

# BLB LIMITED

4760-61/23A, Ansari Road, Darya Ganj, New Delhi – 110002.

---

## NETWORK SECURITY POLICY

### POLICY STATEMENT:


"It shall be the responsibility of the I.T. Department to provide adequate protection and confidentiality of all corporate data and proprietary software systems, whether held centrally, on local storage media, or remotely, to ensure the continued availability of data and programs to all authorized members of staff, and to ensure the integrity of all data and configuration controls."

### MAIN SECURITY POLICIES:

- Confidentiality of data is to be maintained through discretionary and mandatory access controls.
- Access to data on laptops and computers is to be secured through encryption or other means, to provide confidentiality of data in the event of loss or theft of equipment.
- Only authorized and licensed software may be installed, and installation may only be performed by I.T. Department staff.
- Use of media from external sources is strictly prohibited within the Organization.
- Workstation configurations may only be changed by I.T. Department staff.
- To prevent the loss of availability of I.T. resources, measures must be taken to backup data, applications and the configurations of workstations. Backup is taken on a weekly basis.

### LAN SECURITY:


#### 1) Workstations:

- a) Users will change their passwords every 14 days.
  - b) Users must logout of their workstations when they leave their workstation for any length of time. Alternatively, Windows workstations may be locked.
  - c) All unused workstations must be switched off after working hours.
  - d) Assigning security equivalences that give one user the same access rights as another user will be avoided where possible.
  - e) Users access to data and applications will be limited by the access control features.
  - f) The system auditing facilities will be enabled.
  - g) Unique passwords will be used.
- 

# BLB LIMITED

4760-61/23A, Ansari Road, Darya Ganj, New Delhi – 110002.

---

- h) The number of grace logins will be limited to 3.
  - i) Network login time restrictions will be enforced preventing users from logging in to the network outside normal working hours.
  - j) In certain areas users will be restricted to logging in to specified workstations only.
- 2) Wiring:
- a) All network wiring will be fully documented with I/O port Numbering
  - b) All unused network points will be de-activated when not in use.
  - c) Users must not place or store any item on top of network cabling.
- 3) Monitoring Software:
- a) The use of LAN analyzer and packet sniffing software is restricted to the I.T. Department.
  - b) LAN analyzers and packet sniffers will be securely locked up when not in use.
- 4) Servers & LAN Equipment:
- a) All servers will be kept securely under lock and key.
  - b) Access to the system console and server disk/tape drives will be restricted to authorized I.T. Department staff only.
  - c) LAN equipments, routers, switches will be kept in secure server rooms.
  - d) Access to server rooms will be restricted to I.T. Department staff only. Other staff, and contractors requiring access to hub rooms will notify the I.T. Department in advance so that the necessary supervision can be arranged.
- 5) Electrical Security:
- a) All servers will be fitted with UPS's that also condition the power supply.
  - b) All routers, switches and other critical network equipment will also be fitted with UPS's.
  - c) In the event of a mains power failure, the UPS's will have sufficient power to keep the network and servers' running until the generator takes over.
  - d) All UPS's will be tested periodically.
- 6) Inventory Management:
- The I.T. Department will keep a full inventory of all computer equipment and software in use throughout the Company.
- 

# BLB LIMITED

4760-61/23A, Ansari Road, Darya Ganj, New Delhi – 110002.

---

## SERVER SPECIFIC SECURITY:

1. This section applies to Windows and Linux servers.
2. The operating system will be kept up to date and patched on a regular basis.
3. Servers will be checked weekly for viruses.
4. Servers will be locked in a secure room.
5. Remote management passwords will be different to the Admin/Administrator/root password.
6. Users possessing Admin/Administrator/root rights will be limited to trained members of the I.T. Department staff only.
7. Use of the Admin/Administrator/root accounts will be kept to a minimum.

For BLB Limited



(Compliance Officer)

# BLB LIMITED

4760-61/23A, Ansari Road, Darya Ganj, New Delhi – 110002.

