# System and Organization Control (SOC 3) Report

# Cyfuture India Pvt. Ltd

## Relevant to Security, Confidentiality, Availability, Processing Integrity, and Privacy

**From 1st July 2025 to 28th February 2026**

## Statement of Confidentiality

In this report Cyfuture India Pvt. Ltd(Service Organization) has engaged the service auditor to:

**a.** Examine the controls within the system relevant to Security, Confidentiality, Availability, Processing Integrity, and Privacy and

**b.** Issue a SOC 3® report that can be posted on its website to encourage prospective customers to contract the service organization's services.

# Table Of Contents


Section 1 Assertion of CYFUTURE Software Solution Limited-Service Organization Management ..... 6

1.1 Assertation CYFUTURE Software Solution Limited, Service Organization Management ..... 7

Section 2 Independent Service Auditor Report ..... 9

2.1 Scope ..... 10

2.2 CYFUTURE Software Solution Limited, Responsibilities ..... 10

2.3 Service Auditors' Responsibilities ..... 10

2.5 Opinion ..... 11

Section 3 Attachment A Service Organization's Description of the Boundaries of CYFUTURE System ..... 12

3.1 Background and Overview of CYFUTURE Software Solution Limited ..... 13

3.1.1 Board of Directors ..... 13

3.1.2 Management's Philosophy and Operating Style ..... 14

3.2 Overview of the services provided (Boundaries of the system) ..... 14

3.3 Control Environment ..... 14

3.3.1 Human Resources ..... 15

3.3.1.1 Organization Structure ..... 15

3.3.1.2 Organization Chart ..... 16

3.3.1.3 Roles & Responsibilities ..... 17

3.3.1.4 Human Resources Policies & Procedures ..... 23

3.3.1.5 New Hire Procedures ..... 24

3.3.1.6 Training & Awareness ..... 24

3.3.1.7 Employee Terminations ..... 24

3.3.1.8 Code of Conduct and Disciplinary Action ..... 24

3.3.2 Risk Management & Assessment ..... 25
3.3.3 Network Security ..... 25
3.3.3.1 Firewall ..... 26
3.3.3.2 Network and Endpoint Protection ..... 27
3.3.3.3 Monitoring ..... 27
3.3.4 Physical and Environmental Security ..... 27
3.3.4.1 Server Room ..... 27
3.3.4.2 Physical Access ..... 27
3.3.4.3 Access to Server Room ..... 28
3.3.4.4 Power Backup and Environmental Security ..... 28
3.3.5 Vendor Management ..... 29
3.3.6 Information & Communication ..... 29
3.3.7 Electronic Mail (e-Mail) ..... 29
3.3.8 Capacity Management ..... 29
3.3.9 Vulnerability Scans & Security Audits ..... 30
3.3.10 Patch Management ..... 30
3.3.11 Help Desk ..... 30
3.3.12 Change Management ..... 30
3.3.13 Incident Response and Management ..... 31
3.3.14 Logical Access ..... 31
3.3.14.1 Security Authorization and Administration ..... 31
3.3.14.2 Security Configuration ..... 31
3.3.14.3 Administrative Level Access ..... 32

3.3.15 Media Disposal ..... 32
3.3.16 Backup and Recovery of Data ..... 32
Attachment B Principal Service Commitments and System ..... 33

# Section 1 Assertion of Cyfuture India Pvt. Ltd -Service Organization Management

## 1.1 Assertation Cyfuture India Pvt. Ltd, Service Organization Management



cyfuture
Thinking Future. Moving Ahead.

CMMI DEV/SVC APPRAISED ISO Great Place To Work. Certified

Date: 02-04-2026

**Management of Cyfuture India Pvt. Ltd. Assertion**

We are responsible for designing implementing, operating and maintaining effective controls within **Cyfuture India Pvt. Ltd.** for "**Providing Data Center, Co-Location Services, Security Services, Dedicated, VPS & Cloud Hosting Services, Customer Support, Remote Technical Support and Managed Services**" throughout the period 1st July 2025 to 28th February 2026, to provide reasonable assurance that Cyfuture's service commitments and system requirements relevant to **Security, Availability, Confidentiality, Privacy and Processing Integrity, (applicable trust services criteria)** set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria. Our description of the boundaries of the system is presented in **attachment A** 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 1st July 2025 to 28th February 2026, to provide reasonable assurance that Cyfuture's service commitments and system requirements were achieved based on the applicable trust services criteria. Cyfuture'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 **attachment B.**

Cyfuture does not use any subservice organization.

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 1st July 2025 to 28th February 2026, to provide reasonable assurance that Cyfuture's service commitments and system requirements were achieved based on the applicable trust services criteria.

**For Cyfuture India Pvt. Ltd.**

**Name: Ajai Rai**

**Title: Chief Technology Officer**

**Date: 02-04-2026**

**Signature:**

Cyfuture India Pvt. Ltd. NOIDA

**Cyfuture India Pvt. Ltd.**
(Formerly known as Cyber Futuristics India Pvt. Ltd.)
**Noida (Corporate office):** Plot No. 197-198, Noida Special Economic Zone, Dadri Road, Phase II, Noida-201305 (U.P.) **Tel:** +91-120-6277700 | **Fax:** +91-120-6277766
**Jaipur (Regd.Office):** G1-227,228 & H1-236,239, Opp. Fire Station, EPIP Sitapura, Jaipur-302022 (RJ) **Tel:** +91-141-2770439/440 | **Fax:** +91-141-2770425
**CIN No.:** U72200 RJ 2001 PTC 017138 | **E-mail:** info@cyfuture.com | www.cyfuture.com

