileges.

Access to the Server Room

Access to the server room is controlled by an access control system. Anunta policies protect sensitive equipment such as servers, communication and power hubs and controls by locating them in secure and server room and bonded areas that are not easily visible / accessible to public and apply appropriate controls to mitigate risks from physical and environmental threats and hazards and opportunities for misuse or unauthorized access. Only Authorized personnel are allowed to enter such sensitive areas controlled with face recognition systems. Third parties are allowed access to the server room only under the supervision of IT team members.

Software

Firewalls

Firewall is configured and in place to protect IT resources. Firewall and switch configuration standards are documented. Firewall and switch configurations are reviewed by management periodically. The ability to modify firewall is limited to the Anunta IT Department. Specifically, IT Department is authorized to request changes from the provider.

Internet Access to Anunta employees is limited through access rules on firewall and restricted to lower-level employees. Only frequently used sites are open to the employees for production purpose. Management level employees are given full access through firewall configuration.

Endpoint Security, Threat Intelligence and Cyberattack Solution

Anunta has deployed CrowdStrike next generation anti-virus for enhance detection and response, Exposure Management, Device Control, host firewall, Counter Adversary operations, investigate, host setup and management and Automated workflows for endpoint security.

Network & endpoint protection / monitoring

Access to Internet services from any company computing device (laptop, workstation, server etc.) or from any company address designation should be made through the company's approved perimeter security mechanisms. External connections to company servers is not permitted.

In order to stop any malware from affecting the security of the customer and organizational data, Anunta uses Endpoint Protection vulnerability scans along with UTM devices. IT team ensures that all the endpoints in organizations are scanned for any vulnerabilities, including public IPs and services hosted on Data Center, and that any malware is dealt with efficiently and in a timely manner.

Monitoring

Anunta has devised and implemented adequate monitoring controls to detect unauthorized information processing activities. Critical servers and systems are configured to log user activities, exceptions and information security events. System administrator and system operator activities are logged and reviewed on a periodic basis.

Capacity management controls are put in place to make certain Anunta's resources are monitored, tuned and projections are made to ensure system performance meets the expected service levels and to minimize the risk of systems failure and capacity related issues. Addition of new information systems and facilities, upgrades, new version and changes are subject to formal system analysis, testing and approval prior to acceptance.

Patch Management

The IT team ensures that all patches to network device/servers operating systems are checked for stability & any availability issues & tested before applying to the production environment. The patch management activity is done with the help of IT team regularly or as and when any critical event occurs and required updates or patch are installed to ensure efficient working of the servers, desktops and critical network devices. Operating system patches are managed and applied as they become available.

Vulnerability Scans & Intrusion Detection/Intrusion Prevention

As per the Audit calendar, all the network settings are audited for any vulnerability by doing scans periodically. These scans are done by the system admin internally and by CERT-In empaneled third-party vendor. Endpoint Protection is installed with the feature of scanning the device automatically and log reports are reviewed by the system Admin.

Anti-virus software has been installed on all desktops & laptops within the scope. Updates to the virus definition files are managed and downloaded by the software itself on a daily basis from the vendor website at specific intervals.

All inbound and outbound e-Mails are scanned for viruses and are cleaned automatically using scan services. Anti-malware and security practices are in accordance with Anunta Malware Protection Policy.

People

Organizational Structure

The organizational structure of Anunta provides the overall framework for planning, directing, and controlling operations. It has segregate personnel and business functions into functional groups according to job responsibilities. This approach helps enable the organization to define responsibilities, lines of reporting, and communication, and helps facilitate employees to focus on the specific business issues impacting Anunta clients.

