



SSAE 18 – SOC 3 REPORT (CYFUTURE)

For the period, 1st January 2023 to 31st July, 2023

Relevant to Security, Confidentiality, Availability and the Suitability of the Design and Operating Effectiveness of Controls

Table of Contents

- SECTION 13**
- 1. MANAGEMENT OF CYFUTURE’S ASSERTION3**
- Section 2.....6**
- 2. INDEPENDENT SERVICE AUDITOR’S REPORT.....6**
- SECTION 3.....9**
- 3. Description of Cyfuture’s “System” throughout the period 1st January 2023 to 31st July, 2023.....9**
- 3.1 Description of Cyfuture’s system throughout the 1st January 2023 to 31st July, 2023 10*
- 3.2 Description of Control Environment, Control Activities, Risk Assessment, Monitoring and Information, and Communication 11*
- 3.3 Risk Management and Risk Assessment 11*
- 3.4 Software 12*
- 3.5 Monitoring 13*
- 3.6 People..... 13*
- 3.7 Procedures 14*
- 3.8 Logical Access 15*
- 3.9 Confidentiality..... 15*
- 3.10 Backup and Recovery of Data..... 15*

SECTION 1

1. MANAGEMENT OF CYFUTURE'S ASSERTION

MANAGEMENT ASSERTION DOCUMENT

Date: 18-10-2023

Management of Cyfuture India Private Limited Assertion

We have prepared the accompanying description of the **Cyfuture India Private Limited (Cyfuture)** system titled **"Data Center Services Including Web Site Hosting, Web App Hosting, Server Co-Location, Disaster Recovery, Backup, Email Hosting, VPS, Dedicated Server, Cloud Hosting and Managed Services"** throughout the period 1st January 2023 to 31st July, 2023 (description), based on the criteria set forth in the Description Criteria DC Section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 3 Report (description criteria).

The description is intended to provide users with information about the system providing data center services including web site hosting, web app hosting, Server co-location, etc. that may be useful when assessing the risk arising from interactions with Cyfuture controls meet the criteria related to internal controls **Security, Availability, Privacy, Process Integrity, and Confidentiality (Applicable Trust Services Criteria)**

As indicated in the description, Cyfuture does not use any sub-services organizations.

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

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

a. The description fairly presents the system the period 1st January 2023 to 31st July, 2023 based on the following description criteria:

The description contains the following information:

- 1) The types of services provided
- 2) The components of the system used to provide the services, which are as follows:
 - a) Infrastructure. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks).
 - b) Software. The application programs and IT system software that support application programs (operating systems, middleware, and utilities).
 - c) People. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
 - d) Procedures. The automated and manual procedures.
 - e) Data. Transaction streams, files, databases, tables, and output used or processed by the system.

Cyfuture India Pvt. Ltd.

(Formerly known as Cyber Futuristics India Pvt. Ltd.)

Noida (Corporate office): Plot No. 197-198, Noida Special Economic Zone, Dabri Road, Phase II, Noida-201305 (U.P.) | **Tel:** +91-120-6277700 | **Fax:** +91-120-6667766

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**

3) The boundaries or aspects of the system covered by the description.

4) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

a) Complementary user entity controls contemplated in the design of the service organization's system.

8) In the case of a SOC 3 report, relevant details of changes to the service organization's system during the period covered by the description.

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


b. The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated as described and if user entities applied the complementary user entity controls, and the subservice organization applied the controls contemplated in the design of Company Name controls period of 1st January 2023 to 31st July, 2023.

c. The Cyfuture controls stated in the description operated effectively the throughout period of 1st January 2023 to 31st July, 2023 to meet the applicable trust services criteria if user entities applied the complementary user entity controls, and the subservice organization applied the controls contemplated in the design of Cyfuture period of 1st January 2023 to 31st July, 2023

Name: AJAI RAI

Signature:

Date:


18/10/2023

Section 2

2. INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Management of Cyfuture India Pvt. Ltd. (Cyfuture)

Scope

We have examined Cyfuture India Pvt. Ltd.'s (Cyfuture) ("Service Organization") accompanying assertion titled "Management of Cyfuture's Assertion" ("assertion") that the controls over "**Providing Data Centre Services including Web Site Hosting, Web Application Hosting, Server co-location, Disaster Recovery, Backup, Email Hosting, VPS, Dedicated Server, Cloud Hosting and Managed Services**" ("system") were effective throughout the period 1st January 2023 to 31st July, 2023, to provide reasonable assurance that Cyfuture'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).

Service Organization's Responsibilities

Cyfuture 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 Cyfuture's service commitments and system requirements were achieved. Cyfuture has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Cyfuture 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. 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.

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 Cyfuture'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 Cyfuture'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.

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 Cyfuture's system were effective throughout the period 1st January 2023 to 31st July, 2023, provides reasonable assurance that Cyfuture's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

A handwritten signature in blue ink, appearing to read 'Sandip Padhi', with a horizontal line drawn through it.

Sandip Padhi

Place Date: - 06-11-2023

SECTION 3

3. Description of Cyfuture's "System" throughout the period 1st January 2023 to 31st July, 2023

3.1 Description of Cyfuture's system throughout the 1st January 2023 to 31st July, 2023

Background and Overview of Services

Cyfuture India Pvt. Ltd is a leading provider of enterprise hosting, cloud hosting, website hosting, and application hosting services to global clients across multiple industries. We have an impressive track record of executing and managing large-scale IT infrastructure projects for several Fortune 500 firms, government institutions, and small & medium enterprises. Our hosting solutions provide our clients the much-needed freedom to focus and grow their business while we effectively manage their mission-critical data center infrastructure and maintenance.