# Section 2 Independent Service Auditor Report

**To management of CYFUTURE Software Solution Limited**

## 2.1 Scope

We have examined Cyfuture India Pvt. Ltd Service Organization's (CYFUTURE) accompanying assertion titled "Assertion of CYFUTURE Service Organization Management" (assertion) that the controls within CYFUTURE **Providing Data Center, Co- Location Services, Security Services, Dedicated, VPS & Cloud Hosting Services, Customer Support, Remote Technical Support and Managed Services** supported by IT, HR and Administration including Legal (system) were effective throughout the period from 1st July 2025 to 28th February 2026, to provide reasonable assurance that CYFUTURE service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality, Availability, Processing Integrity, and Privacy (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria.

## 2.2 CYFUTURE Software Solution Limited, Responsibilities

In section 1, CYFUTURE has provided its assertion titled "Assertion of CYFUTURE Software Solution Limited-Service Organization Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated in the description. CYFUTURE is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; specifying the control objectives and stating them in the description ; identifying the risks that threaten the achievement of control objectives; selecting the criteria stated in the assertion, and designing, implementing and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

## 2.3 Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on 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 AICPA. Those standards require that we plan and perform our 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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included the following:

- 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 CYFUTURE 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 CYFUTURE 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.

## 2.4 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.

## 2.5 Opinion

In our opinion, management's assertion that the controls within CYFUTURE Providing Data Center, Co- Location Services, Security Services, Dedicated, VPS & Cloud Hosting Services, Customer Support, Remote Technical Support and Managed Services supported by IT, HR and Administration including Legal System were effective throughout the period from 1st July 2025 to 28th February 2026, to provide reasonable assurance that CYFUTURE 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
PAC-FIRM-LIC-47383
Kalispell, Montana
April 02, 2026

# Section 3 Attachment A Service Organization's Description of the Boundaries of CYFUTURE System

## 3.1 Background and Overview of CYFUTURE Software Solution Limited

Cyfuture India Pvt. Ltd. is a leading provider of comprehensive IT infrastructure and support services. The company offers a wide range of solutions, including Data Center and Co-Location services, Security Services, Dedicated and VPS Hosting, and Cloud Hosting tailored to meet diverse business needs. In addition to hosting services, Cyfuture excels in delivering exceptional Customer Support, Remote Technical Support, and Managed Services, ensuring seamless operations for its clients. These services are supported by robust IT, HR, Administration, and Legal frameworks, enabling Cyfuture to maintain high-quality standards and compliance across its offerings. With a focus on reliability, security, and innovation, Cyfuture empowers businesses to scale effectively and achieve operational excellence.

CYFUTURE 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. CYFUTURE 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.

### 3.1.1 Board of Directors

1. Mr. Anuj Bairathi – Founder & CEO
2. Mr. Gary Barlow – Director UK Operations
3. Mrs. Shilpi Agarwal – Chief Strategy Officer
4. Mr. Rana Ray – Chief Business Officer
5. Mr. Ravish Sharma – Chief Operating Officer
6. Mr. Munish Mahajan- Chief Human Resources Officer
7. Mr. Ajai Rai – Chief Technology Officer

### 3.1.2 Management's Philosophy and Operating Style

The Executive Management team assesses risks prior to venturing into business ventures and relationships. The Executive Management team to interact with operating management on a daily basis.

## 3.2 Overview of the services provided (Boundaries of the system)

The specific products and services and location(s) included in the scope of the report are as below:

| **Products and Services in scope:** |
| --- |
| Providing Data Center, Co-Location Services, Security Services, Dedicated, VPS & Cloud Hosting Services, Customer Support, Remote Technical Support and Managed Services |
| **Geographic Location Scope:** |
| Plot no 197/198 Noida Special Economic Zone Noida Dadri Road, Noida Phase II Noida -201305, Uttar Pradesh, India |

## 3.3 Control Environment

CYFUTURE has established an internal controls framework that reflects the overall control environment within the organization and its various processes, the risk assessment procedure, control activities that help in meeting the overall control objectives, information and communication, and monitoring components of internal control.

CYFUTURE's governance strategy is designed to generate business value by concentrating on the most critical factors. The key principles driving this approach include:

- Transparency and Accountability
- Compliance

- Efficiency and Effectiveness
- Customer-Centric Approach
- Continuous Improvement
- Trust Integrity

CYFUTURE looks at governance from a process perspective and provides regular updates on operational performance. The enhanced governance framework is highlighted below.