CEO is responsible for oversight of Anunta. The Anunta site is locally managed by the following individuals / teams:

- NOC Monitoring Services (EUEM)
- Network Services
- Telecom and WAN Support
- Server Support Services
- End User Support Services (EUC)
- Centralized Support Desk (CSD)
- IT Asset Management
- IT Supplier Management
- Software Development and Maintenance
- Incident, problem and Change Management Services
- Management Information Services (MIS)
- Physical Security and Administration
- Human Resource, Recruitment and Training
- Information Security
- Centre of Excellence (CoE) and Project Management (PMO)

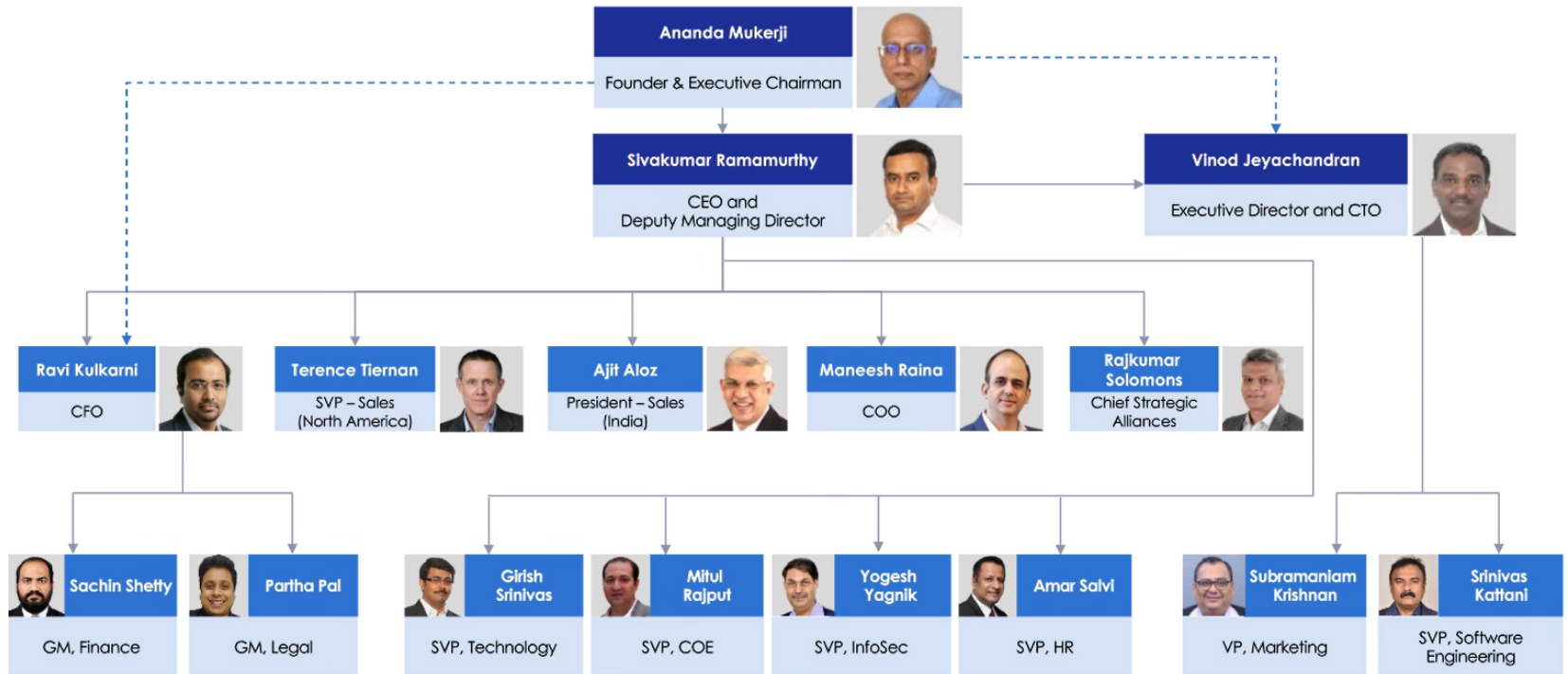
The management team meets periodically to review business unit plans and performances. Weekly, monthly meetings and calls with senior management, and department heads are held to review operational, security and business issues, and plans for the future.

Anunta's Information Security policies define and assign responsibilities/accountabilities for information security. Regular management meetings are held to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.

(This page/space left blank intentionally)

Organization Chart

Leadership & Management Team



Roles and Responsibilities

The following are the responsibilities of key roles.

Founder and Executive Chairman

Founder and Executive Chairman is the head of the organization and manages the company's budget and allocates its resources. Create strategic business plans for meeting the company's goals. Promote development and research for boosting business growth. Track technology advancements and trends to stay competitive.