Organizational business goals are varied. And, so are our hosting solutions. The only thing constant is our years of expertise and ability to provide customized solutions to each client according to their distinct business needs. Our team of engineers ensures that the data center infrastructure of our clients is up and running with regular system upgrades to ensure maximum security of their data and increased efficiency of their computing systems. We currently own and operate state-of-the-art Tier III data center facilities in Noida and Jaipur (India) which are equipped with cutting-edge hardware and software to deliver best-in-class data center and cloud hosting solutions.

Cyfuture is certified against the requirements of ISO 27001:2013, ISO 9001: 2008 & HIPAA

Significant Changes during the Review Period

None

Subservice Organizations

Cyfuture does not use any subservice organization.

Boundaries of the System

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

Products and Services in Scope
The scope of this report is limited to Cyfuture for providing Data Centre activities including Co-Location Services, Security Services, Dedicated Hosting, VPS & Cloud Hosting Services, Customer Support, Remote Technical Support, and Managed Services.
Products and Services <u>NOT</u> in Scope
The report does not cover the following services. <ul style="list-style-type: none">• Cloud Hosting services using CloudOye Application.• Third-party Cloud hosting services such as AWS/Azure
Geographic Locations in Scope

Noida, India	Meghdoot , Plot no 197/198 Noida Special Economic Zone Noida Dadri Road, Noida Phase II Noida - 201305
--------------	---

All the above material activities and operations in scope are performed from the above 01 office location. Unless otherwise mentioned, the description and related controls apply only to the location covered by the report. The data center site at Jaipur, India is specifically excluded from the scope of this report.

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

Control Environment

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

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

Integrity and Ethical Values

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.

Board of Directors

Business activities at Cyfuture are under the direction of the Board of Directors. The company is governed by its Board of Directors headed by its promoter director Mr. Ratan Chand Bairathi, Ms. Shilpi Agrawal, Mr. Rajiv Bairathi & Mr. Anuj Bairathi as the CEO. Oversees the company's India operations playing a key role in strategy and client management.

Management's Philosophy and Operating Style

The Executive Management team at Cyfuture assesses risks prior to venturing into business ventures and relationships. The size of Cyfuture enables the executive management team to interact with operating management on a daily basis.

3.3 Risk Management and Risk 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 its ability to provide reliable processing for User Organizations. This process consists of the Information Security team identifying significant risks in their areas of responsibility and implementing appropriate measures to address those risks.

Information Security Policies

Cyfuture has developed an organization-wide Information Security Policies. Relevant and important Security Policies (IS Policies) are made available to all employees via shared drive and intranet. Changes to the Information Security Policies are reviewed by IS Team and approved by CEO/CISO prior to implementation.

Monitoring

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

Performance monitoring reports cover server parameters such as disc space, incoming/outgoing network traffic, packet loss, CPU utilization, etc. These system performance reports are reviewed by management on a periodic basis.

Information and Communication

The infrastructure comprises physical and hardware components of the System including facilities, equipment, and networks

Physical Access

The entrance is secured by a security person, access control, and CCTV surveillance. The physical and Environmental Security of Cyfuture is controlled and governed by physical security policies forming part of the Cyfuture IS Policy.

Entry to the Cyfuture offices is restricted to authorized personnel by a biometric access control system. All employees are provided with access cards. These cards open the door lock. Attendance is recorded through a biometric system. All visitors have to sign the visitors register and are given an inactive visitor card

3.4 Software

Firewalls

FortiGate 1500D with High Availability is installed and Configured for the Core Infrastructure in Active/Active Mode, where both the Firewalls are being used for Load Balancing and Fault Tolerance.

The Firewalls include Antivirus, IPS, Antispam, and other UTM features enabled for the protection of the Completed Infrastructure.

Network & Endpoint protection / monitoring

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

3.5 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.

Vulnerability Scans & Security Audits

As per the Audit calendar, all the network devices and services are audited for vulnerabilities by doing periodic vulnerability scans. These scans are done by the system admin internally. Cyfuture uses Open Vas for vulnerability scans.

3.6 People

Organizational Structure

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

Mr. Anuj Bairathi manages and oversees all India operations. The management team meets Quarterly to review business unit plans and performances. Meetings with CEO and department heads are held to review operational, security, and business issues, and plans for the future.

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

Human Resources Policies and Procedures

Cyfuture maintains written Human Resources Policies and Procedures. The policies and procedures describe Cyfuture practices relating to hiring, training and development, performance appraisal and advancement and 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 reviews these policies and procedures on a 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 Cyfuture Human Resources Policy at intranet hr.cyfuture.com.

New Hire Procedures

New employees are required to read HR corporate policies and procedures and are provided online access to these policies along with the 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 is on file for employees. 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.

3.7 Procedures

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

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 handling the changes that are to be made. All the changes need to be subjected to a formal Change Management process.

Every change to such baselined 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 the production environment. The impact of implementing every significant change is analyzed and approved by the IS team Head before such implementation. A sign-off was obtained from the person who had requested the change after the implementation of the change.

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 Corp IT networking ticketing tool. For Network incidents, the Cyfuture IT team received incident tickets via the WHMCS ticketing tool and are resolved by them. The 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 CISO.

3.8 Logical Access

Security Authorization and Administration

Email is sent from HR to the 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 Cyfuture HR/Admin policy and IS policies. Any additional access is recommended by the line manager and approved IT Head. The company has a 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 the IT team and authorized users. Access to storage, backup data, systems, and media is limited to the IT team through the use of physical and logical access controls.

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 the IT team, must be justified to and approved by the IT team.

3.9 Confidentiality

Secure procedures are established to ensure the 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.

3.10 Backup and Recovery of Data

Cyfuture has developed formal policies and procedures relating to backup and recovery. The backup policy 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 Policy"