ARYA FIN-TRADE SERVICES (INDIA) PRIVATE LIMITED

INFORMATION SECURITY & NETWORK SECURITY POLICY

Version	**2024/01.02**
Review Date	**05/04/2024**
Review & Approved by	**Reviewed by Technology Committee & Approved by Board of Directors**

1. 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 authorised members of staff, and to ensure the integrity of all data and configuration controls."

Summary of Main Security Policies.

1.1 Confidentiality of all data is to be maintained through discretionary and mandatory access controls.
1.2 Internet and other external service access is restricted to authorised personnel only.
1.3 Access to data on all laptop computers is to be secured through encryption or other means, to provide confidentiality of data in the event of loss or theft of equipment.
1.4 Only authorised and licensed software may be installed, and installation may only be performed by I.T. Department staff.
1.5 The use of unauthorized software is prohibited. In the event of unauthorized software being discovered it will be removed from the workstation immediately.
1.6 Data may only be transferred for the purposes determined in the Company's data-protection policy.
1.7 All diskette drives and removable media from external sources must be virus checked before they are used within the Company.
1.8 Passwords must be as per Password Policy.
1.9 Workstation configurations may only be changed by I.T. Department staff.
1.10 The physical security of computer equipment will conform to recognized loss prevention guidelines.
1.11 To prevent the loss of availability of I.T. resources measures must be taken to backup data, applications and the configurations of all workstations.
1.12 A business continuity plan will be developed and tested on a regular basis.

2. VIRUS PROTECTION

2.1 The I.T. Department will have available up to date virus scanning software for the scanning and removal of suspected viruses.
2.2 Corporate file-servers will be protected with virus scanning software.
2.3 Workstations will be protected by virus scanning software.
2.4 All workstation and server anti-virus software will be regularly updated with the latest anti-virus patches by the I.T. Department.
2.5 No disk that is brought in from outside the Company is to be used until it has been scanned.
2.6 All systems will be built from original, clean master copies whose write protection has always been in place. Only original master copies will be used until virus scanning has taken place.
2.7 All removable media containing executable software (software with .EXE and .COM extensions) will be write protected wherever possible.
2.8 All demonstrations by vendors will be run on their machines and not the Company's.
2.9 Shareware is not to be used, as shareware is one of the most common infection sources. If it is absolutely necessary to use shareware it must be thoroughly scanned before use.
2.10 New commercial software will be scanned before it is installed as it occasionally contains viruses.
2.11 All removable media brought in to the Company by field engineers or support personnel will be scanned by the IT Department before they are used on site.
2.12 To enable data to be recovered in the event of a virus outbreak regular backups will be taken by the I.T. Department.
2.13 Management strongly endorse the Company's anti-virus policies and will make the necessary resources available to implement them.
2.14 Users will be kept informed of current procedures and policies.

2.15 Users will be notified of virus incidents.
2.16 Employees will be accountable for any breaches of the Company's anti-virus policies.
2.17 Anti-virus policies and procedures will be reviewed regularly.
2.18 In the event of a possible virus infection the user must inform the I.T. Department immediately. The I.T. Department will then scan the infected machine and any removable media or other workstations to which the virus may have spread and eradicate it.

3. PHYSICAL SECURITY OF COMPUTER EQUIPMENT

Physical Security of computer equipment will comply with the guidelines as detailed below.

3.1 DEFINITIONS

3.1.1 Area
Two or more adjacent linked rooms which, for security purposes, cannot be adequately segregated in physical terms.

3.1.2 Computer Server Room
Mainframe, minicomputer, fileserver plus all inter-connected wiring, fixed disks, telecommunication equipment, ancillary, peripheral and terminal equipment linked into the mainframe, contained within a purpose built computer Server Room .

3.1.3 Computer Equipment
All computer equipment not contained within the COMPUTER SERVER ROOM which will include PC's, monitors, printers, disk drives, modems and associated and peripheral equipment.

3.1.4 High Risk Situation(s)
This refers to any room or AREA which is accessible at ground floor level
At first floor level, but accessible from adjoining roof at any level via external fire escapes or other features providing access rooms in remote, concealed or hidden areas.

3.1.5 Lockdown Device(s)
A combination of two metal plates, one for fixing to furniture, or the building structure, and the other for restraining the equipment which is immobilised when the two plates are locked together. The plate for restraining the equipment should incorporate an enclosure or other mechanism which will hinder unauthorised removal of the outer PC casing and render access to internal components difficult.

3.1.6 Approved
Approved security system.

3.1.7 Personal Computers (PC's)
Individual computer units with their own internal processing and storage capabilities.

3.2.1 Security Marking
All computer hardware should be prominently security marked by branding or etching with the name of the establishment and area postcode. Advisory signs informing that all property has been security marked should be prominently displayed externally. The following are considered inferior methods of security marking; text comprised solely of initials or abbreviations, marking by paint or ultra violet ink (indelible or otherwise), or adhesive labels that do not include an etching facility.

