DATA PROTECTION & SECURITY MEASURES at COGITO

As per the international reports, the average cost of a security data breach is more than $3.5 million. And increasing risk from unauthorized access, encourage us to work with a highly secured and compliant annotation platform backed with quality certified delivery centers protect clients from costly mistakes th at arise from poor data security practices.

As, for the vast majority of our clients, data security and IP Protection are often prime concerns before they partner with us. Cogito mandates security adherence at all times by all Employee(s) and has put in place strict measures to ensure client data security and confidentiality. Listed below are the stringent measures we have put in place to protect our Client Interests:

CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENTS (NDAs)

Our policies ensure confidentiality of Client Data is maintained at all times:

a. To ensure the security and confidentiality of information, a Confidentiality Agreement is executed with each client and all private concerns are respected.

b. We also sign appropriate NDAs with each individual Employee working on our Client's Project to ensure the client interests is protected adequately.

c. Employees cannot disclose any proprietary information directly or indirectly to anyone outside the project team or company, or use, copy, publish, summarize or remove such information from the company premises.

EMPLOYEE BACKGROUND CHECKS

a. Thorough background checks (including criminal checks) are performed for all employees before on-boarding.

b. Data access is restricted only to employees whose background checks have been successfully completed.

c. On-going background checks and diligence are also performed for existing employees.

PHYSICAL SECURITY

a. Cogito is divided into 2 well-defined zones (Front office & Admin, and Production Area) with protected and non-protected areas.

b. Agents are not allowed to carry pen and paper on production floor.

c. Electronic Devices such as mobile phones, PDA etc are not allowed on the production floor.

d. Random Audits to ensure security policies are followed.

e. Disciplinary action for the non-compliance.

f. 24*7 monitoring of all infrastructure by on-site security personnel.

ACCESS CONTROL

a. Entrance in production area is restricted via Biometric Access.

b. Production area is under 24x7 CCTV surveillance.

c. Limited, applicable application access provided as per operations.

d. CDs, DVDs, pen drive, disk drive, or any other storage devices are not allowed in the production areas without prior permission from authorized management team members.

e. Well defined passwords & access control for authorized internal persons.

DATA SECURITY

a. The Data received from the client during the time of processing is via approved and secure channels only.

b. Data sharing protocols are complied with, restricting data visibility to authorized personnel only, which is further tracked to ensure safe disposal of data after necessitated usage. All such data transfers are logged and recorded for auditing and compliance purposes.

c. No local storage provided, all data are stored at central storage.

d. Regular audits of the central storage server.

EMAIL SECURITY

a. Agents are given organization email facility only when required.

b. No mails can be sent outside the organization from the given mail facility (except pre-approved domains).

INTERNET ACCESS SECURITY

a. Restricted access to internet sites is allowed only if it is a process requirement.
b. Continuous monitoring of web traffic and disciplinary actions taken for violations.
c. Professional firewall system restricts the users to surf or access unauthorized sites.
d. Limited access to the network through login IDs and password protection.
e. High level of anti-spam, anti-virus and anti-spywares ensure that the data is not hacked or leaked outside the organization.

AWARENESS PROGRAMS

a. All employees are trained on the security measures which are enforced on every individual across the organizational hierarchy. Regular update trainings and security quizzes are conducted to assess employee understanding.
b. Regular awareness program are conducted on data protection and its legality.
c. Awareness of information security through class room sessions, intranet sessions, posters, mailers etc.

TOLERANCE POLICY

Cogito mandates security adherence at all times by all employees and has a zero percent tolerance towards any unethical practice. All such issues are dealt with in the strictest manner to ensure minimum impact to the service delivery.

CLIENT SUGGESTIONS

In addition to all the best practices that we regularly implement, we welcome suggestions from our clients to further strengthen our data security measures. We offer to abide by any specific requests that a client makes to improve the security of their intellectual property.