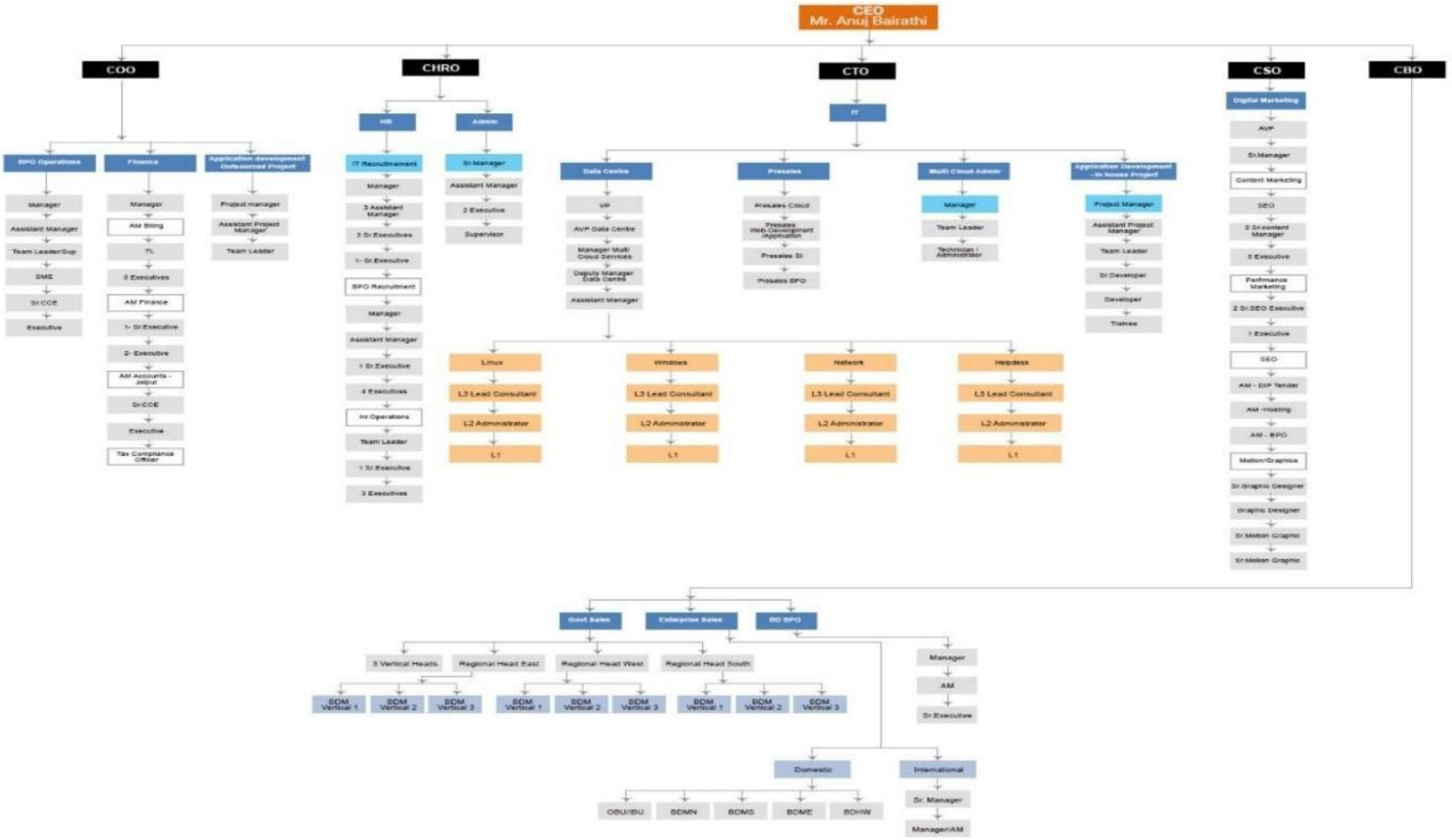
### 3.3.1 Human Resources

#### 3.3.1.1 Organization Structure

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

The management team meets regularly to review business unit plans and performances. Meetings with the MD and department heads are held to review operational, security and business issues, and plans for the future.

### 3.3.1.2 Organization Chart



### 3.3.1.3 Roles & Responsibilities

Management is responsible for the assignment of responsibility and delegation of authority within CYFUTURE. The following are the responsibilities of key roles:

**a. Role of IT Infra Head**

- Organize management review meeting within stipulated intervals and report the performance of the Information Security System to top management.
- Availability of Infrastructure/Human Resource and Monitoring.
- Impart training on Information Security System throughout the Company.
- Initiate action on: Corrective action on non-conformities, Development activities to maintain and improve Information Security systems, to represent the needs of customers in internal functioning,
- Handling all Technical Issues.
- Ensure VAPTs are conducted on Quarterly basis.

**b. Role of CISO**

- To work in co-ordination with the Information Security Management Team, issue guidelines, incorporate appropriate procedures, conduct routine internal audit checks to verify the compliance to the Information Security Policies and Procedures and detect incidents.
- Lead the System Administration Team and Information Security Management Team in the information security related activities.
- Prepare security briefs for the Information Security Management Team.
- Maintain Information Security Management System.
- Establish the Security Risk Assessment Process, and Review Risk Assessment Reports and status.
- Establish, support, control and mitigate risk by better the Risk management process for Information systems.
- Maintain the Statement of Applicability.
- Monitor ongoing compliance with security standards.
- Establish and maintain contacts with external security resources.
- Evaluate changes in asset base and resultant security implications.
- Manage the timely resolution of all issues and questions regarding responsibilities for Information security management within that relate to achieving and maintaining full compliance with the Information Security Policies and Procedures.

