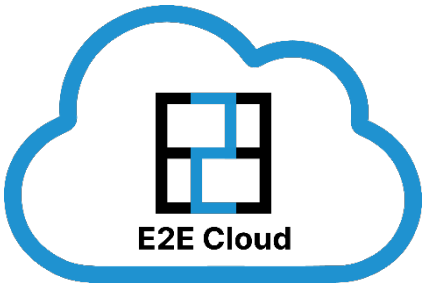

System and Organization Controls (SOC) 3 Report over the E2E Cloud Platform System Relevant to Security, Availability, and Confidentiality for the Period 01 May, 2024 to 31 August, 2024

AUDIT AND ATTESTATION BY

INTERCERT®

Management Assertion

E2E Networks Limited
CIN- L72900DL2009PLC341980
1st Floor, A-24/9,Mohan Cooperative Industrial Estate
Mathura Road,New Delhi-110044, Phone No. +91-11-4084-4964
Email: hr@e2enetworks.com, **website** https://www.e2enetworks.com

Assertion by Management of E2E Networks Limited

We are responsible for designing, implementing, operating, and maintaining effective controls within E2E Networks Limited's System (system) throughout the period 01 May, 2024 to 31 August, 2024, to provide reasonable assurance that E2E Networks Limited'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*, in AICPA Trust Services Criteria. Our description of the boundaries of the system is presented in attachment A (E2E Cloud Platform System) 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 01 May, 2024 to 31 August, 2024, to provide reasonable assurance that E2E Networks Limited's service commitments and system requirements were achieved based on the applicable trust services criteria. E2E Networks Limited'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 (Service Commitments and System Requirements).

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 01 May, 2024 to 31 August, 2024, to provide reasonable assurance that E2E Networks Limited's service commitments and system requirements were achieved based on the applicable trust services criteria.

For E2E Networks Limited

Report of Independent Accountant

Independent Service Auditor's Report on a SOC 3 Examination

To the Management of E2E Networks Limited

Scope

We have examined E2E Networks Limited accompanying assertion titled "Assertion of E2E Networks Limited Management" (assertion) that the controls related to E2E Cloud Platform were effective for the Period 01 May, 2024 to 31 August, 2024 , to provide reasonable assurance that E2E Networks Limited 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, in AICPA Trust Services Criteria.

Service Organization's Responsibilities

E2E Networks Limited 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 E2E Networks Limited service commitments and system requirements were achieved. E2E Networks Limited has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, E2E Networks Limited 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 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.

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 E2E Networks Limited were effective for the Period 01 May, 2024 to 31 August, 2024 to provide reasonable assurance that E2E Networks Limited service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

For,
INTERCERT INC

Neha Mishra, Certified Public Accountant
License Number: PAC-CPAP-LIC-033276
Date: November 15, 2024

E2E Cloud Platform System

Overview

E2E Networks is the leading hyperscaler from India with focus on advanced Cloud GPU infrastructure, listed on the National Stock Exchange (NSE). The company is popular for providing accelerated cloud computing solutions, including cutting-edge Cloud GPUs like NVIDIA A100/H100 GPUs and upcoming H100 on the Cloud, making it the leading IAAS provider focused on advanced Cloud GPU capabilities in India.

E2E Networks Cloud computing solutions are built on the principles of affordability, assistance, accessibility, accommodative, and AtmanirbharBharat (self-reliant India), which are collectively referred to as the 5As of E2E Cloud. The company has been instrumental in helping India become self-reliant in the cloud infrastructure by offering a true public cloud platform that is multi-region, smart dedicated compute, and designed to cater to the unique needs of Higher Education and Research, Enterprises businesses and next generation of AI/ML startups in the country.

Our platform has further strengthened its position as the leading accelerated computing cloud platform from India by demonstrating its capabilities in the AI/ML, NLP, Computer Vision and Generative AI on its Cloud GPU platform. The company has well earned its reputation as a trusted and reliable partner of choice for Higher Education and Research Institutions, Enterprises and AI/ML startups in India and Globally.

E2E Networks was amongst the first few providers out of India providing contractless computing with low latency. The company's advanced Cloud Computing solutions, including Cloud GPUs like NVIDIA A100/H100 and upcoming GH100 are aimed at helping India rise as an AI/ML superpower transforming Higher Education, Research and Enterprises across industry and academia.

Myaccount Portal is a cloud-hosted portal built by E2E Networks Limited hereby referred to as E2E.