CEO (Chief Executive Officer) and Deputy Managing Director

CEO leads the global and local business and organization development strategies and the public face of the organization. CEO is responsible for making major corporate decisions, managing overall operations, and setting the company's strategic direction. CEO is accountable to the board of directors or stakeholders.

COO (Chief Operating Officer)

COO leads the operation team to bring operational excellence, strategic alignment and improved performance to the organization contributing to its long-term success and growth. COO is responsible to streamline and optimize operational process for increased efficiency and to enhance cross functional collaboration fostering better communication and coordination among different departments.

SVP HR & Training

The SVP HR & Training is responsible for developing and executing human resource strategy in support of the overall business plan and strategic direction of the organization, specifically in the areas of succession planning, talent management, change management, organizational and performance.

CFO (Chief Finance Officer)

The chief financial officer head of finance and responsible for tracking cash flow and financial planning and analyzing the company's financial strengths and weaknesses and proposing strategic directions.

CSA (Chief Strategic Alliance)

Chief Strategy Officer heads the organization strategy team and develop a comprehensive, inclusive strategic plan and growth strategy by collaborating with the CEO, senior leadership and the board of directors, which determines the enterprise's overall vision, evaluates the overall business portfolio, and M&A plan.

CISO (Chief Information Security Officer/SVP InfoSec)

The Chief Information Security Officer (CISO) heads the Information Security and responsible for establishing and maintaining the enterprise vision, strategy and program to protect information assets and technologies. CISO also directs staff in

Anunta Technology Management Services Limited (Anunta)

Confidential

implementing and maintaining processes and establish appropriate standards and controls across the organization to reduce information and information technology (IT) risks.

CISO/SVP InfoSec is responsible for:

- Updating and implementing Information Security Management System (ISMS) policies and procedures, guidelines, manuals, Standard Operating Procedure (SOP), and other information security related documents;
- Performing Risk Assessment (RA) and updating the risk register;
- Implementing the risk treatment plan and controls;
- Sharing mitigation status of key risks in semi-annual Management Review Meeting (MRM);
- Performing Internal ISMS Audit and tracking corrective action for non-compliances;
- Reviewing information security incidents;
- Performing Root Cause Analysis (RCA) for information security incidents;
- Imparting information security training as part of induction program; and
- Sharing periodic information security awareness e-mails.

ISM (Information Security Manager)

Information Security Manager reports to CISO and responsible to implement and manage security policies and conduct risk assessment, vulnerability assessment and penetration testing. ISM is also responsible for developing and conducting information security training and awareness program, monitor and respond to security incidents and breaches and to collaborate with Technology team to implement security controls and measures.

Infrastructure Systems and Support team (IT team)

The COO heads the IT team and is responsible for providing strategic direction to the IT team for managing and maintaining IT infrastructure of the organization for implementing technology strategy and IT related policies and procedures.

The IT team is responsible for the following:

- Maintaining workstations and servers;
- Maintaining network components and network connectivity within Anunta network;
- Access provisioning and revocation from domain, network devices and servers;
- Maintaining and updating the hardening guidelines for workstations, servers, and network devices;
- Configuring workstations, servers, and network devices in accordance with hardening guidelines;
- Conducting and coordinating Vulnerability Assessment (VA) and Penetration testing (PT);
- Resolving issues and observations identified during VA and PT exercise;
- Monitoring deployment of antivirus agents on workstations and servers;
- Monitoring the status of antivirus definitions on workstations and servers;
- Implementing infrastructure related changes within Anunta environment; and
- Monitoring resolution of IT incidents on a timely basis.

HR Team

The Head – HR leads the HR team and is responsible for providing strategic direction to the HR team and managing human capital of the organization. HR team is responsible for:

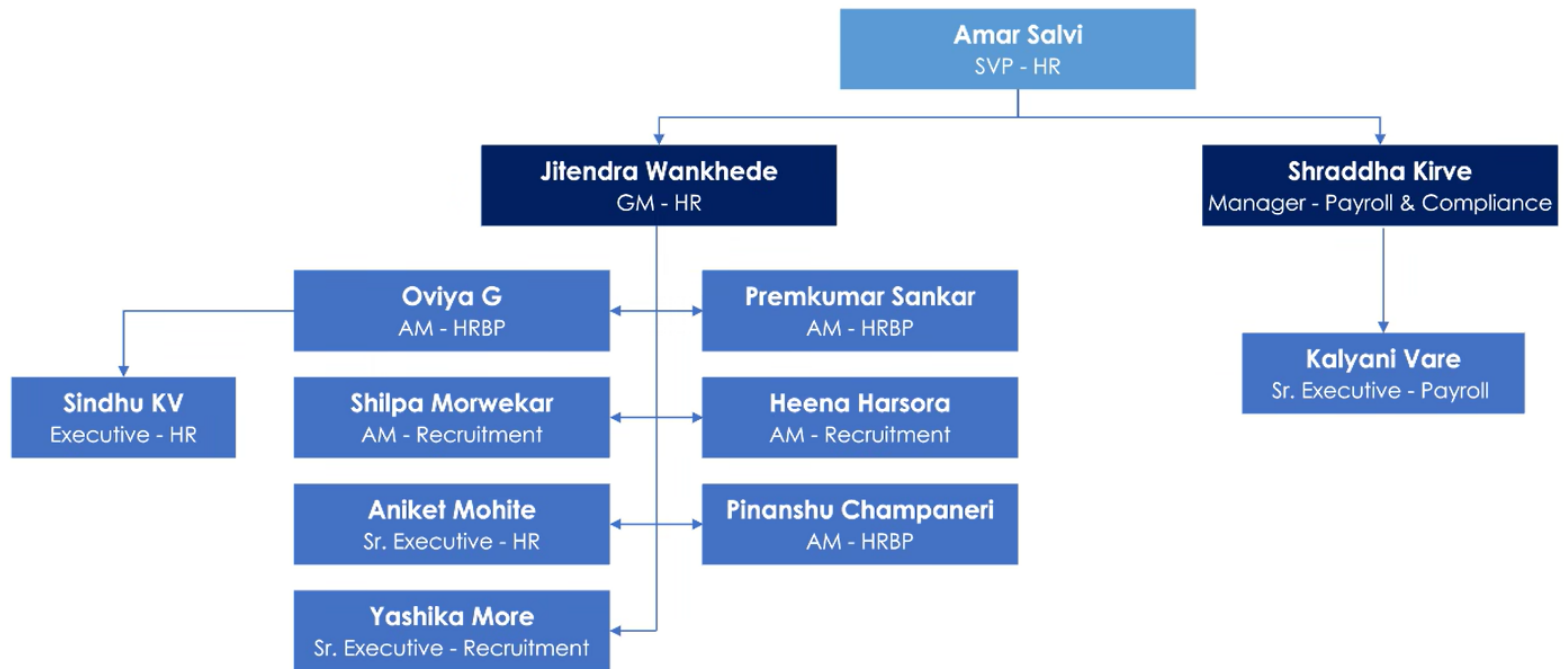
- conducting background verification for recruits;
- conduct induction training for new joiners;
- managing employees transfer and separation;
- driving employee development, welfare, and performance management programs;
- documenting job descriptions for key designations; and
- maintaining employee records.

Talent Acquisition Group (TAG) Team

The Head – TAG leads the TAG team and is responsible for providing guidance for hiring resources as per project / department requirement for the organization. TAG team is responsible for preparation of recruitment plan, shortlisting candidates, scheduling interviews, issuance of offer letters and collection and submission of Background Check (BGC) documents.

Listed below is the HR organization structure:

HR – Org Structure



Admin and Facility Team

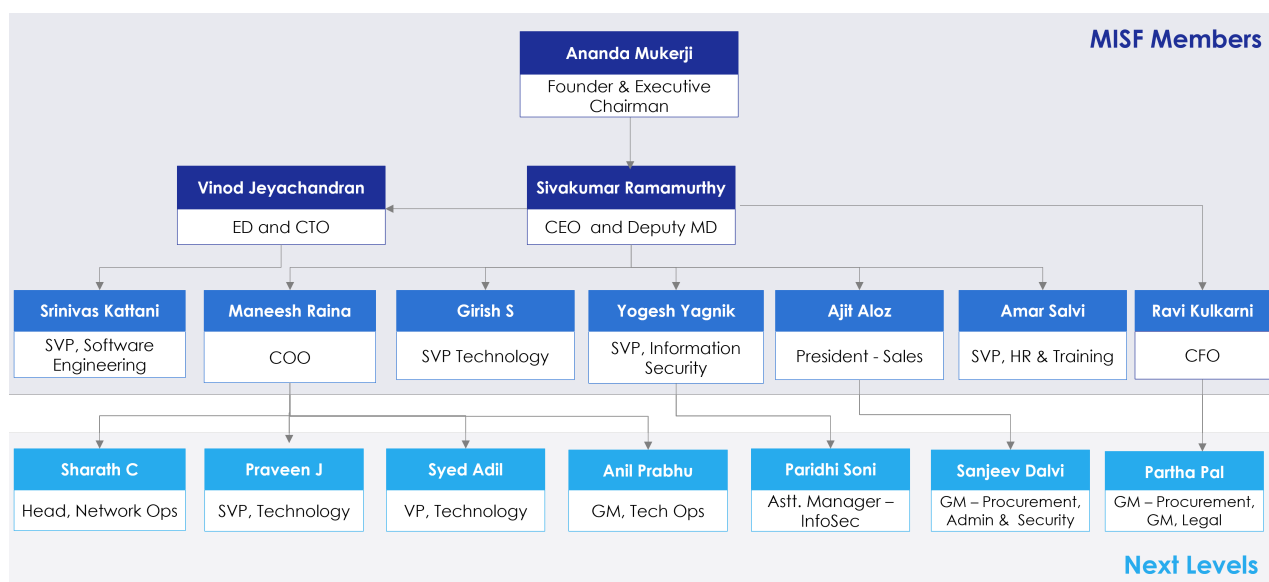
The Head – Facility is responsible for providing strategic direction to the facility team for managing physical infrastructure and managing logistics. Facility team is responsible for:

- implementing physical access processes;
- monitoring entry / exit within premises;
- maintaining adequate environmental protection controls;
- conducting fire drills and managing and maintaining physical assets; and
- granting and revoking physical access to office premises and client restricted areas.

Information Security Executive Committee

An Executive Committee is responsible for to oversee information security compliance, data privacy compliance and risk related matters is in place to ensure comprehensive governance in this area. This committee is also responsible to provides inputs and direction for security and privacy initiatives in the organization.

Listed below is the organization chart of Information Security Executive Committee.



Roles and Responsibilities

As per their roles and job responsibilities, the following team may involve in development of code, offering services and support to Anunta's clients and may have access to production environments. The teams mentioned below are in scope of this report.

Team	Responsibilities
<ul style="list-style-type: none"> • NOC Monitoring Services (EUEM) • Network Services • Telecom and WAN Support • Server Support Services • End User Support Services (EUC) 	<ul style="list-style-type: none"> ○ Incident and Problem management ○ Service request management ○ Change management ○ Patch management ○ Asset management ○ Configuration and back up management ○ Capacity and Demand management ○ DR/BC management ○ Service availability management ○ Vendor management ○ Infrastructure monitoring ○ Log management and review ○ IT Documentation ○ Service design and Project plan ○ Service improvement
<ul style="list-style-type: none"> • Centralized Support Desk (CSD) 	<ul style="list-style-type: none"> ○ Service request/ticket recording, classification, and prioritization ○ Service request tracking and closure
<ul style="list-style-type: none"> • IT Asset Management 	<ul style="list-style-type: none"> ○ IT asset inventory ○ IT asset classification ○ IT asset life cycle management
<ul style="list-style-type: none"> • IT Supplier Management 	<ul style="list-style-type: none"> ○ Third party staffing ○ Supplier relationship management
<ul style="list-style-type: none"> • Incident, Problem and Change Management Services 	<ul style="list-style-type: none"> ○ Prioritized incident management ○ Problem management ○ Change management
<ul style="list-style-type: none"> • Software Development and Maintenance 	<ul style="list-style-type: none"> ○ Software designing, development, testing, implementation, maintenance, and support
<ul style="list-style-type: none"> • Human resource, Recruitment and Training 	<ul style="list-style-type: none"> ○ Human Resource recruitment ○ Onboarding ○ Orientation, Training and Awareness ○ Payroll and appraisal ○ Offboarding ○ HR lifecycle management
<ul style="list-style-type: none"> • Administration and Physical Security 	<ul style="list-style-type: none"> ○ Physical security management ○ Visitor management ○ Office equipment management such as CCTV, Generator, UPS, Access control, Fire control etc. ○ Material movement ○ Procurement and supplier relationship ○ Coordination with building management system ○ Fire drills ○ Building management
<ul style="list-style-type: none"> • Management Information Services (MIS) 	<ul style="list-style-type: none"> ○ Service request analysis ○ Service reporting
<ul style="list-style-type: none"> • Centre of Excellence (CoE) and Project Management (PMO) 	<ul style="list-style-type: none"> ○ Project management ○ Service design ○ Service transition ○ Release and deployment management
<ul style="list-style-type: none"> • Information Security 	Designing, Implementation, Management and Governance of frameworks such as ISO 27001, ISO 27701, ISO 20000, SOC2

