

I.T. SECURITY POLICY
For
SHAKUMBHARI ENTERPRISES

Prepared by:

MR.VIVEK SHARMA
General Manager - IT

Version 1.1

© SHAKUMBHARI ENTERPRISES

The intellectual property contained within this publication is the property of SHAKUMBHARI ENTERPRISES.

This publication is protected by copyright. Any unauthorized projection, editing, copying, reselling and rental or distribution of the whole or part of this publication in whatever form (including electronic and magnetic forms) is prohibited.

Effective from: 15th June 2020

Security Patching Policy

Owner:	MR.VIVEK SHARMA General Manager - IT
Related Documents:	Information Security Policy, Computer and Network usage, Vulnerability Scan policy.

Document Control

This document is subject to change control and any amendments will be recorded below.

Change History

Version	Date	Circulation	Changes
1.0	15/06/2006	HR, IT, Finance and CEO	First formal Issue
1.1	15/09/2007	HR, IT, Finance and CEO	Revision
1.2	15/09/2008	HR, IT, Finance and CEO	Revision
1.3	15/09/2009	HR, IT, Finance and CEO	Revision
1.4	15/09/2010	HR, IT, Finance and CEO	Revision
1.5	15/09/2011	HR, IT, Finance and CEO	Revision
1.6	15/09/2012	HR, IT, Finance and CEO	Revision
1.7	15/09/2013	HR, IT, Finance and CEO	Revision
1.8	15/09/2014	HR, IT, Finance and CEO	Revision
1.9	15/09/2015	HR, IT, Finance and CEO	Revision
2.0	15/09/2016	HR, IT, Finance and CEO	Revision

Version Awareness

The audience of this document should be aware that a physical copy may not be the latest available version. The latest version, which supersedes all previous versions, is available at [//Parasvanath/IT Policies](#). Those to whom this policy applies are responsible for familiarizing themselves periodically with the latest version and for complying with policy requirements at all times.

TABLE OF CONTENTS

1. POLICY STATEMENT	5
2. VIRUS PROTECTION	6
3. PHYSICAL SECURITY OF COMPUTER EQUIPMENT.....	8
3.1. DEFINITIONS	8
3.2. REQUIRED PHYSICAL SECURITY	8
3.3. SECURITY FOR COMPUTER SUITE	10
4. ACCESS CONTROL.....	11
5. LAN SECURITY	13
6. SERVER SPECIFIC SECURITY	15
7. LINUX SPECIFIC SECURITY	ERROR! BOOKMARK NOT DEFINED.
8. WIDE AREA NETWORK SECURITY	16
9. TCP/IP & INTERNET SECURITY	16
10. VOICE SYSTEM SECURITY	ERROR! BOOKMARK NOT DEFINED.
11. GLOSSARY	18

I.T. Security Policy

1. POLICY STATEMENT

"It shall be the responsibility of the SHAKUMBHARI ENTERPRISES-IT 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, and wherever possible these access controls should meet with C2 class security functionality.
- 1.2. Internet and other external service access are restricted to authorised personnel only.
- 1.3. Access to data on all laptop/Client data 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 unauthorised software is prohibited. In the event of unauthorised software being discovered it will be removed from the workstation immediately.
- 1.6. Data may only be transferred for the purposes determined in the Organisation's data-protection policy.
- 1.7. All drives and removable media from external sources must be virus checked before they are used within the Organisation.
- 1.8. Passwords must consist of a mixture of at least 8 alphanumeric characters, and must be changed every 30 days and must be unique.

- 1.9. Workstation configurations may only be changed by I.T. Department staff.
- 1.10. The physical security of computer equipment will conform to recognised 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 servers. No data will be saved on individual PCs; management and support functions are excluded from this but taking the backup of their important data on the server dedicated shared drive will be the individual responsibility.
- 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. Each campaign will have a dedicated Trend Micro Antivirus server to keep all the PC of that LAN updated with latest antivirus system.
- 2.3. Workstations will be protected by virus scanning software. A scheduled virus scan will be pushed through antivirus server on daily basis.
- 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 Organisation is to be used until it has been scanned. No one on floor (apart from management and IT support staff) can bring any floppy disk, CD, hard disk or any other media drive to SHAKUMBHARI ENTERPRISES premises. In such an event when this is absolutely needed, a written prior approval from the General Manager -IT will be taken.
- 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 Organisation's machines.
- 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 Organisation 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 of all the server will be taken by the I.T. Department, the frequency and type of the data back will depend on the requirement as deemed fit.
- 2.13. Management strongly endorse the Organisation'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 Organisation'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 remove the PC from the network, 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 Data centre/computers will comply with the guidelines as detailed below.