- Ensure that responsibilities are defined for, and that procedures are in effect, to promptly detect, investigate, report and resolve Information security incidents within CYFUTURE.
- Seek legal guidance in case of illegal activities or hacking related to CYFUTURE. Notify such issues to the senior management and to the Information Security Management Team immediately.
- Evaluate and recommend on new security products to be implemented across CYFUTURE.
- Initiate protective and corrective measures if a security problem is discovered

**c. Role of Compliance Head**

- Defining the necessary level of knowledge on existing and emerging regulatory compliance requirements across the organization.
- Developing the annual compliance work plan that reflects the organization & unique characteristics.
- Guiding in a productive, professional way, the compliance teams.
- Providing strategic direction to the management team on compliance.
- Preparing and presenting clear and concise compliance reports to the Board.
- Interacting with regulators on compliance issues.
- Coordinating internal compliance review and monitoring activities
- Independently investigating and acting on matters related to compliance.
- Monitoring external review processes.
- Develop and implement company policies and regulation.
- Oversee all business operation relating to compliance including
- Policies and Procedure.
- Design and monitor control system to deal with violations of legal rules and internal policies
- Regularly assess the efficiency of control system and recommend effective improvement.
- Review and evaluate company procedure and reports to identify hidden risks or common issues.
- Assist in conducting internal and external security audits to assess compliance with regulations and policies.
- Stay informed about industry best practices and security standard, implementing them to enhance the organization's security.
- Identify areas for improvement withing the security program and propose enhancements to processes and procedures.

**d. Role of Compliance Manager**

- Achieve full compliance with all relevant laws, regulations, and standards

- Ensure that all employees are aware of and adhere to compliance requirements
- Identify, assess, and manage compliance risks to protect the organization from legal and financial penalties
- Ensure robust internal controls are in place to safeguard the organization's assets and data.
- Promote a culture of ethics and compliance throughout the organization.
- Ensure accurate and timely reporting of compliance activities and issues to senior management and stakeholders.
- Build and maintain a strong, skilled, and motivated compliance team.
- Effectively manage relationships with regulatory bodies, auditors, and external partners.
- Continuously improve compliance processes and procedures to enhance efficiency and effectiveness.
- Align compliance activities with the organization's strategic goals and support overall business objectives.
- Establish the organization as a leader in compliance and ethical business practices.

**e. Role of Compliance Lead**

- As per the requirement design, develop, implement and analyze compliance programs for the CYFUTURE Organization.
- Revise compliance programs as necessary to meet changing needs of CYFUTURE organization.
- Proactively read through the compliance guidelines, requirements and standards.
- To review & guide against the policies & procedures to compliance executive.
- To coordinate & handle the external audits.
- Develop and implement a compliance program to ensure the organization operates in accordance with regulations.
- Although it led and motivate using leadership skills and qualities, there are the responsible duties for performance.
- Monitor and assess current projects compliance risks for.
- Contribute to the development and delivery of security awareness programs for employees
- Assist in conducting internal and external security audits to assess compliance with regulations and policies
- Monitoring compliance process - start to end.
- Identify areas for improvement withing the security program and propose enhancements to processes and procedures
- Monitor the response to actual or suspected breaches in the confidentiality, integrity or availability of information assets**.**

**f. Compliance Specialist**

- Design, develop, implement and analyze compliance programs for the company.
- Revise compliance programs as necessary to meet changing needs of company.

- Proactively read through the compliance guidelines, requirements and standards.
- Compile and analyze both internal and external information to prepare compliance audit data & another checklist.
- Collect and coordinate internal compliance data with other departments to support said departments.
- Implement policies, procedures and systems to provide administrative support to departments.
- Answer questions regarding regulations to help other members or clients of company better understand.
- Study both existing and new legislation, enforce obedience to policies and advise management on necessary actions to make sure company complies with local, state and country legal requirements.
- Stay current on industry standards by continuing education, reading publications, talking with peers and joining professional groups.
- Explore new, innovative opportunities to add value to your job and the job of everyone in the company.
- Assist compliance manager to administer all processes and procedures and ensure working within regulation framework and develop and implement all policies and recommend ways to minimize risk.
- Educate staff about security risks, best practices, and proper handling of sensitive information
- Coordinate a response to actual or suspected breaches in the confidentiality, integrity or availability of information assets**.**

**g. Head – HR Operations**

- Develop corporate plans for a variety of HR matters.
- Overseeing HR initiatives, systems, and tactics.
- Provide proactive and strategic guidance and support for organizational planning and development initiatives that align the human resources agenda in support of key business strategies and initiatives.
- Understand business strategies and how to develop high impact human capital solutions
- Have a data-driven mindset to assess organizational metrics and provide insights into the business
- Consistently measures the effectiveness of HR initiatives and programs to ensure they are delivering desired outcomes
- Help foster a culture of innovation, in an environment that requires high levels of scalability, security, and reliability
- Provide daily support to managers with employee attraction, development, and retention issues which may include: Annual reviews, Leadership coaching, Career pathing, Advanced HR reporting and metrics, Special project assistance
- Closely partner with HR Centers of Excellences and other HRBPs to deliver superior results to the business.
- Act to support the human factor in the company by devising strategies for performance evaluation, compensation, and system. etc.
- Supervise the work of the HR team and provide guidance.
- Deal with grievances and violations invoking disciplinary action when required.

- Report to senior management by analyzing data and using HR metrics.
- Oversee, refine, and execute employee standards and procedures, using and improving HR existing and recommended systems and processes.
- Maintain and enhance employee benefits programs, including compensation, health insurance, expenses, vacation, and other personnel packages.
- Ensure legal compliance by monitoring and implementing applicable HR federal and state requirements, conducting investigations, and maintaining records.
- Identify and recommend areas of improvement to internal standard operating procedures, including team restructuring and morale.
- Support departments in the development and delivery of strategic HR plan to fit with the overall business direction.
- Plan, monitor, and appraise HR activities by scheduling management conferences with employees, hearing and resolving employee grievances, training managers to coach and discipline employees, and counseling employees and supervisors.
- Champion the HR process, ensuring the process is up to date and of high quality, providing clarity and connection for all employees and their role about the overall vision.
- Maintain management guidelines by preparing, updating, and recommending human resource policies and procedures.
- Build strong relationships with external suppliers, fostering trust and promoting collaboration.
- Drive an effective client-service HR team that instils company-wide trust and value for the HR function
- Have executive presence and strong communication skills to partner with senior levels of management
- Strong collaboration skills within and outside of HR
- Serve as a role model, thought leader on Human Capital issues, and coaches other HRBPs in their development.
- Handle confidential matters with discretion.
- Knowledge of ISMS Required.