3.2.2 Locking of PC Cases
PC's fitted with locking cases will be kept locked at all times.

3.2.3 Siting of Computers
Wherever possible, **COMPUTER EQUIPMENT** should be kept at least 1.5 metres away from external windows in **HIGH RISK** SITUATIONS.

3.23.2.5 Blinds
All external windows to rooms containing **COMPUTER EQUIPMENT** at ground floor level or otherwise visible to the public should be fitted with window blinds or obscure filming.

3.2.6 Lockdown Devices
For any item of **COMPUTER EQUIPMENT** with a purchase price in excess of 1,500 which is not directly covered by an intruder alarm, the processing unit should have a **LOCKDOWN DEVICE** fitted to the workstation. **LOCKDOWN DEVICES** should conform to loss prevention standards. Mobile workstations are unlikely to be suitable for these devices. When it is impossible or undesirable to anchor hardware, such equipment can be moved to a security store or cabinet outside normal hours of occupation.

3.2.7 Intruder Alarm
An intruder alarm incorporating the following features should be installed. Installation, maintenance and monitoring by an APPROVED company.

3.2.11 Check Detectors

Building managers should ensure, as part of their normal duties at locking up time, that internal space detectors have not been individually obscured or had their field of vision restricted.

3.3. Computer Server Room

3.3.1 The computer Server Room should be housed in a purpose built room.

3.3.2 There shall not be Wooden Walls or Wooden Floorings.

3.3.3 Secure doors giving access to the room or AREA, from within the building, should be solid.

3.3.4 The computer Server Room should contain an adequate air conditioning system to provide a stable operating environment to reduce the risk of system crashes due to component failure.

3.3.5 No water, rain water or drainage pipes should run within or above the computer Server Room to reduce the risk of flooding.

3.3.7 Power points should be raised from the floor to allow the smooth shutdown of computer systems in case of flooding.

3.3.8 Where possible generator power should provided to the computer Server Room to help protect the computer systems in the case of a mains power failure.

3.3.9 Access to the computer Server Room is restricted to IT Department staff.

3.3.10 All contractors working within the computer Server Room are to be supervised at all times and the It Department is to be notified of their presence and provided with details of all work to be carried out, at least 48 hours in advance of its commencement.

4. ACCESS CONTROL

4.1 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.

4.2 Users requiring access to systems must make a written application on the forms provided by the I.T Department.

4.3 Where possible no one person will have full rights to any system. The I.T. Department will control network/server passwords and system passwords will be assigned by the system administrator in the end-user department. The system administrator will be responsible for the maintaining the data integrity of the end-user department's data and for determining end-user access rights.

4.4 Access to the network/servers and systems will be by individual username and password, or by smartcard and PIN number/biometric.

4.5 Usernames and passwords must not be shared by users.

4.6 Usernames and passwords should not be written down.

4.7 Usernames will consist of initials and surname.

4.8 All users will have password as per Password Policy.

4.9 Default passwords on systems such as Oracle and SQLServer will be changed after installation.

4.10 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.

4.11 File systems will have the maximum security implemented that is possible. Where possible users will only be given Read and Filescan rights to directories, files will be flagged as read only to prevent accidental deletion.

5 LAN Security

Hubs & Switches

5.1 LAN equipment, hubs, bridges, repeaters, routers, switches will be kept in secure hub rooms. Hub rooms will be kept locked at all times. Access to hub 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.

Workstations

5.2 Users must logout of their workstations when they leave their workstation for any length of time. Alternatively Windows worksations may be locked.

5.3 All unused workstations must be switched off outside working hours.

Wiring

5.4 All network wiring will be fully documented.

5.5 All unused network points will be de-activated when not in use.

5.6 All network cables will be periodically scanned and readings recorded for future reference.

5.7 Users must not place or store any item on top of network cabling.

5.8 Redundant cabling schemes will be used where possible.

Monitoring Software

5.9 The use of LAN analyser and packet sniffing software is restricted to the I.T. Department.

5.10 LAN analysers and packet sniffers will be securely locked up when not in use.

5.11 Intrusion detection systems will implemented to detect unauthorised access to the network

Servers

5.12 All servers will be kept securely under lock and key.

5.13 Access to the system console and server disk/tape drives will be restricted to authorised I.T. Department staff only.

Electrical Security

5.14 All servers will be fitted with UPS's that also condition the power supply.

5.15 All hubs, bridges, repeaters, routers, switches and other critical network equipment will also be fitted with UPS's.

5.16 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.

5.17 Software will be installed on all servers to implement an orderly shutdown in the event of a total power failure.

5.18 All UPS's will be tested periodically.

Inventory Management

5.19 The I.T. Department will keep a full inventory of all computer equipment and software in use throughout the Company.