3.1. DEFINITIONS

3.1.1. COMPUTER SUITE

Servers (all file servers/data base servers), Networking equipments, plus all inter-connected wiring, fixed disks, telecommunication equipment, ancillary, peripheral and terminal equipment linked into the server or EPAX, contained within a purpose built computer suite.

3.1.2. COMPUTER EQUIPMENT

All computer equipment contained within the **COMPUTER SUITE** which will include **PC's**, monitors, printers, disk drives, modems and associated and peripheral equipment.

3.1.3. PERSONAL COMPUTERS (PC's)

Individual computer units with their own internal processing and storage capabilities.

These guidelines apply to the location or room comprising the purpose built computer suite.

3.2. REQUIRED PHYSICAL SECURITY

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.

3.2.2. Locking of PC cases

PC's fitted with locking cases will be kept locked at all times.

3.2.3. Sitting of Computers

Wherever possible, **COMPUTER EQUIPMENT** should be kept at least 1.0 metres away from external windows in **HIGH RISK SITUATIONS**.

3.2.4. Opening Windows

All opening windows on external elevations in **HIGH RISK SITUATIONS** should be fitted with key operated locks.

3.2.5. 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 Rs. 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.

3.2.9. Location of Intruder Alarms

Detection devices should be located within the room or **AREA** and elsewhere in the premises to ensure that unauthorised access to the room or **AREA** is not possible without detection. This should include an assessment as to whether access is possible via external elevations, doors, windows and roof lights.

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.

3.2.14. Alarm Zoning

The ability to zone the intruder alarm from the main control panel should be provided to enable authorised usage of other areas of the building outside normal hours, whilst retaining alarm detection within the room or **AREA**.

3.2.17. Alarm Shunt Lock

The alarm should have the facility for setting and un-setting within the room or **AREA** independently of the status of the main premises control panel via a shunt lock on the room or **AREA** access door. It should not be possible to set the main system if the room or **AREA** detection is 'shunted out'.

3.2.18. Alarm Confirmation

Visual or audio alarm confirmation should be provided at the monitoring facility for all conventional detection within the room or **AREA**.

3.2.19 1.Superior Protection of Signal Transmission

Monitored signalling to the Alarm Receiving Centre should be either by direct line or use monitoring service.

3.2.20. External Windows to Have Locks

All opening windows within the perimeter of the room or **AREA** should be fitted with key-operated window locks.

3.3. SECURITY FOR COMPUTER SUITE

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

3.3.2. Partitions separating the room or AREA from adjoining rooms and corridors should be a minimum of 150mm solid non lightweight blockwork or brickwork devoid of glazing or other openings except for protected doors as defined below. Where glazing is essential for lighting or other purposes this should be protected by bars.

3.3.3. Secure doors giving access to the room or AREA, from within the building, should be solid timber at least 45mm thick and unglazed. The locking should be by 2 mortise deadlocks with registered keys, a micro switch being available for an alarm shunt lock.

Door fittings should comprise 3 hinges, supplemented by 2 hinge bolts if outward opening doors. Inward opening doors to room or AREA should have a London bar (a metal strip strengthening the locking post of the door frame).

3.3.4. The computer suite 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 suite to reduce the risk of flooding.

3.3.6. The floor within the computer suite should be a raised false floor to allow computer cables to run beneath the floor and reduce the risk of damage to computer equipment in the case 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 suite to help protect the computer systems in the case of a mains power failure.