**h. Purchase Head**

- Overall responsibility for Purchasing and Cost Estimating activities across the business.
- Create and implement best practice purchasing vision, strategy, policies, processes and procedures to aid and improve business performance.
- Take ownership of the purchasing policy, guidelines and any associated documents.
- Approved / verify Purchase orders, invoices and other purchase documents to ensure value for money, quality standards and delivery terms with technical and operational after input from stakeholders where appropriate.
- Assist or provide inputs to finance for vendor payments and cash flow management.
- Provide / Approve / Verify input costing to the sales team for various projects.
- Initiate and develop creative and innovative purchase processes (CRM).

- Provide leadership to departments under control. Coach, mentor and develop direct reports and manage a high performing team that delivers continuous improvement, benefit and cost reductions.
- Complete regular performance reviews, manage attendance, holidays, disciplinary issues and procedures as appropriate.
- Set department objectives and monitor ongoing progress and performance.
- Ensure strong communication between teams under leadership to facilitate exchange of information and in order to implement change and improvements.
- Input and hold responsibility for Purchasing and cost estimating budgets.

**i. Purchase Executive**

- Keep a track of Purchase Orders in the database.
- Tracking invoices received against purchase order issued.
- Verify purchase order details with respect to invoices received and other terms & conditions.
- Coordination with vendors regarding invoice related clarifications/issues.
- Get the credit notes where applicable especially ISP (Internet Service Provider) related invoices with SLA breach/service issue as far as up time are considered.
- Taking acceptance from the requestor/end user regarding services/material received against purchase order.
- Timely tax Invoice submission in accounts team.

**j. Admin Specialist**

- Manage relationships with vendors to ensure timely delivery of goods and services.
- Negotiate contracts and agreements to achieve cost-effective solutions.
- Supervise the upkeep and maintenance of office facilities, including HVAC, electrical, and other systems.
- Liaise with maintenance staff and contractors to address any issues promptly.
- Ensure all departmental administrative activities comply with company policies and local regulations.
- Plan and execute departmental events, meetings, and workshops.
- Handle event logistics, including venue selection, catering, and equipment setup.
- Monitor and manage departmental budgets for administrative activities.
- Optimize resource allocation to enhance operational efficiency.
- Identify inefficiencies in administrative processes and propose improvements.

- Implement best practices for effective office operations.

**k. Admin General Manager**

- Formulate and execute a comprehensive global administrative strategy aligned with corporate objectives.
- Identify opportunities for innovation and implement cutting-edge practices to enhance efficiency.
- Oversee administrative operations across multiple regions, ensuring consistency and best practices.
- Lead cross-regional teams to deliver high-quality administrative support and services.
- Develop and implement global SOPs to ensure standardized processes across all locations.
- Monitor compliance and regularly review practices to maintain consistency and efficiency.
- Provide visionary leadership to regional and global administrative teams.
- Build leadership pipelines by mentoring and developing future leaders within the administrative function.
- Drive the adoption of advanced global facility management tools and technologies.
- Lead digital transformation initiatives to modernize administrative operations.
- Manage and negotiate global vendor contracts, ensuring optimal cost efficiency and quality.
- Establish and monitor global vendor performance metrics.
- Oversee and manage global administrative budgets, ensuring efficient resource utilization.
- Identify cost-saving opportunities through strategic planning and innovative practices.
- Ensure adherence to global regulatory requirements and corporate policies.
- Develop and implement risk mitigation strategies for global administrative functions.
- Collaborate with corporate executives to align administrative strategies with overall organizational goals.
- Act as a trusted advisor to senior leadership on administrative operations.

#### 3.3.1.4 Human Resources Policies & Procedures

CYFUTURE maintains written Human Resources Policies and Procedures. The policies and procedures describe 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 behavior 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 during Induction. Personnel policies and

procedures are documented in the Human Resources Policy at intranet.

#### 3.3.1.5 New Hire Procedures

New employees are required to read and accept HR corporate policies and procedures and are provided online access to these policies along with HR manual. 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.
Reference checks are completed for prospective employees. Employees are required to sign Employee Confidentiality Agreement which forms an integral part of employee file. Discrepancies noted in background investigations are documented and investigated by the Human Resources Department. Any discrepancies found in background investigations result in disciplinary actions, up to and including employee termination.

#### 3.3.1.6 Training & Awareness

Appropriate training enables employees & contractors to comply with their responsibilities as it relates to the Information Security Policy. All CYFUTURE employees (including contractors) are subject to mandatory Security Awareness training upon onboarding and on monthly basis as refresher trainings. This training is managed and tracked to ensure organization-wide completion. HR Team maintains the records of such training programs.

#### 3.3.1.7 Employee Terminations

Termination or change in employment is processed as per extant HR related procedures. There are clearly identified and assigned responsibilities regarding 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 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 prior roles are removed and new access privileges are created as appropriate for the current job roles and responsibilities.

#### 3.3.1.8 Code of Conduct and Disciplinary Action

CYFUTURE 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. An employee whose conduct does not comply with an element of the code of conduct and has been found to have breached the same is prosecuted as per defined process and policies.