Commitment to competence

Anunta's formal job descriptions outline the responsibilities and qualifications required for each position in the company. Training needs are identified on an ongoing basis and are determined by current and anticipated needs of business. Employees are evaluated on an annual basis to document performance levels and to identify specific skill training needs.

Assignment of Authority and Responsibility

Management is responsible for the assignment of responsibility and delegation of authority within Anunta.

Human Resources Policies and Procedures

Anunta maintains written Human Resources Policies and Procedures. The policies and procedures describe Anunta practices relating to hiring, training and development, performance appraisal and advancement and the termination. Human Resource ('HR') policies and practices are intended to inform employees on topics such as expected levels of integrity, ethical behaviour and competence.

The Human Resources department review these policies and procedures on periodic basis to ensure they are updated to reflect changes in the organization and the operating environment. Employees are informed of these policies and procedures upon their hiring and sign an acknowledgement form confirming their receipt. Personnel policies and procedures are documented in the Anunta Human Resources Policy.

New Hire Procedures

New employees are required to read Anunta's corporate policies and procedures and sign or acknowledge form stating that they have read and understand them. Hiring procedures require that the proper educational levels have been attained along with required job-related certifications, if applicable, and industry experience. If a candidate is qualified, interviews are conducted with various levels of management and staff.

Background and reference checks are completed for prospective employees within one month to employment by third party specialized in this. Employees are required to sign Employee Confidentiality Agreement and are on file for employees. Discrepancies noted in background investigations are documented and investigated by the Human Resources Department in conjunction with a third-party verification agency. Any discrepancies found in background investigations result in disciplinary actions, up to and including employee termination.

Training and Development

On an ongoing basis, Anunta examines its training and development needs from a business standpoint, both in terms of current needs either internal or customer driven. Anunta compares these needs to the current skills held by its employees. On an as-needed basis, Anunta may select certain employees to receive additional training to meet the current and anticipated needs of the organisation. Anunta also offers regular trainings prepared in-house to undertake trainings on a periodic basis on relevant topics. These trainings are attended by all technical employees of the specific department the training belongs to.

Performance Evaluation

Anunta has a performance review and evaluation program to recognize employees for performance and contributions. Anunta performance evaluation process is also used to help employees improve their performance and skill levels. Employees performance reviews, promotion and compensation adjustment are performed every 12 months. The performance evaluation is reviewed with the employee and signed by the employee, their manager.

New Employee Training

HR coordinates to provide information security awareness program to all employees as part of induction. HR maintains the records of information security awareness training namely attendance sheets and feedback forms from employees. Employees undergo security awareness training regularly.

Employee Refresher Training

All employees of Anunta and where relevant third-party users and contractors receives information security and data privacy trainings annually as per their job roles. Annual refresher training, awareness and educations ensure the coverage of organization information security polices, acceptable use of resources, data privacy, information security incident reporting and consequences of noncompliance as per disciplinary action to ensure users are aware of the security practices to safeguard information and information systems they handle.

Employee Terminations

Termination or change in employment is being processed as per Anunta HR related procedures. There are clearly identified and assigned responsibilities with regard to termination or change in employment.

All employees, contractors and third-party personnel are required to return physical and digital Identification/access tokens provided to them by Anunta or its clients on their termination of employment or contract.

