BIHAR STATE POWER TRANSMISSION COMPANY LTD., PATNA
(Regd. Office – VidyutBhawan, Bailey Road, Patna)
(TIN VAT No – 1011257007, TIN CST No – 10011146136, CIN – U40102BR2012SGC018889)
Head Office, Vidyut Bhawan, Bailey Road, Patna -800021

Order

Sub: Adoption of IT/Cyber Security Policy in BSPTCL

As per article 1 of CEA cyber security guidelines 2021, all utilities must have Cyber security Policy. IT/Cyber security policy of BSPTCL has been prepared containing basic guidelines related to Desktop usage, LAN Security, Relocation/purchase/licensing of hardware & software & Cyber security.

The Board of Directors of Bihar State Power Transmission Company Limited in its 103rd Meeting held on 13.12.2022 vide its Resolution No. 103-12 accorded its approval for adoption of IT/Cyber Security in BSPTCL.

All officers of BSPTCL are hereby requested to ensure compliance from the date of issue of this order in letter and spirit.

By Orders
23.12.2022
(Anil Kumar)
GM(HR&Adm)

ENCL: As above

3013
23-12-2022

IT Security Policy

for

Bihar State Power Transmission Company Limited (BSPTCL)

Sl. No.	Version No	Author	Purpose/Change	Date
1.	V1	IT Team	Created	18.07.2022

Table of Contents

1. Introduction

1.1 Information Security

Information Security Policies are the cornerstone of information security effectiveness. The Security Policy is intended to define what is expected from an organization with respect to security of Information Systems. The overall objective is to control or guide Human behaviour in an attempt to reduce the risk to information assets by accidental or deliberate actions. Information security policies underpin the security and well being of information Resources. They are the foundation, the bottom line, of information security within an organization. We all practice elements of data security. At home, for example, we make sure that Deeds and insurance documents are kept safely so that they are available when we need them. All office information deserves to be treated in the same way. In an office, having the right information at the right time can make the difference between success and failure. Data Security will help the user to control and secure information from Inadvertent or malicious changes and deletions or unauthorized disclosure.

There are three aspects of data security:

a. **Confidentiality**: Protecting information from unauthorized disclosure like to the press, or through improper disposal techniques, or those who are not entitled to have the same.

b. **Integrity**: Protecting information from unauthorized modification, and ensuring that information, such as a beneficiary list, can be relied upon and is accurate and complete.

c. **Availability**: Ensuring information is available when it is required. Data can be held in many different areas, some of these are:
   - Network Servers
   - Personal Computers and Workstations
   - Laptop and Handheld PCs
   - Removable Storage Media (Floppy Disks, CD-ROMS, Zip Disks, Flash Drive etc.)
   - Data Backup Media (Tapes and Optical Disks)

2. Data Loss Prevention

Leading Causes of Data Loss:

- Natural Disasters
- Viruses
- Human Errors
- Software Malfunction

- Hardware & System Malfunction

Computers are more relied upon now than ever, or more to the point the data that is contained on them. In nearly every instant the system itself can be easily repaired or replaced, but the data once lost may not be retraceable. That's why of regular system backups and the implementation of some preventative measures are always stressed upon.

2.1 Natural Disasters

While the least likely cause of data loss, a natural disaster can have a devastating effect on the physical drive. In instances of severe housing damage, such as scored platters from fire, water emulsion due to flood, or broken or crushed platters, the drive may become unrecoverable.

The best way to prevent data loss from a natural disaster is an **offsite back up**. Since it is nearly impossible to predict the arrival of such an event, there should be more than one copy of the system back up kept, one onsite and one off.

The type of media back up will depend on system, software, and the required frequency needed to back up. Also be sure to check back ups to be certain that they have properly backed up.

