LeapSwitch Networks Private Limited

System and Organization Controls (SOC 3®) Report

Description of its Infrastructure as a Service (IaaS) and Bare Metal as a Service relevant to the Trust Services Criteria of Security, Availability and Confidentiality

August 1, 2025 through June 30, 2026

STATEMENT OF CONFIDENTIALITY

This report is intended solely for the information and use of LeapSwitch Networks Private Limited, user entities of LeapSwitch's Infrastructure as a Service (IaaS) and Bare Metal as a Service during some or all of the period August 1, 2025 through June 30, 2026, and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the nature of the services provided by LeapSwitch, the trust services criteria relevant to security, availability and confidentiality, and the risks that may threaten the achievement of LeapSwitch's service commitments and system requirements. This report is not intended to be and should not be used by anyone other than these specified parties. Unauthorized use, reproduction or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

1 Independent Service Auditors' Report..... 5
2 Management Assertion Provided by LeapSwitch Networks Private Limited..... 9
3 Description of Systems Provided by the Service Organization..... 12

SECTION 1

INDEPENDENT SERVICE AUDITORS' REPORT

1 INDEPENDENT SERVICE AUDITORS' REPORT

To the management of LeapSwitch Networks Private Limited

Scope

We have examined the accompanying assertion of Management of LeapSwitch Networks Private Limited (the "Service Organization" or "LeapSwitch") related to its Infrastructure as a Service (IaaS) and Bare Metal as a Service titled "Description of systems provided by the Service Organization" (the "Assertion") that the controls within LeapSwitch's in-scope services ("system") were effective throughout the period August 1, 2025, to June 30, 2026, to provide reasonable assurance that LeapSwitch's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. LeapSwitch's principal service commitments and system requirements are presented in Section 3.

LeapSwitch uses the Data Centre services of YOTTA and L&T (Subservice Organizations). Certain service commitments and system requirements based on the applicable trust services criteria can be met only if certain types of controls that management expects to be implemented at the subservice organizations are suitably designed and operating effectively. The Description of the Boundaries of the LeapSwitch System presents the types of complementary subservice organization controls assumed in the design of the Service Organization's controls. Our examination did not include the services provided by the subservice organizations, and we have not evaluated whether the controls management expects to be implemented at the subservice organizations have been implemented or whether such controls were suitably designed and operating effectively throughout the period August 1, 2025, to June 30, 2026.

Complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at LeapSwitch, to achieve LeapSwitch's service commitments and system requirements based on the applicable trust services criteria. The Description of the Boundaries of the LeapSwitch System presents the complementary user entity controls assumed in the design of LeapSwitch's controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

LeapSwitch 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 LeapSwitch's service commitments and system requirements were achieved. Management of LeapSwitch has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, LeapSwitch is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountant's Code of Ethics for Professional Accountants. We have complied with those requirements. We applied the Statements on Quality Control Standards as established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within the Service Organization's system were effective throughout the period August 1, 2025, to June 30, 2026, if complementary subservice organization and user entity controls contemplated in the design

of the Service Organization's controls operated effectively, to provide reasonable assurance that LeapSwitch's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Accorp Partners CPA LLC

ACCORP PARTNERS CPA LLC
License No.: PAC-FIRM-LIC-47383
Kalispell, Montana
Date: August 31, 2026

SECTION 2

MANAGEMENT'S ASSERTION PROVIDED BY SERVICE ORGANIZATION

Management Assertion of LeapSwitch Networks Private Limited

We are responsible for designing, implementing, operating and maintaining effective controls within LeapSwitch Networks Private Limited ('LeapSwitch') related to the Infrastructure as a Service (IaaS) and Bare Metal as a Service throughout the period August 1st, 2025 to June 30th, 2026, to provide reasonable assurance that LeapSwitch's service commitments and system requirements relevant to security, availability and confidentiality were achieved. Our description of the boundaries of the system is presented in Section 3 and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period August 1st, 2025 to June 30th, 2026, to provide reasonable assurance that LeapSwitch's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality ("applicable trust services criteria") set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). LeapSwitch's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section 3.

