

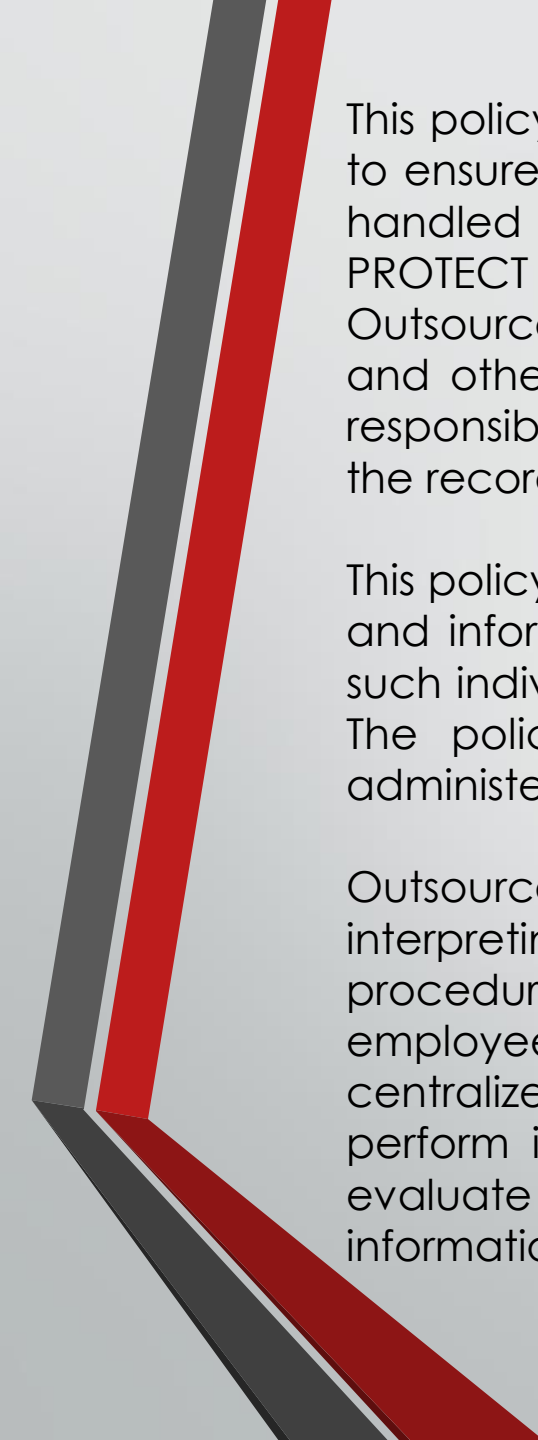


AN ISO/IEC 27001:2013 Certified Company

**OutsourceBiz India Private Limited**  
BusinessProcess **Evolution**

# **Computer Network, Internet Security Policy and Procedures**

## **Data Security and Protection**



This policy is to establish administrative direction, procedural requirements and technical guidance to ensure the appropriate protection of OutsourceBiz India Pvt. Ltd.' s documents and information handled by and stored on OutsourceBiz India Computer Networks. The main goal of this policy is to PROTECT the business - OutsourceBiz India Pvt. Ltd. and OutsourceBiz India Pvt. Ltd. Customers. OutsourceBiz India Computer Network stores PHI (Personal Health Information as per US HIPAA Laws) and other pertinent information for hundreds of thousands of Customer Clients/Patients. It is the responsibility of OutsourceBiz to PROTECT this information as their information is being processed, or the records are stored in archives.

This policy applies to all authorized users who access OutsourceBiz India Pvt. Ltd. computer networks and information system. Throughout policy, the word USER will be used to collectively refer to all such individuals who are AUTHORIZED to work on OutsourceBiz Computer Network and peripherals. The policy also applies to all computer and data communication systems owned by or administered by OutsourceBiz India Pvt. Ltd.

OutsourceBiz is responsible for establishing, maintaining, implementing, administering, and interpreting organization-wide information systems security policies, standards, guidelines, and procedures. While responsibility for information systems security on a day-to-day basis is every employee's duty, specific guidance, direction, and authority for information systems security is centralized for OutsourceBiz in the Information Technology Department. This department will perform information systems risk assessments, prepare information systems security action plans, evaluate information security products, and perform other activities necessary to assure a secure information systems environment.

## **NETWORK SECURITY POLICY**

INTRUSION DETECTION SYSTEM – All the Data operation areas of OutsourceBiz are closely observed by CCTV Monitoring 24/7. A close observer is appointed to monitor any malicious activity or policy violation of network and systems of OutsourceBiz. Any detected activity or violation is typically reported to the OutsourceBiz India Pvt. Ltd. Management Committee. Each Floor has an assigned Floor Supervisor for each shift, and each of these Floor Supervisor has a designated Assistant – who takes over during the time the Supervisor has to be away from the floor. The Floor Supervisor workstation is located at a strategic location from where – all the workstation monitors in the floor is visible.

## **ANTIVIRUS**

Antivirus software is used to safeguard computers from malware - including Viruses, Computer Worms, and Trojan horses. Antivirus software will also remove or prevent Spyware and Adware, along with other forms of malicious programs. All systems are protected with AVG antivirus Business Edition with features including Antispam protection, Antispyware protection, Firewall protection, Online Protection Shield, Link scanner Protection, Anti Rootkit protection and Email scanning.

OutsourceBiz IT Department will periodically check the individual systems to monitor the activity of installed antivirus and full scanned of the system.