2.2 Viruses

A virus is a form of malicious code and, as such it is potentially disruptive. It may also be transferred unknowingly from one computer to another. The term Virus includes all sorts of variations on a theme, including the nastier variants of macro- viruses, Trojans and Worms, but, for convenience, all such programs are classed simply as virus.
Viruses tend to fall into 3 groups: -

- Dangerous: - Such as .Resume. and .Love letter. which do real, sometimes Irrevocable, damage to a computer's system files, and the programs and data held on the computer's storage media, as well as attempting to steal and transmit user ID and password information.

- Childish**:** - Such as .Yeke., .Hitchcock., .Flip., and Diamond, which do not, generally, corrupt or destroy data, programs, or boot records, but restrict themselves to irritating activities such as displaying childish messages, playing sounds, flipping the screen upside down, or displaying animated graphics.

- Ineffective: - Those, such as .Bleah., which appear to do nothing at all except reproduce themselves, or attach themselves to files in the system, thereby clogging up the storage media with unnecessary clutter. Some of these viruses are ineffective because of badly written code, - they should do something, but the virus writer didn't get it quite right.

Within all types there are some which operate on the basis of a triggered event usually a date such as April 1st, or October 31st, or a time such 15:10 each day at the Tea Time virus activates.

Viral infection increases at rate of nearly 200-300 new Trojans, exploits and viruses every month. There are approximately 65135 "*wild*" or risk posing viruses (source SARC dated Sep 1, 2003). With those numbers growing every day, systems are at an ever-increasing risk to become infected with a virus.

There are several ways to protect against a viral threat:-

- Install a Firewall on system to prevent hackers access to users data.
- Install an anti-virus program on the system and use it regularly for scanning and remove the virus if the system has been infected. Many viruses will lie dormant or perform many minor alterations that can cumulatively disrupt system works. Be sure to check for updates for antivirus program on a regular basis. Back up and be sure to test backups from infection as well. There is no use to restore virus infected back up.
- Beware of any email containing an attachment. If it comes from anonymous sender or don't know from where it has come or what it is, then don't open it, just delete it & block the sender for future mail.

Protection of computer from virus infection

- Make regular backups of important data.
- Install antivirus software on computer and use it daily.
- Update the antivirus software with the latest signature files on weekly/fortnightly basis. Antivirus software does no good unless it is frequently updated to protect against the most recent viruses.
- Upgrade the antivirus software when new releases are provided.
- Never open or execute a file or e-mail attachment from an unidentified source. If user is unsure of the source, delete it.
- Recent viruses have been written so that they come from friends and colleagues. Be cautious with attachments even from trusted sources.
- If it was sent knowingly, an attachment could still contain a virus. Saving it as a file and running the virus scan software will catch any virus that it has been set up to find, therefore will catch most of them.

2.3 Human Errors

Even in today's era of highly trained, certified and computer literate staffing there is always room for the timelessness of accidents. There are few things that might be followed: -

- Be aware. It sounds simple enough to say, but not so easy to perform. When Transferring data be sure it is going to the destination. If asked "*Would you like to replace the existing file*" make sure, before clicking "yes".
- In case of uncertainty about a task, make sure there is a copy of the data to restore from.
- Take extra care when using any software that may manipulate drives data Storage, such as: partition mergers, format changes, or even disk checkers.
- Before upgrading to a new Operating System, take back up of most important files or directories in case there is a problem during the installation. Keep in Mind slaved data drive can also be formatted as well.
- Never shut the system down while programs are running. The open files will, more likely, become truncated and non-functional.

2.4 Software Malfunction

Software malfunction is a necessary evil when using a computer. Even the world's top Programs cannot anticipate every error that may occur on any given program. There are still few things that can lessen the risks:

- Be sure the software used will mean ONLY for its intended purpose. Misusing a program may cause it to malfunction.
- Using pirated copies of a program may cause the software to malfunction, resulting in a corruption of data files.
- Be sure that the proper amount of memory installed while running multiple programs simultaneously. If a program shuts down or hangs up, data might be lost or corrupt.
- Back up is a tedious task, but it is very useful if the software gets corrupted.