The Service Organization uses YOTTA and L&T facilities ("subservice organizations") for its Data Centre services. Complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at LeapSwitch, to achieve LeapSwitch's service commitments and system requirements related to the Infrastructure as a Service (IaaS) and Bare Metal as a Service based on the applicable trust services criteria. The accompanying Description of the Boundaries of Infrastructure as a Service (IaaS) and Bare Metal as a Service presents the types of complementary subservice organization controls assumed in the design of LeapSwitch's controls. The actual controls at the subservice organizations are not disclosed.

Complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at LeapSwitch, to achieve LeapSwitch's service commitments and system requirements related to the Infrastructure as a Service (IaaS) and Bare Metal as a Service based on the applicable trust services criteria. The accompanying Description of the Boundaries of Infrastructure as a Service (IaaS) and Bare Metal as a Service presents the complementary user entity controls assumed in the design of LeapSwitch's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period August 1st, 2025 to June 30th, 2026, to provide reasonable assurance that LeapSwitch's Infrastructure as a Service (IaaS) and Bare Metal as a Service commitments and system requirements were achieved based on the applicable trust services criteria.

For LeapSwitch Networks Private Limited



Authorized Signatory
Date: 31st August 2026

SECTION 3

DESCRIPTION OF THE SYSTEM

3 DESCRIPTION OF SYSTEMS PROVIDED BY THE SERVICE ORGANIZATION

3.1 Overview of service organization and in-scope services

Leapswitch Networks Private Limited (hereinafter referred to as 'LeapSwitch') located at Office 410, Spectra Commercial, Pratik Nagar, Paud Road, Pune – 411038 delivers a services since 2006 providing cloud hosting, cloud virtual servers, bare-metal dedicated servers, platform-as-a-service cloud and colocation services. We provide a reliable infrastructure for your websites with a 100% network uptime and power uptime guarantee. We operate out of 19 worldwide locations in 3 continents in 10 countries. We offer Robust Infrastructure in 19 locations worldwide. We embrace the digital journey of Enterprise and SMB Clients with our unique approach and innovative products serving 20000+ Customers.

Description of Services Offered

CORE BUSINESS SERVICES

a. CloudPe Platform (Infrastructure-as-a-Service - IaaS)

CloudPe is LeapSwitch's flagship cloud platform, designed to offer scalable, secure, and high-performance infrastructure solutions for businesses of all sizes.

Compute Services

- ***Virtual Machines (VMs):*** Customizable VMs with various configurations to meet diverse workload requirements.
- ***CloudPe GPU:*** High-performance GPUs suitable for AI, machine learning, and graphics-intensive applications.
- ***Kubernetes:*** Managed Kubernetes clusters for containerized application deployments.

Storage Solutions

- ***S3 Object Storage:*** Scalable object storage compatible with S3 APIs, ideal for storing unstructured data.
- ***Block Storage Volumes:*** High-speed block storage volumes that can be attached to VMs for persistent storage needs.

Add-ons

- ***Load Balancers:*** Distribute incoming traffic across multiple servers to ensure high availability and reliability.
- ***Firewalls:*** Advanced firewall configurations to protect against unauthorized access and threats.
- ***Virtual Private Cloud (VPC):*** Isolated network environments for enhanced security and control over resources.

b. Bare Metal Servers

Leapswitch offers bare metal dedicated servers that provide enhanced performance, security and control.

Specifications

- ***Hardware:*** Latest Intel/AMD processors with configurations up to 256 cores and 2TB RAM.
- ***Storage:*** Options include HDDs, SSDs, and U.3 NVMe drives.
- ***Network:*** Premium Tier 1 bandwidth ensuring low latency and high throughput.
- ***Access:*** Full root and IPMI access for complete control over the server environment.

C. Additional Services

a. Virtual Private Servers (VPS)

Leapswitch provides both managed and self-managed VPS solutions, offering flexibility and control.

- ***Managed VPS:*** Includes server management, monitoring, and support.
- ***Self-Managed VPS:*** Provides root access, allowing users to configure and manage the server independently.

b. Web Hosting

- ***Shared Hosting:*** Affordable hosting solutions with SSD storage and unlimited email accounts.
- ***Reseller Hosting:*** Enables clients to start their own hosting business with white-label solutions.

c. Business Email Solutions

Secure and reliable email hosting services suitable for businesses of all sizes.

d. Backup & Disaster Recovery

Ransomware-protected cloud backup solutions to ensure data safety and business continuity

3.2 Principal Service Commitments and System Requirements

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

LeapSwitch establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in LeapSwitch'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.