5.20 Computer hardware and software audits will be carried out periodically via the use of a desktop inventory package. These audits will be used to track unauthorised copies of software and unauthorised changes to hardware and software configurations.

6. Server Specific Security

This section applies to Windows, UNIX, Linux and Novell servers.

6.1 The operating system will be kept up to date and patched on a regular basis.

6.2 Servers will be checked daily for viruses.

6.3 Servers will be locked in a secure room.

6.4 Where appropriate the server console feature will be activated.

6.5 Remote management passwords will be different to the Admin/Administrator/root password.

6.6 Users possessing Admin/Administrator/root rights will be limited to trained members of the I.T. Department staff only.

6.7 Use of the Admin/Administrator/root accounts will be kept to a minimum.

6.8 Assigning security equivalences that give one user the same access rights as another user will be avoided where possible.

6.9 Users access to to data and applications will be limited by the access control features.

6.10 Intruder detection and lockout will be enabled.

6.11 The system auditing facilities will be enabled.

6.12 Users must logout or lock their workstations when they leave their workstation for any length of time.

6.13 All unused workstations must be switched off outside working hours.

6.14 All accounts will be assigned a password as per Password Policy.

6.15 The number of concurrent connections will be limited to 1.

6.16 Network login time restrictions will be enforced preventing users from logging in to the network outside normal working hours.

6.17 In certain areas users will be restricted to logging in to specified workstations only.

7. Wide Area Network Security

7.1 Wireless LAN's will make use of the most secure encryption and authentication facilities available.

7.2 Users will not install their own wireless equipment under any circumstances.

7.3 Dial-in modems will not be used if at all possible. If a modem must be used dial-back modems should be used. A secure VPN tunnel is the preferred option.

7.4 Modems will not be used by users without first notifying the I.T. Department and obtaining their approval.

7.5 Where dial-in modems are used, the modem will be unplugged from the telephone network and the access software disabled when not in use.

7.6 Modems will only be used where necessary, in normal circumstances all communications should pass through the Company's router and firewall.

7.7 Where leased lines are used, the associated channel service units will be locked up to prevent access to their monitoring ports.
7.8 All bridges, routers and gateways will be kept locked up in secure areas.
7.9 Unnecessary protocols will be removed from routers.
7.10 The preferred method of connection to outside Companies is by a secure VPN connection, using IPSEC or SSL.
7.11 All connections made to the Company's network by outside Companys will be logged.

8. TCP/IP & Internet Security

8.1 Permanent connections to the Internet will be via the means of a firewall to regulate network traffic.
8.2 Permanent connections to other external networks, for offsite processing etc., will be via the means of a firewall to regulate network traffic.
8.3 Where firewalls are used, a dual homed firewall (a device with more than one TCP/IP address) will be the preferred solution.
8.4 Network equipment will be configured to close inactive sessions.
8.5 Where modem pools or remote access servers are used, these will be situated on the DMZ or non-secure network side of the firewall.
Workstation access to the Internet will be via the Company's proxy server and website content scanner
8.7 All incoming e-mail will be scanned by the Company's e-mail content scanner.

Network Security

1. Terminals in the form of workstations or devices and peripherals connected on a network shall be accessed only by the authorized personnel.
2. Proper access control mechanisms and procedures shall be in place to restrict the access through terminals to authorized personnel only.
3. In a networked computing environment, the user is often required to access the systems from remote locations or through communication lines.
4. Login ID and Password shall be used as a first level authorization. Depending on the criticality of the IS resource two-factor authorizations shall be used.

Firewalls

Organizational networks have one or many logical gates through which data in transit leaves and enters the organizational networks. Such network access connects the secure organizational networks to unsecured external networks. Firewalls are software devices, which function as logical security guards frisking every packet that enters/leaves the secure organizational networks.

The following are the policies framed in this regard:

1. All the traffic from inside to outside and from outside to inside shall pass only through the firewall. There shall be no alternate route possible for the network traffic. Such Network Traffic shall also cover Wireless network traffic.
2. The organizational security policy shall determine what traffic must be permitted to pass through the firewall.

Controls with regards to the firewalls are classified in the following groups:

1. Physical Security Controls: Machines in various locations including servers, firewalls, nodes and communicating devices have to be physically secured.
2. Operating System Security: A Firewall must run a secure and tamper-proof OS. The network administrator shall ensure that patches with regards to the OS are up to date.
3. Change Control Procedures: The network administrator shall ensure that the patching process is complete. Whenever there is any change in the access rules it must be properly authorized and managed. If the privileges of the users are changed it must be properly authorized and managed.
4. Verification of documents: The documents with regards to the network diagram configuration have to be thoroughly examined for vulnerabilities.

Examination of log:

Firewalls provide facility for logging every transaction that passes through it. These logs shall be examined at regular intervals by technical experts. It is essential to ensure that the log files are not tampered with.
Policy shall be reviewed annually or as and when necessary.