2.5 Hardware Malfunction

The most common cause of data loss, hardware malfunction or hard drive failure, is another necessary evil inherent to computing. There is usually no warning that hard drive will fail, but some steps can be taken to minimize the need for data recovery from a hard drive failure:

- Do not stack drives on top of each other-leave space for ventilation. An over Heated drive is likely to fail. Be sure to keep the computer away from heat Sources and make sure it is well ventilated.
- Use an UPS (Uninterruptible Power Supply) to lessen malfunction caused by Power surges.

- NEVER open the casing on a hard drive. Even the smallest grain of dust settling on the platters in the interior of the drive can cause it to fail.
- If system runs the scan disk on every reboot; it shows that system is carrying High risk for future data loss. Back it up while it is still running.
- If system makes any irregular noises such as clicking or ticking coming from the drive. Shut the system down and call Hardware Engineer for more information.

3. Desktop Usage Policy

3.1 Using Floppies/ CD/ Flash Drives

- Floppy should be used in consultation with system administrator/in charge computer centre and should be scanned before use.
- Unofficial Floppies, CDs or Flash Drives should not be used on office systems.
- Floppy should be write-protected if data is to be transferred from floppy to system.

3.2 Password

- Keep the system screen saver enabled with password protection.
- Don't share or disclose your password.
- User should not have easily detectable passwords for Network access, screen saver etc.
- A strong password must be as long as possible, include mixed-case letters, include digits and punctuation marks, not be based on any personal information, not be based on any dictionary word, in any language.
- Never use the same password twice.
- Change password at regular intervals.

3.3 Backup

- Backup should be maintained regularly on the space provided on central server of the department or on the storage media as per department policy.
- Keep paper copy of server configuration file.
- Keep the DATs or other removable media in a secure location away from the computer.
- Always backup the data before leaving the workstation.
- For sensitive and important data offsite backup should be used.

3.4 Physical Safety of System

- Protect the system from unauthorized use, loss or damage, e.g. the door should be locked when not in the office.
- Keep portable equipment secure.
- Position monitor and printers so that others cannot see sensitive data.
- Keep floppy disks and other media in a secure place.

- Seek advice on disposal of equipment.
- Report any loss of data or accessories to the System Administrator/in charge computer centre.
- Keep the system and sensitive data secure from outsiders.
- Get authorization before taking equipment off-site.
- Take care when moving equipment (Read instruction on moving equipment).
- Install UPS system with adequate battery backups to avoid any data loss or corruption due to power failure.
- System should be properly shut down before leaving the office.
- Log-off the system if you are leaving your seat.
- Never remove the cables when your PC is powered ON since this can cause an electrical short circuit.
- Do not stop scandisk if system prompts to run it at the time of system start-up.
- Always use mouse on mouse pad.
- Be gentle while handling keyboard and mouse.
- Do not open case of the hardware.
- Make sure that there is some slack in the cables attached to your system.

3.5 Computer Files

- All file level security depends upon the file system. Only the most secure file system should be chosen for the server. Then user permission for individual files, folders, drives should be set.
- Any default shares should be removed.
- Only required file and object shares should be enabled on the server.
- Never download or run attached files from unknown email ID.
- Always keep files in the computer in organized manner for easy accessibility. If required create new folders and sub-folders.
- Avoid creating junk files and folders.
- System files and libraries should not be accessed as it can cause malfunctioning of system.
- When transferring data, be sure it is going to the destination. If asked "*Would you like to replace the existing file*" make sure, before clicking "yes".

3.6 General Instructions

- In case of uncertainty about a task, make sure there is a copy of the data to restore from.
- Follow instructions or procedures that come from System administrator/In charge computer centre time to time.
- Users are not supposed to do his or her personal work on computers.
- Please intimate System administrator/In charge computer centre in case of system malfunction.