Provide highly available infrastructure, with redundant power, network, and cooling at all data centers. LeapSwitch Commit to 99.9% uptime SLAs for network connectivity and hardware availability. LeapSwitch empower customers with 24X7 support via call, chat, ticketing system and email.

3.3 Components of the System used to provide services

People

LeapSwitch staff provides support for the above services in each of the following functional areas:

Board of Directors - the Board of Directors' primary responsibility is to protect the shareholders' assets and ensure they receive a return on their investment. The Board meets regularly with our Founder & CEO and various members of our executive team.

Founder & CEO - making major corporate decisions, managing the overall operations and resources of a company, acting as the main point of communication between the board and corporate operations and being the public face of the company.

IT Team - responsible for provisioning and maintenance of IT infrastructure in LeapSwitch offices.

HR Team - responsible for hiring employees, personnel screening, termination, exit of employees, maintaining interoffice relationships, discipline.

Technical Team – Provides customer assistance by troubleshooting and resolving service-related issues.

Cloud Team – Manages and supports customers using LeapSwitch's cloud hosting and virtualization services.

Monitoring Team – Continuously monitors server uptime, performance, and infrastructure health to ensure service reliability.

Network Team (Infrastructure & Network Engineers) – Designs, manages and maintains the data center infrastructure, network connectivity, and security.

Sales Team – Engages with customers to understand requirements and deliver tailored hosting and infrastructure solutions.

Data

Leapswitch does not inspect, approve or monitor content of data that clients deploy their Infrastructure service provided by Leapswitch. Leapswitch does not claim data ownership over the client information entered or processed through its application/ systems that belong to clients only.

Procedures and Policies

Formal policies and procedures exist that describe logical access, information security, user data confidentiality, risk management and change management. All teams are expected to adhere to the LeapSwitch's policies and procedures that define how services should be delivered.

Boundaries of the System

Services in scope	LeapSwitch's Description of its Infrastructure as a Service (IaaS) and Bare Metal as a Service
Geographic locations in scope	Office 410, Spectra Commercial, Pratik Nagar, Paud Road, Pune – 411038
Scope Exclusion	• IaaS for Data Centre Hosting – Physical facilities (power, cooling, security) managed by third-party providers are excluded. • Customer-Managed Configurations – Configurations, applications and data managed directly by customers are excluded.

3.4 Relevant aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. This section provides information about the five interrelated components of internal control at LeapSwitch, including:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring controls

Control Environment

Management Philosophy

LeapSwitch's control environment reflects its management's philosophy concerning the importance of security in delivering its services. LeapSwitch's Information Security Committee meets half yearly to review the information security posture of the organisation. Information Security Steering Committee oversees the information security activities of LeapSwitch. The Security Committee members are from each of the business lines and support functions.