### 3.3.2 Risk Management & Assessment

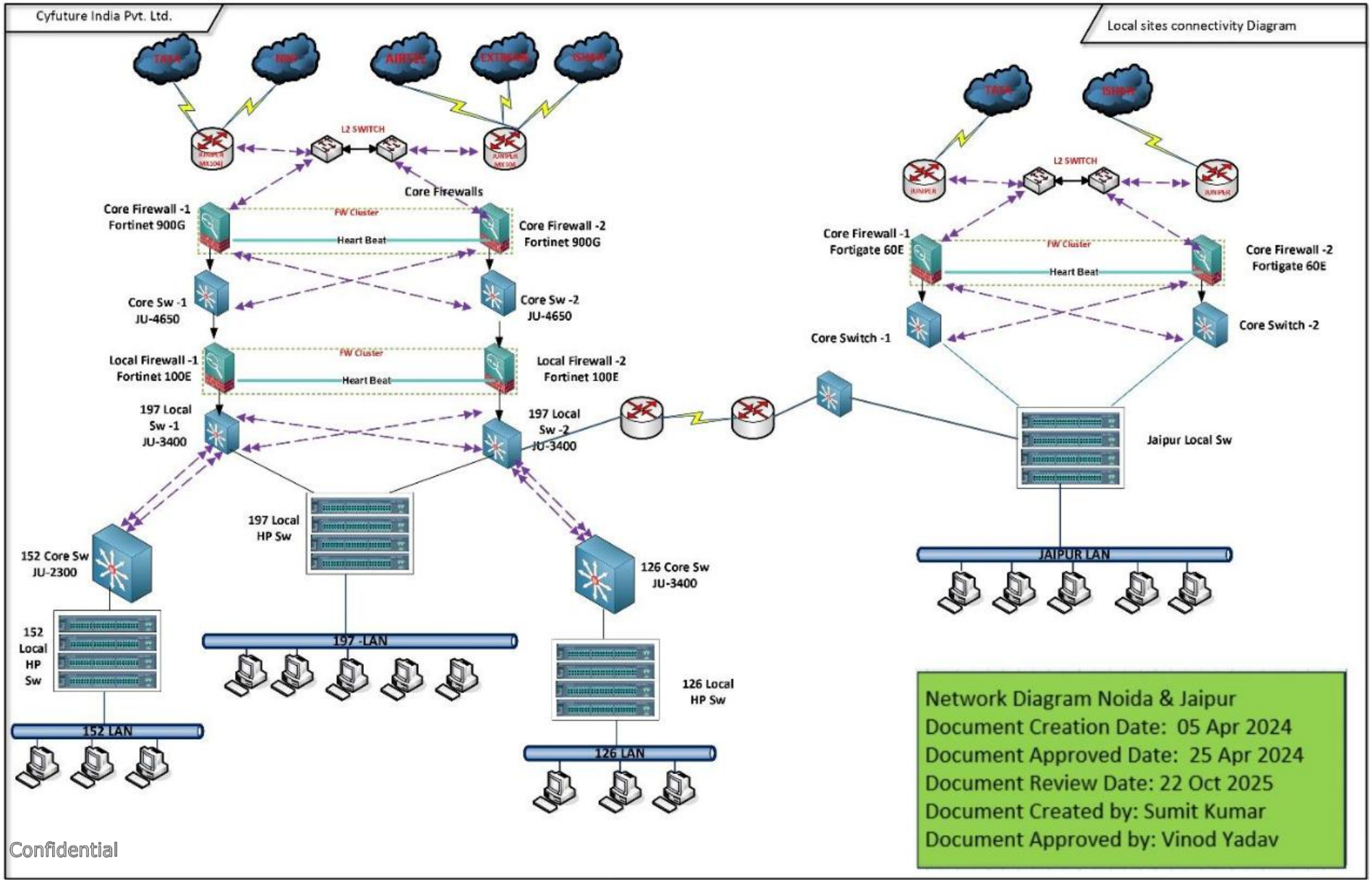
Risk assessments are performed annually to identify current risk levels, with recommendations to minimize those risks that are determined to pose an unacceptable level of risk to CYFUTURE. As part of this process, security threats are identified and the risk from these threats is formally assessed.
CYFUTURE has operationalized 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 Information Security team identifying significant risks in their areas of responsibility and implementing appropriate measures to address those risks.
Following steps are involved in performing risk assessments

- Risk identification for each asset in a process and at Organizational level.
- Risk analysis & evaluation for each asset in a process & at Organizational level.
- Risk treatment & residual risk.

Risk assessment comprises of calculating the level of risk associated with assets belonging to a particular business process. It is done in a manner to assess and evaluate the criticality of impact on business by a particular risk also to identify the areas where organization needs to focus over information security. Apart from the asset-based risk assessment, the Company has also conducted organization-based risk assessment which is based on internal as well as external issues, needs and expectations of interested parties etc. The threats, vulnerabilities associated with every asset are evaluated along with threat impact, probability of occurrence and chances of detection (on a rating basis) of the threat. This determines the Risk Factor, which is then put into an equation to derive a risk value. The risk value is then compared to the organizational threshold (i.e., accepted risk value) which is treated appropriately (i.e., treat, transfer, avoid, accept). The identified risks will be treated (mitigated) so that risk levels are reduced. The output of a risk assessment will include a complete risk register and risk treatment plan. Any action plans are tracked to completion. Regular management meetings are held to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.