Myaccount Portal is a portal where customers can launch and experience the E2E Cloud services. Here is the quick list of E2E Cloud services which are the part of scope.

- Nodes
- GPU
- Load Balancer
- Auto Scaling
- Kubernetes

- Volumes
- Image
- Backups
- EQS
- Scalable File System
- Object Storage
- Container Registry
- DBaaS
- CDN
- Firewall
- Reserved IP
- VPC

Data Centers

The above products are serviced from data centers operated by E2E. Below is a list of E2E's production data center locations that host the above products and operations for E2E's Cloud Platform:

- Delhi - NCR - India
- Delhi – NCR -2 – India
- Mumbai – India

Infrastructure

Myaccount Portal uses a virtual and secure network environment on top of E2E Cloud infrastructure to ensure that the platform is always protected. This is achieved by hosting the application inside a virtual private cloud (VPC) and accompanying firewalls on the infrastructure provider. Myaccount platform backend infra only specific authorized to the concerned team and filters traffic to the private networks with limited access.

When a customer's client device connects to the application over the internet, their data is encrypted and secured over HTTPS. It then passes through the E2E Cloud Internet Gateway.

The internal networks of E2E Cloud are protected by deny-by-default security groups and firewalls to ensure that only deliberately allowed traffic can pass through.

Software

E2E Networks Limited is responsible for managing the development and operation of the Myaccount Portal platform including infrastructure components such as servers, databases, and storage systems.

People

E2E Networks Limited's staff have been organized into various functions like Sales, Support, Engineering, Product Management, etc. The personnel have also been assigned to the following key roles:

Senior Management: Senior management carries the ultimate responsibility for achieving the mission and objectives of the organization. They ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the organization's mission. They also assess and incorporate the results of the risk assessment activity into the decision-making process. The senior management understands that their support and involvement is required in order to run an effective risk management program that assesses and mitigates IT-related mission risks.

Information Security Officer: The Senior Management assigns the role of Information Security Officer to one of its staff members who is responsible for the performance of the information security program of the organization. Decisions made in these areas are based on an effective risk management program. The Information Security Officer is responsible for identifying risks, threats, and vulnerabilities, and adding controls to mitigate these risks. Additionally, they also summarize remaining residual risks and report the same to Senior Management in a timely manner.

Compliance Program Manager: The company assigns the role of Compliance Program Manager to a staff member who would be responsible for the smooth functioning of the Information Security Program. The Compliance Program Manager takes care of the effective

and timely completion of tasks required for the functioning of all information security controls, across all functions/departments of the organization.

System Users: The organization's staff members are the users of the IT systems. The organization understands that use of the IT systems and data according to an organization's policies, guidelines, and rules of behaviour is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, staff members that access IT resources are provided with annual security awareness training.

Data

Data, as defined by E2E Networks Limited, constitutes the following:

- Transaction data
- Electronic interface files
- Output reports
- Input reports
- System files
- Error logs

All data that is managed, processed and stored as a part of the Myaccount Portal is classified as per the Data Classification Policy which establishes a framework for categorizing data based on its sensitivity, value, and criticality to achieving the objectives of the organization.

Change Management

A documented Change Management policy guides all staff members in documenting and implementing application and infrastructure changes. It outlines how changes to the Myaccount Portal system are reviewed, deployed, and managed. The policy covers all changes made to the Myaccount Portal, regardless of their size, scope, or potential impact.

The change management policy is designed to mitigate the risks of

- Corrupted or destroyed information
- Degraded or disrupted software application performance

- Productivity loss
- Introduction of software bugs, configuration errors, vulnerabilities, etc

A change to the Myaccount Portal can be initiated by a staff member with an appropriate role. E2E Networks Limited uses a version control system to manage and record activities related to the change management process.

The version control system maintains source code versions and migrates source code through the development and testing process to the production environment. The version control software maintains a history of code changes to support rollback capabilities. It also facilitates the code review process which is mandated for all changes.

To initiate a change, the developer first creates a feature branch with the updated code. Once the code change is ready for review, the developer submits the code for peer review and automated testing, known as a pull request. For all code changes, the reviewer must be different from the author. Once a pull request is approved, the change can be released to production.

The ability to implement changes in the production infrastructure is restricted to only those individuals who require the ability to implement changes as part of their responsibilities.

Incident Management

E2E Networks Limited has an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers. Customers are directed to contact E2E Networks Limited via the support email address provided during onboarding to report failures, incidents, concerns, or other complaints in the event there were problems.