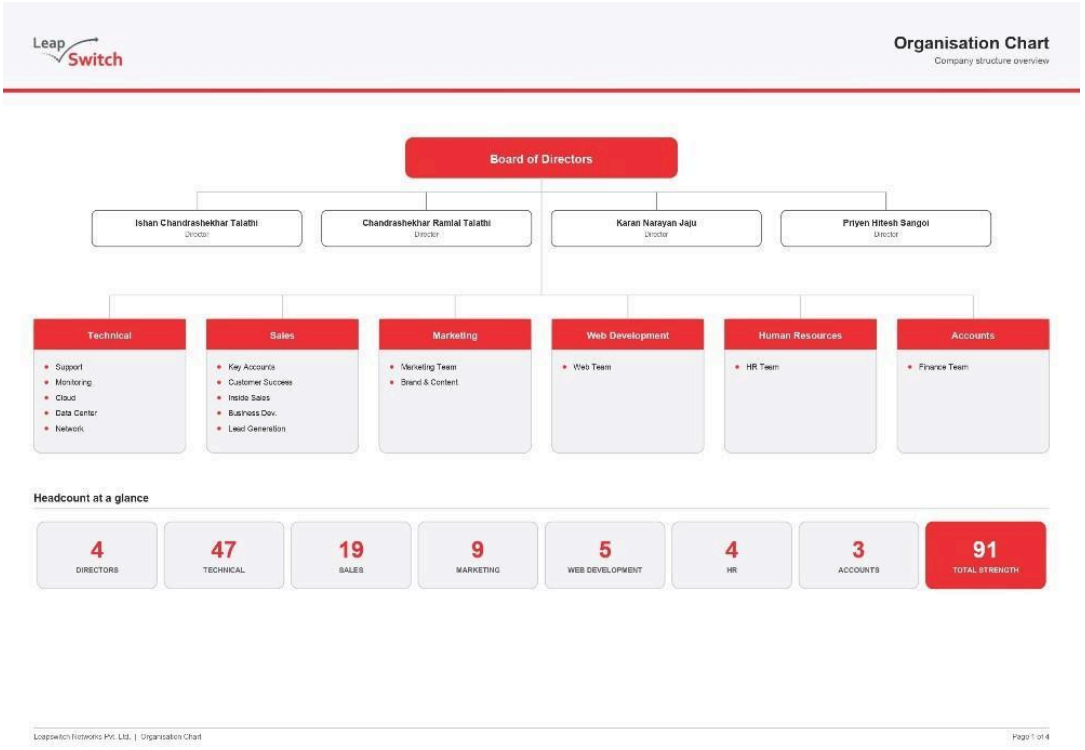
The Information Security Committee is charged with establishing overall security policies and procedures for LeapSwitch. The importance of security is emphasized within LeapSwitch through the establishment and communication of policies and procedures and is supported by investment in resources and people to carry out the policies. In designing its controls, LeapSwitch has taken into consideration the relevance of controls to meet the relevant trust criteria. To assist in LeapSwitch's efforts to protect and secure its information and those of its clients, it has adopted an Information Security Policy to work in concert with information security and confidentiality methods and procedures. In addition, key operating methods and procedures are documented. This information is presented in this report and further describes LeapSwitch's controls placed in operations.

LeapSwitch's control environment is a collaborative effort of multiple functions to establish and enhance controls and mitigate risks which the business may encounter. It reflects the commitment of management and its owners to maintain controls through policies and procedures and organizational structure.

LeapSwitch maintains a control environment with several elements including corporate structure, organization structure, personnel policies and procedures and other elements listed below.

Organizational Structure

LeapSwitch is organized into separate departments based on business roles and functions. Each of the members of the management team has a distinct, separate responsibility within the organization to promote an appropriate segregation of duties.



Management Oversight

LeapSwitch is governed by its board of directors and has ultimate responsibility for overseeing the policies and operations of the organization. The board and the senior management meet

periodically to discuss pertinent issues and provide guidance for the organization's direction and operations.

Personnel Policies and Procedures

LeapSwitch has standard hiring and termination policies and procedures. The procedures include screening potential employees through interview process, reference checks, formal offer letters and new employee training. Employee disciplinary procedure and Human Resource Policy have been implemented.

LeapSwitch also has developed a Non-Disclosure Agreement. Employees are required to sign the Non-Disclosure Agreement, acknowledging that they will adhere to company's policies and procedures. Policies relating to information security before hiring, during employment and on termination have been implemented as part of the Information Security Management System.

Employee Training

LeapSwitch conducts induction training for all new employees as part of the onboarding process and annual information security awareness training is provided to all staff, along with department-specific, role-based skill training delivered according to an established training calendar.

Risk Assessment Process

LeapSwitch recognizes the importance of risk management in properly managing corporate and client assets and providing high-quality, cost-effective services to its clients. It has placed controls into operation, risk assessment process to identify and manage risks that could affect their ability to provide reliable services for user organizations.

This process requires their senior management team to review the results of operations and meets regularly to identify any risks and develop and implement appropriate measures to address these risks. The risk assessment process focuses on analyses of threats, probabilities of occurrence, potential business impacts, and associated mitigation plans. The risk assessment process is an ongoing process as business operations, workflow, or technologies change. The senior management team provides management review and oversight of projects.

Control Activities

Description of the control activities is provided below.

Information Security Policies & Procedures

- LeapSwitch has developed organization-wide Information Security Policies.
- Domains within the IT and Security Policies include Access Control, Asset Management, Risk Assessment, Business Continuity Planning, incident management and Change Control.
- The organization policies, Information security related policies and procedures are made available for all the employees in the organization repository. All the employees have access to the policy and procedures. Whenever a new employee joins the organization, these processes form a part of the onboard induction.