3.3.9. Access to the computer suite is restricted to IT Department staff.

3.3.10. All contractors working within the computer suite are to be supervised at all

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 an alphanumeric password of at least 8 characters.
- 4.9. Passwords will expire every 30 days and must be unique.
- 4.10. Intruder detection will be implemented where possible. The user account will be locked after 3 incorrect attempts.
- 4.11. The I.T. Department will be notified of all employees leaving the Organisation's employment. The I.T. Department will then remove the employee's rights to all systems.
- 4.12. Network/server supervisor passwords and system supervisor passwords will be stored in a secure location in case of an emergency or disaster, for example a fire safe in the I.T. Department.
- 4.13. Auditing will be implemented on all systems to record login attempts/failures, successful logins and changes made to all systems.
- 4.14. I.T. Department staff will not login as root on to UNIX, Linux systems, but will use the su command to obtain root privileges.
- 4.15. Use of the Administrator username on Windows is to be kept to a minimum.

- 4.16. Default passwords on database systems such as Oracle will be changed after installation.
- 4.17. On Linux systems, rights to rlogin, ftp, telnet, ssh will be restricted to I.T. Department staff only.
- 4.18. Where possible users will not be given access to the Linux shell prompt.
- 4.19. 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.
- 4.20. File systems will have the maximum security implemented that is possible. Where possible users will only be given Read and File scan 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/server rooms. Hub/server 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 workstations 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 be 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 take 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 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 data & applications will be limited by the ACL (Access control list).
- 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 of a minimum of 8 characters.
- 6.15. Users will change their passwords every 30 days.
- 6.16. Unique passwords will be used.
- 6.17. The number of grace logins will be limited to 3.
- 6.18. The number of concurrent connections will be limited to 1.

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

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 Organisation'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 Organisations is by a secure VPN connection, using IPSEC or SSL.
- 7.11. All connections made to the Organisation's network by outside organisations 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.
- 8.6 All incoming e-mail will be scanned by the Organisation's e-mail content scanner hosted at service provider's premises.

9. Glossary

Access Control	The process of limiting access to the resources of a system only to authorised programs, processes, or other systems.
Audit Trail	A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.
Authenticate	To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.
Authorisation	The granting of access rights to a user, program, or process.
C2 Security	American security classification generally accepted world-wide, classifying the level of security provided.
CE	Products which meet the essential requirements of European Community directives for safety and protection carry this mark. Products which carry the CE mark may be sold anywhere in the community.
DISA	Direct inward system access. DISA is used to allow an inward-calling person access to an outbound line.
Discretionary Access Control	A means of restricting access to objects based upon the identity and need to know of the user, process, and/or groups to which they belong.
File Security	The means by which access to computer files is limited to authorised users only.
Firewall	A device and/or software that prevents unauthorised and improper transit of access and information from one network to another.
Ftp	File transfer protocol. Protocol that allows files to be transferred using TCP/IP.
Hub	Network device for repeating network packets of information around the network.
Identification	The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.
Internet	World wide information service, consisting of computers around the globe linked together by telephone cables.
LAN Analyzer	Device for monitoring and analysing network traffic. Typically used to monitor network traffic levels. Sophisticated analysers can decode network packets to see what information has been sent.
Laptop	Small portable computer.

Mandatory Control	Access	A means of restricting access to objects based upon the sensitivity of the information contained in the objects and the formal authorisation of subjects to access information of such sensitivity.
Modem		Device which allows a computer to send data down the telephone network.
Password		A protected, private character string used to authenticate an identity.
PBX		Private branch exchange - small telephone exchange used internally within an organisation.
Rlogin		Remote login. Protocol that allows a remote host to login to a UNIX host without using a password.
Shareware		Software for which there is no charge, but a registration fee is payable if the user decides to use the software. Often downloaded from the Internet or available from PC magazines. Normally not that very well written and often adversely effects other software.
Telnet		Protocol that allows a device to login in to a UNIX host using a terminal session.
UPS		Uninterruptible power supply. Device containing batteries that protects electrical equipment from surges in the mains power and acts as a temporary source of power in the event of a mains failure.
Username		A unique symbol or character string that is used by a system to identify a specific user.
Virus		Computer software that replicates itself and often corrupts computer programs and data.
Voice Mail		Facility which allows callers to leave voice messages for people who are not able to answer their phone. The voice messages can be played back at a later time.