## **BACKUP AND RESTORE STRATEGIES**

OutsourceBiz Information Technology Department recognizes that the backup and maintenance of data for servers is critical to the viability and operations of the respective OutsourceBiz departments.

Members of OutsourceBiz India Pvt. Ltd. store their important data in the File server, which is located in the OutsourceBiz office premises.

The content of data backed up varies from server-to-server. Three most important servers are

- 1. Application Server (s)**
- 2. Database Server (s)**
- 3. File Server(s)**

In Application Server (s) all downloaded client data from Secured FTP (or received via any other valid source) is stored. While processing, all the data (Provided by the client) is preserved as per the client's security policy and their requirement. Once all the processing for a batch of data is completed and sent to the client, this data is compressed and stored in another location of OutsourceBiz network and the burned to DVD for future reference and safe keeping.

Database backup is taken daily from the direct access drive in database server.

All members of OutsourceBiz India Pvt. Ltd. keep their important data on the File Server and OutsourceBiz IT department periodically saves the data at another location of the OutsourceBiz Network.

## **SERVERS**

Operating system of Application server and Database servers is Windows Server 2017 Standard edition.

Operating system for the File server is Windows Server 2019.

Application Server is a web server where custom made applications (developed by OutsourceBiz software team) are hosted in the IIS. Authorized Users connect to the application with browser from OutsourceBiz desktop system.

Database Server OS is Microsoft SQL Server 2017 - Standard Edition.

The File Server is attached to the network to provide a location for shared disk space. OutsourceBiz users store their data in specific folders and process their job.

## **PASSWORD POLICY**

On the desktop computers, password is assigned when enrolled on the system.

System Administrator changes the password periodically and advises the specific users.

All servers of OutsourceBiz are protected by a very strong password policy. Users have right to access the servers if warranted and permitted by the Systems Administrator.

Passwords are required to be alpha numeric and the number of characters is minimum 10. Passwords must be changed for every server - once a month. This is mandatory

# SECURITY FOR WORK AREA (DATA ENTRY/CLAIMS PROCESSING)

## LOCKED DOOR

OutsourceBiz Data Entry/Claims Processing area is a highly secured zone. Main door of data operation area is secured by an access control system. Only authorized persons are permitted to access the data operation area by swapping their Magnetic Access Card at the entry door. ABSOLUTELY NO VISITORS ARE PERMITTED IN THIS AREA UNLESS THEY HAVE EACH SIGNED A HIPAA APPROVED SECURITY CLEARANCE FORM AND ARE ACCOMPANIED AT ALL TIMES BY A SENIOR MEMBER OF THE OutsourceBiz India Pvt. Ltd. MANAGEMENT, AUTHORIZED FOR THIS PURPOSE. NO EXCEPTIONS TO THIS RULE IS ALLOWED.

## EMAIL POLICY

Email is a business communication tool and users are required to use this tool in a responsible, effective and lawful manner. All OutsourceBiz email users have a responsibility to maintain the company's security policy. Each and every employee signed a CONTRACT before being allowed to use/access the Official OSB email system. This policy is an integral part of OutsourceBiz Employee Contract that each employee signs while being accepted for employment.

1. An email message may go to persons other than the intended recipient. If it contains confidential or commercially sensitive information or data, this could be damaging to OutsourceBiz's reputation.
2. Letters, files and other documents attached to emails may belong to others. By forwarding this information, without permission from the sender, to another recipient, you may be liable for copyright infringement.

3. Email is a fast form of communication. Often messages are written and sent simultaneously, without the opportunity to check for accuracy. If any OutsourceBiz Employee sends emails with any libelous, defamatory, offensive, racist or obscene remarks, they will be subject severe disciplinary action, including summary dismissal and/or legal action.

All email account of OutsourceBiz can be monitored without prior notification. If there is evidence that any email user of OutsourceBiz is not adhering to the guidelines set out in this policy, the company reserves the right to take disciplinary action, including termination and/or legal action.

### **WEBSITE ACCESS POLICY**

This policy setting allows OutsourceBiz to restrict users access to the certain websites. OutsourceBiz Users are only authorized to access only the sites which are related to their work. OutsourceBiz restricts certain type of web content such as streaming media or content that might violate OutsourceBiz's website access policy.

OutsourceBiz Employees are NOT allowed to access non-business related email account via the WEB, while using company's machine.

### **MOBILE COMPUTING AND PORTABLE STORAGE**

Users are not allowed to bring their own PDA in the data operation facility area. Any storage media like USB jump drives, smart phones, IPODS, Portable SD or CF Memory Cards are strictly prohibited in the facility area.

## **WIRELESS DEVICE ACCESS POLICY**

The goal of this policy is to protect data and information from unauthorized use and malicious attack. In order to provide wireless access to authorized users to OSB's network, every device must be assigned with static IP and the MAC address of that device should be authenticated to OSB's router. THERE WILL BE NO WIRELESS ACCESS TO ANY OF THE SERVERS OR PCs.

## **INTERNET FACING GATEWAY CONFIGURATION**

Not all desktops in facility area of OutsourceBiz are connected to the internet. This privilege is allowed as per requirement. Only those PCs can connect to internet in the facility area, which MAC addresses are allowed in the router. Users DO NOT HAVE ACCESS TO administrative controls in their system.

Until there are no more bad guys in the world and everyone agrees to mind his or her own business, the process of managing security never ends. The scope of this policy will change over time as newer threats are created. This policy will be reviewed from time to time and changes may be made by the Management Committee with approval from the Resident Director, and final concurrence from the Chairman and Managing Director.

This document is not all inclusive. There are many other functions and services that OutsourceBiz may provide that demand specific security provisions.