- The Information Security Manager is responsible for overseeing information security and ensuring that security processes are continuously maintained and updated.
- All the information security related artefacts like the asset register are stored in a safe location. These would be used during the risk assessment activities and Information Security Committee

S.No	Document Name
1	Context of the organization
2	Information Security Policy Statement
3	Information Security Manual
4	Information Security Procedure Manual
5	End user acceptable use policy
6	Statement of Acceptance
7	Internal Audit procedure
8	Procedure for Corrective Action
9	Procedure for Continual Improvement
10	Document Control Procedure
11	Annual Internal Audit plan
12	BCP & DR Plan
13	Security Objectives
14	Risk Assessment Methodology
15	Roles, Responsibilities & Authorities
16	Communication Policy
17	Management Review Meeting Procedure
18	Whistle Blower Policy
19	Succession Planning

Change Management

LeapSwitch has a formal change control procedure in place. This change control procedure relates to the change control process for updating, replacing an existing information processing facility of LeapSwitch. This includes changes in IT infrastructure (hardware configuration changes, software configuration changes like OS upgrade, OS change, Vulnerability patch updating), facilities. Changes to bare metal server configurations or deployments within the data center are managed through a formal change management process. Changes are recorded in the change register.

Incident Management

An organization level incident register is maintained by the Information Security Manager, should a need arise. All incidents, as deemed appropriate, are logged in the incident register and are monitored by the Information Security Committee. Customers report incidents through Leapswitch's 24×7 support ticketing system via the client portal, with categorization

by department. Multi-channel support including live chat, telephone, and email is available to ensure timely escalation and resolution of incident.

Business Continuity and Backup

LeapSwitch has rolled out a Business Continuity Policy which serves as a guide to recovery teams.

Asset Management

LeapSwitch are equipped with the latest hardware, software and networking infrastructure. Offices are connected to the internet using high speed communication links, backed up by redundant networks. All employees are provided with laptops which are installed with end point protection software. The software and hardware assets are logged in an asset register and updated by the IT team members. Comprehensive asset register for bare metal servers is maintained for data centers to ensure accurate inventory tracking, ownership and accountability of physical infrastructure components. Movement of bare metal servers in and out of the data center is documented.

User Account Management

A formal user access provisioning process are implemented to assign or revoke access rights for all user types to all systems and services.

- LeapSwitch IT team after obtaining authorization from the owner of the information system or service, enables access for the use of the information system or service.
- Separate approval for special access rights must be needed from management.
- LeapSwitch IT team periodically verifies that the level of access granted is appropriate to the access policies and is consistent with other requirements such as segregation of duties.
- LeapSwitch IT team periodically reviews access rights with owners of the information systems or services based on business requirements.

The allocation and use of privileged access rights are restricted and controlled. The allocation of privileged access rights is controlled through a formal authorization process in accordance with the relevant access control policy.

Network Security Controls

LeapSwitch has implemented FortiGate and Sophos Firewall to protect business critical information from unauthorized access. IP whitelisting and port restrictions are configured in the ACL. Separate logical networks are established to isolate infrastructure administrative functions from the operation of management consoles. A structured and secure network architecture has been developed and implemented for the data centers incorporating core components such as routers, TOR switches, firewalls, IPMI switches, and server racks to ensure high availability, controlled access and reliable data flow across the infrastructure.

Physical and Environmental Security

Physical access into the facility of LeapSwitch is monitored through video surveillance by security guards. Access is controlled through the use of access device systems. Access to the work areas is limited to authorized personnel based on job function, and physical security access permissions are reviewed monthly by the administration team. LeapSwitch has deployed air conditioning systems, fire extinguishers and environmental monitoring systems.

Personnel Security

Background checks are performed on new employees. Employees are required to sign a non-disclosure agreement on joining the organisation. The new positions are supported by job descriptions. Once employed, employees are subject to LeapSwitch’s procedures for accessing systems and sanctions for violating LeapSwitch’s information security policy. Employees are educated on incident reporting procedures for prompt reporting of any security incidents. At the time of exit, Human Resources Department ensures that all assets are returned and access to information assets have been terminated through email confirmation.

Monitoring Controls

LeapSwitch’s senior management and supervisory personnel monitor the quality of internal control performance as a normal part of their daily activities. To assist in this monitoring, management has established Key Performance Indicators reporting specifically designed to report on information security objectives. LeapSwitch also has an internal audit program whereby internal audit of Information Security Management System is being conducted at least once a year. The Zabbix monitoring tool is installed to manage the performance, availability, and health of its managed services customers' infrastructure and systems. In the event of bare metal server downtime or hardware failure, necessary spare parts are maintained in stock and a dedicated support team is available to ensure timely repair and restoration of services.