Incident response procedures and centralized tracking tools consist of different channels for reporting production system incidents and weaknesses. Production infrastructure is configured to generate audit events for actions of interest related to operations and

security. Security alerts are tracked, reviewed, and analyzed for anomalous or suspicious activity.

Where required, security incidents are escalated to privacy, legal, customer, or senior management team(s)and assigned a severity rating. Operational events are automatically resolved by the self-healing system.

- Low severity incidents are those that do not require immediate remediation. These typically include a partial service of E2E Networks Limited being unavailable (for which workarounds exist). These do not require someone to be paged or woken up beyond normal work hours.
- Medium severity incidents are similar to low but could include scenarios like suspicious emails or unusual activity on a staff laptop. Again, these do not require immediate remediation or trigger automatic calls outside work hours. Low and medium-severity incidents usually cover the large majority of incidents found.
- High severity incidents are problems an active security attack has not yet happened but is likely. This includes situations like backdoors, malware, and malicious access to business data (e.g., passwords, payment information, vulnerability data, etc.). In such cases, the information security team must be informed and immediate remediation steps should begin.
- Critical severity incidents are those where a security attack was successful and something important was lost (or irreparable damage caused to production services). Again, in such cases, immediate actions need to be taken to limit the damage.

Post-mortem activities are conducted for incidents with critical severity ratings. Results of post-mortems may include updates to the security program or changes to systems required as a result of incidents.

Availability

E2E Networks Limited has a documented business continuity plan (BCP) and testing performed against the recovery time objectives (RTOs) and recovery point objectives (RPOs). At least daily backup schedules are maintained to protect sensitive data from loss in the event of a system failure. Backups are restored at least annually as part of operational activities and are included as part of the BCP test plan.

Asset Management (Hardware and Software)

Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets are classified appropriately, patched, and tracked as part of configuration management. E2E Networks Limited uses tagging tools to automatically facilitate the company's hardware and software asset inventory. This helps to ensure a complete and accurate inventory of technology assets with the potential to store or process information is maintained.

Physical Security

The in-scope system and supporting infrastructure are hosted by E2E Cloud. As such, E2E Cloud is responsible for the physical security controls of the in-scope system. E2E Networks Limited reviews the SOC 2 report provided by E2E Cloud on an annual basis, to ensure their controls are in accordance with standards expected by the customers of the Myaccount Portal.

[Space Intentionally Left Blank]

Service Commitments and System Requirements

Service Commitments

Commitments are declarations made by management to customers regarding the performance of the E2E's Cloud Platform System. Commitments to customers are communicated via Terms of Service, E2E Cloud Platform Service Level Agreements, and/or Data Processing Agreements. Data Processing Agreements define the security and privacy obligations which the processors must meet to satisfy the organization's obligations regarding the processing and security of customer data.

System Requirements

E2E has implemented a process-based service quality environment designed to deliver the E2E's Cloud Platform System products to customers. These internal policies are developed in consideration of legal and regulatory obligations, to define E2E's organizational approach and system requirements.

The delivery of these services depends upon the appropriate internal functioning of system requirements defined by E2E to meet customer commitments.

The following processes and system requirements function to meet E2E's commitments to customers with respect to the terms governing the security and privacy of customer data:

- Access Security: E2E maintains data access and logical security policies, designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Access to systems is restricted based on the principle of least privilege.
- Change Management: E2E requires standard change management procedures to be applied during the design, development, deployment, and maintenance of E2E applications, systems, and services.
- Incident Management: E2E monitors internal communication channels, audit logs and signals to determine the validity of security threats. Confirmed threats, including threats related to security and privacy, are escalated to the appropriate team including incident management. E2E's dedicated security personnel will react promptly to potential and known incidents.
- Data Management: E2E complies with any obligations applicable to it with respect to the processing of Customer Personal Data. E2E processes data in accordance with E2E Cloud Platform Terms of Service and/or Data Processing Agreements, and complies with applicable regulations.
- Data Security: E2E maintains data security and privacy policies and implements technical and organizational measures to protect customer data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. E2E takes appropriate steps to ensure compliance with the security measures by its employees, contractors and vendors to the extent applicable to their scope of performance.
- Third-Party Risk Management: E2E conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy

appropriate to their access to data and the scope of the services they are engaged to provide. E2E conducts routine inspections of sub processors to ensure their continued compliance with the agreed upon security and privacy requirements. E2E defines security and privacy practices that must be applied to the processing of data and obtains contractual commitments from suppliers to comply with these practices.

[End of the Report]