Last updated on December 8, 2022

Ericom Security Measures for Data Protection

1. **Third Party Assessments** are performed for an accurate, unbiased understanding of security posture**.**
   - Annual audits against the SOC 2 Type II standard, an industry-standard that focuses on non-financial reporting controls as they relate to security, availability, and confidentiality of a cloud service.
   - Annual penetration tests in the application and infrastructure levels using well-known, independent auditors.

2. **Physical access controls** are employed for the prevention of unauthorized persons gaining access to Customer Data processing systems.

   The Ericom Services are hosted by Oracle OCI, Amazon Web Services ("AWS") and MedOne, a Ridge Cloud Service Provider and protected by the security and environmental controls of such providers. (Ericom does not rent physical cages or racks for bare metal.)
   - Each production environment hosting the Ericom Services is logically isolated in a Virtual Private Cloud (VPC).
   - Customer Data stored within the host datacenters are encrypted at all times. The hosting provider does not have access to unencrypted Customer Data.
   - All datacenters are ISO 27001 certified.
   - More information about hosting providers physical access controls and security are available at: https://aws.amazon.com/security/, https://www.oracle.com/security/cloud-security/ and https://medone.co.il/en/medonecloud/cloud-security-and-standards/ .

3. **Admission control** measures are taken for the prevention of the use of data processing systems without authorization.
   - Access limited to members of Ericom Engineering or Operations, and only those team members that need access.
   - Strong password policies are in place. Passwords are changed every 90 days with no re-use of recent passwords allowed. All passwords are documented securely.
   - A Certificate is required to establish any connection.
   - Staff members that do get access to the Ericom Cloud Infrastructure are required to access the Cloud through a Jump Box with 2FA.
   - Screen lock policy is implemented across all of Ericom.
   - All lock screens require a password.

4. **Virtual access control** measures are taken to limit the access of persons entitled to use a data processing system to only Customer Data to which they have a right of access, and that Customer Data cannot be read, copied, modified or removed without authorizations in the course of Processing or use and after storage.
   - All virtual machines are subject to the same access controls as listed above.

5. **Transmission control** measures are taken to prevent Customer Data from being read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of Customer Data by means of data transmission facilities is envisaged.
   - Encryption is used for secure communications wherever practical.
   - Audit Logs are retained for all types of access (not only reporting)
   - All backups are encrypted and securely stored
   - No removable media is permitted

6. **Input control** measures are taken so that it is possible to check and establish whether and by whom Customer Data have been entered into data processing systems, modified or removed.
   - All entries are logged with Time/Date stamps and includes identifiers for entering party.
   - Controls are in place to ensure only authorized access is granted.

7. **Assignment control** measures are employed to process Customer Data in accordance with the Agreement with Customer.
   - Confidentiality agreements are in place for all individuals with data access
   - Training is conducted during onboarding and on a regular basis
   - No third parties used for the processing of data other than listed Sub-Processors.
   - Privacy policy describes rights and obligations of [agent and principal?]

8. **Availability control** measures are taken to protect Customer Data from accidental destruction or loss.
   - Ericom provides redundancy at the Global Cloud level and then N+1 at the Data Center components level as well as the Services level.
   - Data Centers are Tier One hosting facilities with air conditioning, fire and smoke detection as well as network and server level security,

9. **Separation control** measures are taken to enable separate processing of Personal Data collected for different purposes**.**
   - Physical and logical segmentation through a 3 tier architecture of management plane, data plane and logging platform
   - Separation of duties within the Ericom team.
   - Discrete Development, QA and Production Environments are maintained for the Ericom Cloud.
   - All routing for Data Processing is performed by Automated Policy Engines.