Information and Communication Systems

LeapSwitch has an information security policy and a communication policy to help ensure that employees understand their individual roles and responsibilities concerning information security. LeapSwitch also has an incident management procedure to ensure significant events are communicated in a timely manner. LeapSwitch business continuity policy provides for process relating to communication of any incident impacting the business continuity. Information Security Management System implemented at LeapSwitch includes formal and informal training programs and the use of email to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems.

Changes in System During the Review Period

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Incidents in the Last 12 Months

No significant incidents have occurred impacting the service environment in the 12 months preceding the end of the review period.

3.5 Applicable Trust Services Criteria

The applicable trust service criteria controls included in this report are Security, Availability and Confidentiality. The controls in LeapSwitch have been designed and implemented to meet each of the criteria stated above and help the reader of this report with information sufficient to understand the basic structure of controls within LeapSwitch. This report, when coupled with an understanding of controls in place at user locations, is intended to permit evaluation of the total system of internal control surrounding the reviewed systems.

3.6 Complementary User Entity Controls

LeapSwitch’s controls are designed with the assumption that certain controls will be implemented by client/ user organizations. In certain situations, the application of specified internal controls at user organizations is necessary to achieve certain confidentiality, security, and availability trust services criteria included in this report.

The following is a representative list of controls that are expected to be in operation at client/user organizations to complement the controls of LeapSwitch (this is not a comprehensive list of all controls that should be employed by the user organizations):

- User entities are responsible for enforcing strong authentication and authorization for all users
- User entities are responsible for Operating system and software security for Installing, configuring and hardening the OS, middleware, databases, and applications running on the bare metal servers.

- User entities are responsible for applying security patches and updates in a timely manner on the bare metal servers.
- User entities are responsible for remote consoles, client VPNs, or administrative access methods are secured against unauthorized use.
- User entities are responsible for availability & redundancy for configuring clustering, load balancing, or failover at the application/system level if required.
- User entities are responsible for Testing and approving system/application changes prior to production deployment.
- User entities are responsible for data encryption at rest and transit
- User entities are responsible for any third-party applications or integrations installed on bare metal systems comply with security best practices.
- User entities are responsible for system monitoring like server performance, uptime, and resource usage (CPU, memory, disk, bandwidth)

3.7 Complementary Subservice Organization Controls

In order to provide its services, LeapSwitch utilizes the Data Centre services of YOTTA and L&T. YOTTA and L&T are SOC2 Type 2 compliant. Responsibilities of Data Centre services includes implementing physical security and availability controls to restrict access to the facility which houses the in-scope system. The scope of this report does not include the Data Centre services and related controls provided by YOTTA and L&T.

LeapSwitch's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to LeapSwitch's services to be solely achieved by LeapSwitch control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of LeapSwitch

The following subservice organization controls should be implemented by YOTTA and L&T and its subservice organizations to provide additional assurance that the trust services criteria described within this report are met.

Subservice Organization	Service Provided
YOTTA	Data Centre services
L&T	Data Centre services

Subservice Organization – YOTTA		
Category	**Criteria**	**Control**
Common Criteria - Security	CC6.4- The entity restricts physical access to facilities and protected information assets (for example, DC, facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	There exists a Physical Access Control Policy that describes the process for controlling physical access to the facilities and server hall. This document is reviewed and approved by the Head DC security and safety.
		Employees' and visitors' access to premises is restricted using access cards. Access to general and restricted areas within premises is granted after receiving