Access privileges are revoked upon termination of employment, contract or agreement. In case of change of employment /role, rights associated with the prior roles are removed and new access privileges are created as appropriate for the current job roles and responsibilities.

Ethical Practices

Anunta reinforces the importance of the integrity message, and the tone starts at the top. Every employee, manager and director consistently maintain an ethical stance and support ethical behaviour. Employees at Anunta encourage open dialogue, get honest feedback, and treat everyone fairly, with honesty and objectivity.

Code of Conduct and Disciplinary Action

Anunta has put forward Code of Conduct and Disciplinary Process in-order to encourage and maintain standards of conduct and ensure consistent and fair treatment for all. Anunta employee whose conduct does not comply with an element of the code of conduct and has been found to have breached the Code is prosecuted as per defined process.

Procedures

IT policies and operating instructions are documented. Procedures described cover server management, server hardening, workstation security system, network management, security patch management, user creation, system audit, ID card activation, etc. Additionally, production and training standard operating procedures are available.

Help Desk

Anunta has put in place a helpdesk function that function out of the IT Department and an integrated helpdesk to handle problems and support requirements of users, support users in case of incidents and manage them without disruption to Anunta business and ensures that changes to any component of Anunta's information assets and infrastructure are controlled and managed in a structured manner.

All requests received at the Help Desk are classified as to their criticality and resolved within the maximum resolution time as detailed in the Anunta Help Desk, Change Management and Incident Response Procedure.

Change Management

Anunta has implemented a well-defined Change management process to ensure that all changes to the information processing facilities, including equipment, supporting facilities and utilities, networks, application software, systems software and security devices are managed and controlled. The Change Management process describes a methodical approach to handle the changes that are to be made to any work product. All the changes need to be subjected to a formal Change Management process.

Incident Response and Management

Procedures for the incident response including identification and escalation of security breaches and other incidents are included in the policy. Users or any other person log all incidents to the Helpdesk. The help desk personnel study and escalate all security incidents to the designated team for further escalation/resolution. Any event related to security of Information assets including facilities and people are termed as an Incident.

When an incident is detected or reported, a defined incident response process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures. Root-cause analyses of all the incidents are performed and the root cause identified shall remedy and reported. The actions proposed from the root-cause analyses are approved.

Logical Access

Security Authorization and Administration

Email is sent from HR to IT helpdesk for all new employees for a new workstation configured with minimum default access to company resources/applications required by an employee to perform the job duty. The default access levels for different departments are defined and documented in HR/Admin policy manual. Any additional access is recommended by the line manager and approved. Company has standard configuration that is implemented across Desktops & laptops individually.

Only the IT team has access to change user profile or give higher access. Other employees do not have local admin privileges on their desktops, only IT team has access to install software on employees' machines. The ability to create or modify users and user access privileges is limited to the IT team.

Access to resources is granted to an authenticated user based on the user's identity through a unique login ID that is authenticated by an associated password. Assets are assigned owners who are responsible for evaluating the appropriateness of access based on job roles. This is documented in Access Control Matrix.

Roles are periodically reviewed and updated by asset owners regularly. Privileged access to sensitive resources is restricted to IT team. Access to storage, backup data, systems, and media is limited to IT team through the use of physical and logical access controls.

Security Configuration

Employees establish their identity to the local network and remote systems through the use of a valid unique user ID that is authenticated by an associated password. Use of encrypted VPN channels help to ensure that only valid users gain access to IT components. Remote access is not permitted to any employee.

Passwords are controlled through Password policy and include periodic forced changes, password expiry and complexity requirements. User accounts are disabled after a limited number of unsuccessful logon attempts; the user is required to contact the IT Support team to reset the password. Local users do not have access to modify password rules. Guest and anonymous logins are not allowed on any machines. Local administrator privilege is restricted to the IT Support Team and is

not available to other users. However, where the project need the team members to have the local admin access, respective line manager will raise a request to senior management which can approve or deny the request based on its merit.

Unattended user workstations are locked within a time of inactivity. Users are required to provide their password to unlock the desktop/laptop.

Administrative Level Access

Administrative rights and access to administrative accounts are granted to individuals that require that level of access in order to perform their jobs. All administrative level access, other than to IT team, must be justified to and approved.