---

## USER MANAGEMENT AND ACCESS CONTROL POLICY

### 1. PURPOSE:

Access control procedures will cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention shall be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

### 2. SCOPE:

The policy applies to all the employees including, but not limited to full time employees, part-time employees, contractors, temporary workers, trainers, volunteers and anyone else granted access to sensitive information by the Company. Further, the policy applies to all systems, computer networks and applications as well as facilities which processes, stores or transmits electronic information.

### 3. DESCRIPTION:

The policy consists of the following sections: User/Application Management and Access Control Policy.

#### i) USER/APPLICATION MANAGEMENT:

- a. Formal procedures shall be in place to control the allocation of access rights to information systems and Application/services. Users shall be granted access based upon the principle of applying the least privilege required for achieving their desired job function.
  - b. Users shall be granted access to information, data and applications on a "need to know" basis. Access shall be restricted according to the user's requirement to access information, data or application on the basis of least privilege to achieve the desired business function.
  - c. An accurate date and time shall be maintained on all systems.
  - d. There shall be a one-to-one relationship between user Ids and individuals. Access to computing resources (e.g. files, applications, and databases) via shared User Ids is strictly prohibited.
- A

# BLB LIMITED

4760-61/23A, Ansari Road, Darya Ganj, New Delhi - 110002.

---

## ii) ACCESS CONTROL:

- a) Users will only be given sufficient rights to all systems to enable them to perform their job function. User rights will be kept to a minimum at all times.
- b) Access to the network/servers and systems will be by individual username and password.
- c) Usernames and passwords of must not be shared by users.
- d) Usernames and passwords should not be written down.
- e) All users will have an alphanumeric password of at least 6 characters.
- f) Passwords will expire every 14 days and must be unique.
- g) The user account will be locked after 3 incorrect attempts.
- h) Default passwords on systems such as SQL Server will be changed after installation.
- i) Access to the network/servers will be restricted to normal working hours. Users requiring access outside normal working hours must request such access in writing on the forms provided by the I.T. Department.

For BLB Limited ✓



(Compliance Officer)

# BLB LIMITED

4760-61/23A, Ansari Road, Darya Ganj, New Delhi – 110002.

---

## PASSWORD POLICY

- The System and The User IDs are password protected and use of wrong password for more than 3 times, shall lock the original password and the User has only option to contact Administrator for renewal of passwords.
- Password set by administrator must be changed at the time of First login.
- The user can change their password any time they wish to do so. However, users shall not be able to operate the system unless they change the password on 15<sup>th</sup> day from the last renewal of password.
- Passwords must consist of a mixture of at least 6 alphanumeric characters, and must be changed periodically and must be unique.
- The renewed password must be alphanumeric, preferably with one special character.
- The renewed password shall not be the same as of the last password.
- Passwords are not shared and treated as confidential information under company policy.
- Use both upper and lower case characters; and
- Passwords must be changed periodically i.e every 14 days(Max.)
- The Login id of the user and renewed password shall never be the same.
- The Password must not be too short or too long. There should be minimum six characters and not more than twelve characters.
- System controls to ensure that the Password is encrypted at members end so that employees of the member cannot view the same at any point of time.

For BLB Limited



(Compliance Officer)

# BLB LIMITED

4760-61/23A, Ansari Road, Darya Ganj, New Delhi – 110002.

---

## DATA BACK-UP POLICY

### PURPOSE AND SCOPE:

This policy applies to all servers in the IT Department. The purpose of this policy is as follows:

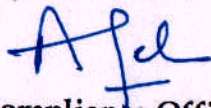
- To safeguard the information assets of BLB Limited.
- To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster.
- To permit timely restoration of information and business processes, should such events occur.
- To manage and secure backup and restoration processes and the media employed in the process.

### BACK-UP POLICY:

The back-up policy of the Company is as follows:

- Back-up of all servers located in Local office & Co-lo premises will be taken on a daily basis to another machine/system located in 4760-61/ Ansari Road Daryaganj, New delhi-110002.
- Weekly backup to external USB hard drive and these backup files will be stored off-site.

For BLB Limited



(Compliance Officer)