Subservice Organization – YOTTA		
Category	**Criteria**	**Control**
		approval from authorized personnel of Yotta.
		Employees access to server hall is restrict to authorized employees using biometric access control system and mantrap. DC Operations team grants the access to server hall based on the approval from DC Security team
		Visitors and vendors requiring access to data centre are issued identification badge and escorted by authorized DC Security team personnel.
		On a Quarterly basis restricted area access reports are generated and shared with the designated owner for the premises for review. Any discrepancies noted are tracked to closure.
		At the time of separation from the organization, employee's and contractor's ID cards and access cards are returned to the security department, and access to the premises is disabled within 24 hours of the last working day.
		Data centre facilities are secured by power fence at the perimeter, full height turnstiles at the entry gate and security guards are stationed at entry and exit point to monitor movement of employees and visitors.
		Dedicated zones are defined for each area allowing only authorized personnel to access specific areas
		Employees, visitors and contractors are issued unique lanyards based on the type of the visitor at the time of entry.
		At the facilities entry point vehicles and personal belongings are scanned.
Availability	A 1.1- The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	The management has established a process for maintaining redundancy of network components.
		There exists a policy and procedure document for capacity management which defines the process to be followed for monitoring and planning and asset capacity. This policy and procedure document are reviewed by Yotta senior management on an annual basis.
		Zabbix application is utilized to monitor availability, system performance and health and generate alerts when specific

Subservice Organization – YOTTA		
Category	**Criteria**	**Control**
		predefined thresholds are breached and corrective actions are taken by respective team.
		Event logs for infrastructure devices are logged within the SIEM application. Ruleset is defined in the SIEM system. Security incidents are notified to the IT team through e-mail communication and corrective actions are taken to resolve the incidents.
	A1.2- The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	CCTV cameras are installed at the entry and exit points of the premises and critical areas. The video surveillance is reviewed on a real time basis, recordings are retained for a minimum period of 90 days and reviewed by the Administration team.
		Environmental protections have been installed at Yotta include the following: • Cooling systems • Smoke detectors • Sprinklers • Fire Extinguisher • Battery and diesel generators • UPS • Fire Alarm
		Environmental protections receive periodic maintenance as per defined schedule for each equipment.
		Management has implemented detection controls to identify environmental anomalies.
		Secondary backup of power supply is installed to be utilized in case of power failure.
		The DC Operations team performs monitoring of temperature for network and UPS rooms during each shift.
		Yotta has a defined Backup Management procedure specifying the backup process to be followed for key applications and servers. The policy is reviewed and approved by Head Storage and Backup on an annual basis.
		Data backups are performed for key applications and servers as per pre- defined schedules.
		Data backups are monitored for successful completion and any errors/failures are tracked to closure. Only authorized employees are allowed to modify backup.

Subservice Organization – YOTTA		
Category	**Criteria**	**Control**
		Ticket is raised in the Tussom application in case of backup failures.
		Backup media tapes are transferred to the offsite storage location on monthly basis and backup transfer records are recorded and documented by the authorized IT team personnel in the ticket raised on Tussom application.
		Backup restoration testing is performed by the Yotta team upon request. The restoration test results are reviewed by the respective Team lead and exceptions identified are followed up through the problem management process.

Subservice Organization – L&T		
Category	**Criteria**	**Control**
Common Criteria - Security	CC6.4- The entity restricts physical access to facilities and protected information assets (for example, DC, facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Entity has documented Physical Access Security Policy governing access by employees / Vendors / Customers.
		All entry points to L&T Data centers are restricted to authorized personnel. These also include any delivery and loading areas as well. Multiple layers of access control security is maintained based on sensitivity. •Main gate entry and access is controlled by the building security team on a 24x7 basis with guarded manpower at each security post. •Boom barrier at main entry of datacenter building •Metal door frame at ground entrance •Turnstile at the DC entrance and security reception •Baggage scanner at reception •The building premises are under 24x7 CCTV surveillance. • 2 factor authentication using Biometric and access control at server hall doors. •Separate material loading entry gate with physical security and CCTV surveillance. •Security Team at reception is equipped with a hand-held metal detector. •Lock and keys for racks and cabinets
		Physical access to office premises is monitored through CCTV installed at key points within the premises.

Subservice Organization – L&T		
Category	**Criteria**	**Control**
		All visitors have to enter their details in the visitor register.
		Visitor cards have access to the common areas only and do not permit access to any secured areas of the facility.
		All visitors need to be pre-authorized with intimation at the gate and required to sign in and are escorted by authorized personnel when accessing the facility.
		ID cards that include an employee picture must be worn at all times when accessing or leaving the facility. No photo ID card is issued to any Vendor or Customer.
		Physical access is setup by the DC physical security team for new joiners after all HR formalities are completed. DC HR team/ HOD sends email for new joiner to DC manager to request physical access creation for the new joiner. Based on that, DC manager instructs DC physical security team to grant physical access. Access request form is filled by the new joiner which is approved and signed by the DC manager. ID cards by default does not have access to any of the sensitive areas.
		Colocation data halls and restricted rooms are physically segregated and require special privileges via the Access control and Biometric system. Customer racks are provided with locks. Keys are securely maintained by Facilities team and a key register is maintained showing when keys are used. Access to such restricted zone is given against written request.
		A monthly review of physical access to sensitive areas against active employee list is planned to be carried out by IT.
		Upon the last day of employment, HR Team/ HOD sends exit email requesting for deactivation of physical access to DC manager for terminated employees. e