Out Bound Communication

Anunta development Applications are accessible in Anunta Network. For uploading the files and communication to the client, external internet access is required. Internet usage is restricted with CISCO firewall. The IT Team periodically reviews and recommends changes to web and protocol filtering rules. Human Resources review these recommendations and decide if any changes are to be made.

Confidentiality

Access to data is restricted to authorized applications through access control software. No confidential customer related data is stored by network team in office network.

All agreements with related parties and vendors include confidentiality commitments consistent with company's confidentiality policy (as described in IT and Security Policies).

Secure procedures are established to ensure safe and secure disposal of media when no longer required. The level of destruction or disposal of media would depend on the information or data stored in the media and the criticality of the information as per the information classification guideline.

Backup and Recovery of Data

Anunta has developed formal policies and procedures relating to back up and recovery. Backup policy is defined in the Backup Policy. Suitable backups are taken and maintained.

Anunta has put in place backup processes that define the type of information to be backed up, backup cycles and the methods of performing backup. The backup media are tested for restoration on a periodic basis to ensure the effectiveness and integrity of backup.

The backup processes are approved by the business owners and comply with the requirements for business continuity, and legal & regulatory requirements. All backup and restoration logs are maintained for retention periods as defined in the backup procedures.

All backup copies are tested periodically to ensure that the data and information are securely retrievable in the event of an emergency without any loss of information. Users are made aware through adequate training their responsibilities for ensuring backup of required data and information.

Data Restoration Procedure

Restoration is done in two cases – primary case is when a Anunta member makes a request to recover some data that they might have lost. The other case when a restoration test is done is during our regular DR test. The relevant IT personnel (i.e., the backup administrator) ensures that the data is restored appropriately.

Applicable Trust Services Criteria and related Controls

The security, availability, confidentiality, and processing integrity trust services categories and Anunta related controls are included in section 4 of this report, "Independent Service Auditor's Description of Tests of Controls and Results".

User- Entity Control Considerations

Services provided by Anunta to user entities and the controls of Anunta cover only a portion of the overall controls of each user entity. Anunta controls were designed with the assumption that certain controls would be implemented by user entities. In certain situations, the application of specific controls at user entities is necessary to achieve relating to the services outlined in this report to be achieved solely by Anunta. This section highlights those internal control responsibilities that Anunta believes should be present for each user entity and has considered in developing the controls described in the report. This list does not purport to be and should not be considered a complete listing of the controls relevant at user entities. Other controls may be required at user entities.

- **Contractual Arrangements**
 - User organizations are responsible for understanding and complying with their contractual obligations to Anunta such as providing input information, review and approval of processed output and releasing any instructions.
- **Other Controls**
 - User Organizations are responsible for ensuring end customer privacy.
 - User Organizations are responsible for ensuring that complete, accurate and timely information is provided to Anunta for processing.
 - User Organizations are responsible for their network security policy and access management for their

networks, application & data.

- User Organizations are responsible for working with Anunta to jointly establish service levels and revise the same based on changes in business conditions
- User Organizations are responsible for implementing sound and consistent internal controls regarding general IT system access and system usage.
- User Organizations are responsible for implementing controls to remove user access for terminated users and who were involved in services associated with Anunta services
- User Organizations are responsible for implementing controls necessary to ensure that transactions relating to Anunta services are appropriately authorized, timely, and complete.
- User Organizations are responsible for ensuring that any data sent to Anunta should be protected by methods to ensure confidentiality, privacy, integrity, availability.
- User Organizations are responsible for logging any complaint, service disruption, or security incident with Anunta
- User Organizations are responsible for reviewing specific SLA reports and hold meetings jointly with Anunta
- User Organizations are responsible for ensuring restricted access control to Anunta applications and systems. In particular, Anunta is responsible to provide complete and accurate access requests during the onboarding process.
- User Organizations are responsible for approving any change requests, releases or UAT sign off on Anunta initiated changes
- User Organizations are responsible for ensuring that input data is provided by them as per the process agreed with Anunta and using the secure HTTPS/SFTP or other secure connections and mechanisms.
- User Organizations are responsible for ensuring that clear instructions are provided to Anunta as part of the onboarding process and project setup.

End of Report