### 3.3.3 Network Security

CYFUTURE has established a well-defined Network Security Policy, supported by an approved and up-to-date network diagram. The policy outlines clear guidelines for securing the network infrastructure, ensuring alignment with industry best practices. The network diagram provides a comprehensive view of the network's architecture, facilitating effective monitoring, management, and troubleshooting. These measures demonstrate CYFUTURE commitment to maintaining a secure and resilient network environment, safeguarding its information assets against potential threats.


Cyfuture India Pvt. Ltd.
Local sites connectivity Diagram
L2 SWITCH
Core Firewalls
Core Firewall -1
Fortinet 900G
FW Cluster
Heart Beat
Core Firewall -2
Fortinet 900G
Core Sw -1
JU-4650
Core Sw -2
JU-4650
Local Firewall -1
Fortinet 100E
Local Firewall -2
Fortinet 100E
197 Local
Sw -1
JU-3400
197 Local
Sw -2
JU-3400
197 Local
HP Sw
152 Core Sw
JU-2300
126 Core Sw
JU-3400
152
Local
HP
Sw
197 -LAN
126 Local
HP Sw
152 LAN
126 LAN
L2 SWITCH
Core Firewall -1
Fortigate 60E
FW Cluster
Heart Beat
Core Firewall -2
Fortigate 60E
Core Switch -1
Core Switch -2
Jaipur Local Sw
JAIPUR LAN
Network Diagram Noida & Jaipur
Document Creation Date: 05 Apr 2024
Document Approved Date: 25 Apr 2024
Document Review Date: 22 Oct 2025
Document Created by: Sumit Kumar
Document Approved by: Vinod Yadav
Confidential

#### 3.3.3.1 Firewall

FortiGate with High Availability is installed and Configured for the Core Infrastructure in Active Mode, where the Firewall being used for the Load Balancing and Fault Tolerance.

The Firewall include Antivirus, IPS, Antispam and other UTM features enabled for the protection of the Completed Infrastructure. The Device configurations comply with all security parameters and has been integration with the Radius server for Authentication. Any change to this device configurations comes with the network and security division. All configuration, backup and rules been documented for the compliance.

#### 3.3.3.2 Network and Endpoint Protection

All systems and devices are protected by the comprehensive endpoint protection system. The endpoints include antivirus, anti-malware and Trojan protection from any source. This also includes the e-mail scanning of the systems which prevents malicious scripts and viruses from the e-mails. Apart from which all systems are restricted to internet with the content filtering system routed through the proxy server.

#### 3.3.3.3 Monitoring

CYFUTURE has 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.

### 3.3.4 Physical and Environmental Security

#### 3.3.4.1 Server Room

CYFUTURE local servers including Domain Controller, Antivirus Server, AD Server, WSUS Server, and Tally Server with Backup server are hosted at the CYFUTURE India server room. The server room offers multi- layered security that ensures compliance control for sensitive information. The server room is equipped with industry-standard controls for Physical Security including Temperature Control, Water and Temperature sensing alarm, Pest and rodent control, Fire suppression system. Access to the server room is controlled through biometric access. The entry and exit to the server room are monitored using CCTV Camera.

#### 3.3.4.2 Physical Access

The entrance is secured with a security person, access control and CCTV surveillance. Physical and Environmental Security is controlled and governed by physical security policies forming part of the IS Policy. Entry to the Office premises is restricted to authorized personnel by a biometric access control system. These cards open the door lock. Attendance is recorded through biometric system. All visitors have to sign the visitors register and are given inactive visitor card. Employees are subjected to show their ID cards at the Security entrance and swipe in/thumb print the access management system. Employees are

granted access only to those areas which they are required 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 wear their access cards/employee identification cards at all times 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. ID cards are issued to new employees based on an access requisition initiated by the Human Resource (HR) group. The HR sends an e-mail to IT department requesting the IT team to issue an access card to the new employee. The IT team ensures that the access card/biometric controls 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.

Visitor Management System is implemented for entry to outsiders visiting the premises for any purpose. All visitors have to get approval prior to visit and make entry in visitors register and are given controlled visitor access card. Security guards control visitor access at all entrance points. Surveillance cameras have been installed at various critical points within & around the facility. Backup of recordings is stored for one month. 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, escorted, under video surveillance and supervised. Appropriate displays at the key entry points inform visitors of their responsibilities.

#### 3.3.4.3 Access to Server Room

Access to the data center is controlled by a bio metric access control system and access allowed to DC infra team. CYFUTURE's policies protect sensitive equipment such as servers, communication and power hubs and controls. Only Authorized personnel are allowed to enter such sensitive areas controlled with separate access cards and biometric systems. Third parties are allowed access to the data center only under the supervision of IT team members and prior information. Visitors are supposed to fill the data center access form.

#### 3.3.4.4 Power Backup and Environmental Security

CYFUTURE's Offices 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 and UPS are under AMC for preventive maintenance. 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. Periodic fire drills are

conducted in coordination with Admin and HR personnel. The fire drills reports are collected and analysis made upon it.

### 3.3.5 Vendor Management

CYFUTURE has a formal vendor assessment process in place to evaluate vendor security controls and processes governed by CYFUTURE Vendor Management policy. During vendor onboarding and on a periodic basis vendor's security controls are assessed, managed, and monitored to ensure an appropriate control environment consistent with CYFUTURE security, availability, and confidentiality commitments.
Risk assessment procedures implemented by CYFUTURE evaluate policies, processes, personnel, systems, and effectiveness of internal controls. The risk assessment is performed at least annually.

### 3.3.6 Information & Communication

CYFUTURE has documented procedures covering significant functions and operations for each major work group. Policies and procedures are reviewed and updated based upon suggestions from security personnel and approval by management. Departmental managers monitor adherence to policies and procedures as part of their daily activities. The management holds departmental status meetings, along with strategic planning meetings, to identify and address service issues, customer problems, and project management concerns. Manager Service Delivery and Sr. Manager Operational Excellence are 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 CYFUTURE's processes to provide timely information to employees regarding daily operating activities and to expedite management's ability to communicate with employees.

### 3.3.7 Electronic Mail (e-Mail)

Communication to Customer organizations and project teams are done 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 the attention of employees towards adherence to specific procedural requirements. CYFUTURE requires two factor authentications from employees to access their e- mails.

### 3.3.8 Capacity Management

Capacity management controls are put in place so as to monitor, tune and project certain CYFUTURE's resources to ensure system performance meets the expected service levels and 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.

### 3.3.9 Vulnerability Scans & Security Audits

FortiGate Endpoint Security 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.

### 3.3.10 Patch Management

The respective vertical team of Windows/Network team ensures that all patches to network device/servers operating systems are tested for stability & availability issues before deploying to the production environment. The patch management activity is done 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 related and marked critical and security are managed and applied as they become available, windows systems are managed through the WSUS patch management system and the network devices OS patching is managed automatically while renewed.

### 3.3.11 Help Desk

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

### 3.3.12 Change Management

CYFUTURE 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. All the changes need to be subjected to a formal Change Management process.

Every change to such base lined components is governed by the change control and management procedures as outlined in the Helpdesk, Change management and Incident Response procedure. CYFUTURE's change management process requires all security patches and system and software configuration changes to be tested before deployment into Stage or Production environments.

All changes are recorded, approved, implemented, tested and versioned before moving to production environment. The impact of implementing every significant change is analyzed and approved by the IS team Head before such implementation. A sign-off obtained from the personnel who had requested for the change after implementation of the change.

### 3.3.13 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 or through email. For Network incidents, IT team received incident tickets via email and are resolved by them. IT team operates 24X7 for all support functions. The help desk personnel or IT team study and escalate all security incidents to the designated team for further escalation/resolution. All security incidents are reviewed and monitored by the IT Team. Corrective and preventive actions are completed for incidents.

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 and the actions proposed are approved by CSP Head.

### 3.3.14 Logical Access

#### 3.3.14.1 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 and IS policies. Any additional access is recommended by the line manager and approved IT Head. Company has standard configuration that is implemented across Desktops & laptops individually.

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

#### 3.3.14.2 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 with the associated

password. Remote access to critical resources is not permitted to any employee. Passwords are controlled through Password policy of the domain controller 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. Unattended desktops are locked within a time of inactivity. Users are required to provide their password to unlock the desktop.

#### 3.3.14.3 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 by IT head.

### 3.3.15 Media Disposal

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.

### 3.3.16 Backup and Recovery of Data

CYFUTURE has developed formal policies and procedures relating to backup and recovery. Backup is defined in the Backup Policy. Suitable backups are taken and maintained. 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_&_Backup_Encryption_Policy**".

# Attachment B Principal Service Commitments and System

# Principal Service Commitments and System

CYFUTURE designs its processes and procedures related to the CYFUTURE Providing Data Center, Co-Location Services, Security Services, Dedicated, VPS & Cloud Hosting Services, Customer Support, Remote Technical Support and Managed Services supported by IT, HR and Administration including Legal to meet its objectives for its Data Center services. Those objectives are based on the service commitments that CYFUTURE makes to its customers, business partners, and vendors, and the operational and compliance requirements that CYFUTURE has established for the services. Service commitments are declarations made by management to its customers regarding the performance of the CYFUTURE Data Center services. Service commitments are set forth in standardized contracts, service level agreements, and in the description of the service offered online and include the following:

- Commitments regarding the security, availability, processing integrity of the system and confidentiality and privacy of information processed by the system in accordance with contractual stipulations.
- Commitments regarding customer interactions as described in the master service agreement, service level agreement, and the system reference document.

CYFUTURE establishes operational requirements that support the achievement of security commitments, relevant operational and compliance requirements, applicable laws and regulations, and other system requirements. These include system requirements (both functional and non-functional) derived from service commitments, published documentation of system functionality, and other descriptions of the system.
Such requirements are communicated in CYFUTURE's system policies and procedures, system design documentation, and contracts with customers.

CYFUTURE has implemented organization-wide information security policies. In addition to these policies, standard operating procedures have been developed and documented on how to carry out specific manual and automated processes required in the operation and development of the CYFUTURE System. System requirements based on the its Cybersecurity Framework include the following:

- Data, personnel, devices, systems, and facilities are identified and managed
- CYFUTURE management understands and manages the cybersecurity risk to organizational operations.
- Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
- Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability

of information.

- Security policies, processes, and procedures are maintained and used to manage protection of information systems and assets.
- Maintenance and repairs of information system components are performed consistent with policies and procedures.
- Technical security solutions are managed to help ensure the security and resilience of systems and assets.
- Anomalous activity is detected and the potential impact of events is understood.
- The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
- Detection processes and procedures are maintained and tested to help ensure awareness of anomalous events.
- Response processes and procedures are executed and maintained to help ensure response to detected cybersecurity incidents.
- Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
- Recovery processes and procedures are executed and maintained to help ensure restoration of systems or assets affected by cybersecurity incidents.