Subservice Organization – L&T		
Category	**Criteria**	**Control**
		Physical access is deactivated by the DC physical security team.
		Employees are required to return their ID cards on the last day to Head office (HO) Admin team, and all ID cards are shredded.
		On a half yearly basis, physical security team performs a reconciliation that physical access for terminated employees has in fact been deactivated in the physical access system. The review and reconciliation is planned to be performed on monthly basis.
		Contractors are provided access cards in accordance with the contractor / vendor access policy after completing onboarding process and after approval from DC manager.
		The sharing of access badges and tailgating are prohibited by policy.
		Mantraps are used for controlling access to highly sensitive facilities.
Availability	A 1.1- The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	L&T DC monitors system processing capacity and usage and takes correction actions to address changing requirements. L&T DC utilizes various tools and sensor systems such as BMS and OEM to monitor physical security and environmental controls including access, fire panel, CCTV, energy consumption, power, temperature and humidity on 24x7 basis through its control room
		L&T data centers are Tier III certified and have been built with additional redundancy. All critical infrastructure components such as power supply, electrical circuits, power backups (UPS, DG set), carrier network circuits, power feeds at racks, and cooling have been provided a secondary system for maximum redundancy. Firewalls in high availability mode, multiple ISPs have been provided for L&T DC internal network redundancy.
	A1.2- The entity authorizes, designs, develops or acquires, implements,	Entity has documented environmental maintenance procedures that define DC operations and maintenance are

Subservice Organization – L&T		
Category	**Criteria**	**Control**
	operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	performed as per defined process and frequency.
		The following environmental controls exist to ensure protection of the L&T data centers a. Fire alarm, fire suppression and life safety system b. multi-zone VESDA detection system c. N+1 UPS and DG set d. Adequate lighting and PAC (Precision Air Conditioner) in data center e. Hydrogen & CO2 level monitoring f. WLD cables for water leakage detection g. Flood control, Rainwater recharging Pits, water collection Pond setup, drainage of excess water through dewatering pumps h. Rodent repellent system i. Raised floors. CCTV are installed at key points for surveillance. Devices are checked on a periodic basis and checklists are prepared.'
		Fire drill is conducted annually.
		Uninterruptible power supply (UPS) devices are in place to secure critical IT equipment against power failures and fluctuations. DG set of sufficient capacity is provided by the facility management / building maintenance to provide power during outage and is maintained by that team.
		Entity has multiple ISPs in place to provide redundancy in case of link failure.
		Physical security/ MEP team monitors the temperature in data hall through BMS system on a regular basis and take corrective actions in case of discrepancy. Daily/ weekly temperature monitoring reports are maintained.
		Physical security/ MEP personnel monitor the status of environmental protections on a regular basis. Many of the critical parameters are monitored on real time basis through a BMS system in the control

Subservice Organization – L&T		
Category	**Criteria**	**Control**
		room. Preventive maintenance plans (PMP), containing schedule of maintenance activities, have been drawn based on manufacturer recommendations and best practices. Maintenance checklists are used where applicable. Annual maintenance contracts (AMCs) are in place for maintenance and testing of fire suppression system, fire panel, fire alarms, smoke detectors, precision ACs, temp/humidity monitoring system, PDU, Water Treatment Plant, DG set, UPS system.
		Backup policy is defined in the information security policies
		Automated backup systems are in place to perform daily backup of log files on NAS.
		Local office (configuration files of various monitoring systems) manual backup is carried out Quarterly on NAS.
		Automated backup systems are configured to send alert notifications to DC IT personnel regarding backup completion / failed status.
		Local office backups are performed on external hard drives.

LeapSwitch management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the trust services criteria through written contracts, such as service level agreements. In addition, LeapSwitch performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with the subservice organization
- Reviewing attestation reports over services provided by the subservice organization.
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization