Dear Reader,

You are receiving this message from the Saboo e-Solutions Resource Center. If you do not wish to receive future issues of Resource Center Learning please reply with the subject UNSUBSCRIBE. Further, if you know of others who would be interested in receiving the Saboo e-Solutions' Newsletter, please forward this email or send their names and email addresses to resources@sabooe-solutions.com.

The security of Clients' data is of paramount importance to BPO Service Providers. They are committed to respecting, protecting and safeguarding privacy and confidentiality of data and information entrusted to them by their clients. Several levels of safeguards can be kept in place to ensure complete protection.

Physical Security

Generally BPO service providers' facilities can have a 3-tier physical security system. Most of the BPO service providers' facilities restrict physical access to the processing and server environment. Each such facility can implement world-class Finger Scan Systems to safeguard the premises from any unauthorized entry. The 3-tier security system is explained below:

Entry of Individual

Physical checking: Security guards are on 24-hour duty at all the locations.

Finger Scan Devices

FINGERSCAN is a multi-functional personal identification device that takes a three-dimensional scan of a person's finger and compares it against a previously enrolled record. Each person has an unclassified identification number, which is used to call up his or her finger record for verification purposes. Although recommended by industry leaders, this type of security measure is not much prevalent yet.

Access Control Cards

Employees and support staff are provided Access Control Cards that permit entry into the office and logs their movement in and out of the office.

Personal Security

Generally every BPO Service Provider has strict personal security system. Salient features of the personal security system are mentioned below:

- ⇨ Every employee of BPO Service Provider signs Non-disclosure agreements (NDA) before joining the company
- ⇨ Personal belongings like bags, cell phones, briefcases are not allowed in the processing center
- ⇨ Internet access is restricted within the processing center
- ⇨ Personal Security is maintained through physical inspections and video surveillances
- ⇨ Usage of removable media is prohibited within the processing center

Machine Level Security

To safeguard the confidentiality of the Clients' data, generally every BPO Service Provider maintains highest degree of Machine Level Security. Features of the Machine Level Security System are as follows:

- ⇨ Customer data security is taken care of by encrypted user authentication, login privileges, password management and control systems
- ⇨ Client creates his/her own password so that no one (not even the ASP personnel wherever applicable) can see or have access to Client's passwords. Generally, the user changes the passwords every 30 days.
- ⇨ If a machine is inactive for 10 minutes, the user has to log in again.
- ⇨ If a login fails thrice, a user must contact the Systems Administrator who restores rights only upon confirmation of user identification.

Network And System Security

Generally the following measures are taken to ensure system security.

- ⇨ BPO Service Providers ensure a paperless environment so data cannot be removed from the facility. There is no physical movement of clients' documents/data as access is only through controlled point-to-point tunneling protocols, 128 bit encryption and SSL secure FTP with user login ensured added protection
- ⇨ Individual accesses within the processing center are controlled through a dedicated Proxy Server
- ⇨ Firewalls are used to protect against threats from any external sources
- ⇨ All Internet browsing and FTP downloads within processing center are restricted and monitored.

Disaster Recovery

BPO Service Providers generally maintain 3 levels back-up system – daily incremental, weekly and monthly. Daily disk and DLT (Digital Linear Tape) based incremental back up of data is done for immediate recovery of data. Weekly and monthly back-ups are also taken in disk and also on DLT. Sometimes data on DLT is kept at an office in another location. This is kept as a back up office to manage disaster effectively and promptly. This facility is fully networked with provisions for necessary high-speed communication links and can be made functional within a short time frame in times of emergency to ensure utmost security.

We appreciate and value your feedback very much. Let us know how we can help make this communication vehicle and the learning resource more valuable to you.

You can always e-mail us at resources@sabooe-solutions.com or call at 1-646-435-7887(USA) or 020 7993 8870(UK) or 91 33 2236 5173 (India).

Sincerely,

Editorial Board, Resource Center
Saboo e-Solutions Pvt. Ltd.
6, Ganesh Chandra Avenue
Kolkata-700013, India
www.sabooe-solutions.com