- User should always work on his/her allotted machines. In case of any urgency/emergency user may use other's machine with consultation of System Administrator/In charge computer centre.
- Antivirus software should be updated timely in consultation with System Administrator/In charge computer centre.
- Don't give others the opportunity to look over your shoulder if you are working on sensitive data/contents.
- Do not use unnecessary shareware.
- Do not install or copy software on system without permission of System administrator/In charge computer centre.
- Avoid unnecessary connectivity of Internet.
- Don't panic in case system hangs. Report it your IT Nodal Officer/System Administrator/In charge computer centre.
- If lock and key system is available then user should ensure the security of all the parts of the computer.
- Please ensure that preinstalled Antivirus is running on the system.
- Food and drinks should not be placed near systems. Cup of Tea/ Coffee or water glass should not be on CPU or Monitor or Key Board.
- Always power off the system when cleaning it.
- Never use wet cloth for wiping the screen.
- Never shut the system down while programs are running. The open files will, more likely, become truncated and non-functional.
- Never stack books/ files or other materials on the CPU.
- Place the cover on the computers when you close the computers at the end of the day.

3.7 Security Policy for Operating System

Computers can operate without application software, but cannot run without an Operating System.

"Operating Systems must be regularly monitored and all required 'housekeeping' routines adhered to."

The operating system of desktop systems within departments will generally run without substantial interference. However, for servers, mini-computers and mainframes, especially those running mature Operating Systems (OS), day to day housekeeping is usually required.

Information security issues to be considered, when implementing the policy include the following:

- Where an upgraded operating system fail to perform as expected, this can result in a loss of stability or even the total failure of some systems.

- Where housekeeping and routine support are informal or incident led, weaknesses in the security safeguards can go undetected and offer the potential for fraud or malicious damage.

3.8 System Software

(1) All system software options and parameters shall be reviewed and approved by the management.
(2) System software shall be comprehensively tested and its security functionality validated prior to implementation.
(3) All vendor supplied default user IDs shall be deleted or password changed before allowing users to access the computer system.
(4) Versions of system software installed on the computer system and communication devices shall be regularly updated.
(5) All changes proposed in the system software must be appropriately justified and approved by an authorised party.
(6) A log of all changes to system software shall be maintained, completely documented and tested to ensure the desired results.
(7) There shall be no standing "Write" access to the system libraries. All "Write" access shall be logged and reviewed by the System Administrator for dubious activities.
(8) System Programmers shall not be allowed to have access to the application system's data and programme files in the production environment.
(9) Procedures to control the use of sensitive system utilities and system programmes that could bypass intended security controls shall be in place and documented. All usage shall be logged and reviewed by the System Administrator and another person independent of System Administrator for dubious activities.

4. Network Organization

This section covers key definitions that are used in this policy and describes the departmental structure relating to PCs and LANs.
Personal Computer (PC) (also called Node): A small computer containing a motherboard with a Central Processing Unit (CPU), memory chips, associated supporting processors, and slots, sockets, or plugs for attaching peripheral equipment, such as a keyboard, video monitor, floppy disk, and hard disk. PCs may be used as stand-alone workstations as a client in a network, or as a terminal for a minicomputer or mainframe.
Network: A series of PCs connected in some type of topology (generally a star, ring or bus), using a special network operating system (NOS) that allows the PCs to share data and resources.

Local Area Network (LAN): A network that is set up for a department or limited geographic area. A peer-to-peer network shares resources with other PCs. A client/ server LAN can include midrange and legacy file servers and database servers.
Wide Area Network (WAN): A network that connects several networks in distant locations. The terms network, LAN, and WAN are synonymous with regard to applicability of the policies described herein.

Network Security
This section discusses the types of security and security policy regarding access control, passwords, and data security in a networked environment.

(A) Types of Security
The Office's network has four types of security:

- Log in/Password (initial access)
- Trustee (directory level access)
- Directory (directory level access)
- File attributes (file level)

Log in/Password

Security is activated when a user logs in to the network. The server requires both a recognizable user name and a password. Each user chooses his or her own password, which is encrypted by the system. If the user forgets the password the network administrator must assign a new one.

Trustee

- A trustee is a user who has been given rights to a directory and the files it contains.
- Trustee rights can be assigned to both individuals and groups. A trustee will not assign directory or file rights to a user who does not have a legitimate need to use that file or directory.
- Trustees will ensure that confidential office information to which they have access is not written to removable media and transported off Office premises unless authorized by the departmental supervisor or performed by authorized individuals as part of backup and emergency/recovery procedures. In addition, reports printed using the data should be distributed only to authorized users.

Directory

The directory security defines a user's rights in a given directory. These rights are:

- Supervisor (assigns the rights for the directory)
- Access control (trustee assignments)
- File scan (search)
- Modify filenames and attributes
- Create new files or subdirectories
- Erase existing files or subdirectories
- Read files
- Write files
- The owner will not assign rights to users who do not have a legitimate need or authority to view or use the information.

File Attributes

The owner of a file has the right to set the following attributes:

- Shareable read only
- Shareable read write
- Non-shareable read only
- Non-shareable read write
- Hidden file
- Delete inhibit
- Rename inhibit

Assignment of these rights is designed to prevent accidental changes or deletions to the files. The owner of a file containing confidential information will not assign access to a user that does not have a legitimate need or authority to use the file.

(B) Network Security Policy

The objective of the Office's network security policy is to provide adequate IT controls over the network. Security features available on the network will be implemented as needed to restrict users to the resources and rights, necessary to perform all the duties of their job descriptions adequately.

The network administrator, based on a written user setup form, from the departmental supervisor, showing password rights and normal work schedule, initially assigns rights. The rights may be expanded only with the written approval of the departmental supervisor.

- **Access Control**

The network administrator will implement available security access control features of the network. These features include the ability to restrict:

- Files that a user can access
- Time periods that a user can log on to the network
- Days of the week that a user can log on to the network
- Workstations that a user can access

Once implemented, network access should be restricted to normal working hours whenever possible. Departmental supervisors can grant exceptions based on need or shift considerations. Adequate supervision and review of work are required for users who have access beyond normal working hours. Generally users should be allowed access only from pre-specified workstations (nodes).

- **Passwords**

The network administrator sets up the user, and the user is required to enter a password on the first log on. Passwords will be set to expire every ninety days.

The system will be set to prompt the user for a password change automatically. Failure to make the change will cause the system to lock out the user. Also, repeated attempts to log on with an incorrect password will cause the intruder detection lockout to activate.

The network software should not display the password on the screen. Users should not let anyone see their password as they are keying it in.

User passwords should have a minimum of six digits, with a mix of alphabetic and numeric characters. Users will not use passwords that can be easily guessed, such as family names, birthdays, and commonly used default passwords, such as "test," "password," or "demo."

Users are not restricted by terminal, but are prohibited from logging on to more than one terminal at a time. Users are mainly subject to an inactive log off and automatic log off is not always available, users should manually log off when not using the terminal for that period of time or longer.

When a user leaves the Office, the personnel department will notify the network administrator, who will delete the user's password. Also, if a password is compromised, the user will change them password.

- **Data Security**

Data should be saved to the appropriate directory, normally either the group directory

or the departmental directory. In some cases, the supervisor authorizes the use of the user's local directory for storing certain types of data. Other members of the group access information on the group directory. Members of the department can access departmental directories. The user's local directory is on the PC and can be accessed only by the user.

User Responsibilities for Data Security
Users are responsible for backing up files on their individual PC hard drives, and departmental supervisors should verify that users are doing so on a regular basis. Users are also responsible for the security of their individual workstations, including security of PC backup disks.

Users are responsible for access security. Passwords should not be written down or seen by others when they are keyed in. Other related responsibilities include noting and reporting maintenance problems (such as disk error messages) before they can cause loss of data; ensuring that the PC data disks are not subjected to excessive heat, electrical fields, dirt, smoke, food particles, or spilled liquids; and ensuring that the PC has a surge protector.

(C) Monitoring the Network

Data Scope
A data scope is a device used to monitor network traffic. Its use, however, requires additional security controls to prevent abuse. Network Security Officer may have access of data scope to reduce any mishappening.

Performance Monitoring
Data integrity and security are enhanced when the system is running smoothly and is at peak performance. The network administrator should monitor performance of the system using available diagnostic tools. One of the duties of the network administrator is to troubleshoot any problems on the network and maintaining performance logs.

(D) Prevention and Detection of Viruses

- The scheduler for the network's antivirus software will be set to scan memory and all Files on the network on a daily basis. Warning messages will be carefully evaluated and corrective action taken.

- If a virus is discovered, the LAN security officer will investigate the origin of the virus. The policy for preventing viruses will be evaluated to determine the cause for the security failure. The security officer will recommend action to prevent future occurrences.

- The origin of most viruses is "pirated" software or shareware or public domain software downloaded from a bulletin board, on-line service, or the Internet. All software will be scanned for viruses before being loaded on a PC.

- The network administrator will purchase and install anti-virus software updates as they become available.

- If the origin of the virus is due to negligence or policy violation on the part of an employee, that employee will be subject to appropriate disciplinary action, which may include termination.

Network Software

This section defines policies regarding:

(A) Software licensing violations
(B) Authorized software
(C) Personal use of Office software
(D) Ownership of software
(E) Custom development of software
(F) Support of purchased software

(A) Software Licensing Violations

All software installed on Office PCs and on the network will comply with the software's licensing agreement. Software licensed for a server is limited to the number of users covered by the license. An original disk must exist for each software application installed on a user's PC. The only exception is software with a site license or public domain software on an authorized list.

In the case of authorized shareware products, if the Office uses the software beyond the trial period, the author will be paid the suggested contribution. So-called "pirated" software will not be installed on Office PCs.

(B) Authorized Software

Only software, authorized by the Office may be installed on a network or on an individual PC. Users will not install personal software on a PC without the approval of their supervisor.

No games or entertainment packages will be installed. The owner must show proof of ownership. An anti virus program will be run before installing any program on a PC. The Office will discourage the use of other than standard authorized software.

(C) Personal Use of Office Software

Users may NOT copy Office-owned software for their personal use, for distribution to others, or for use on another Office PC. Office software may be copied only for legitimate backup purposes.

(D) Ownership of Software
PC software developed by Office employees on Office-owned equipment and/ or during normal working hours, is owned by the Office.

(E) Support of Purchased Software
The officer in charge (usually the network administrator) of the department that recommend LAN-based commercial software is responsible for completing and returning the product registration forms. A copy of the receipt and product identification number (usually the serial number) should be recorded for reference when making support calls.

Officer in charge or IT matters or Nodal Officer (IT) of user departments as may be authorized by the HOD should note (from the box or software license information) the support period expiration and coordinate with users to ensure that calls are made before expiration of the service period.

For other than off-the-shelf LAN software, the Office will obtain a written agreement detailing terms of maintenance support. The contract will clearly define hardware maintenance services and costs.

Network Hardware
This section will discuss the Office's policy regarding the following:
(A) User responsibilities for hardware
(B) Hardware maintenance
(C) Integration with other systems
(D) Modems

(A) User Responsibilities for Hardware
Hardware refers to the physical components of the LAN-the PC workstations, Monitors, peripheral equipment, routers, modems, etc.

- Users are responsible for taking reasonable care of the system and reporting to a supervisor any maintenance problems, particularly disk errors or other problems that might cause loss of data.

- Users may not remove hardware from the Office or transfer equipment to other locations in the Office without supervisory approval.

- Users should avoid subjecting PCs to excessive vibration or bumps. Hard jolts while a PC is running can damage the hard disk drive. Smoke, heat, magnetic fields, and excessive dust can also damage LAN equipment. All PCs should have a surge protector.
- Users should use good judgment when eating or drinking in the vicinity of PCs and LAN equipment.
- The network administrator should locate the server in a secure area.

(B) Hardware Maintenance

The network administrator may, from time to time, get into annual maintenance agreements for selected equipment as deemed necessary. The network administrator will have emergency phone numbers and contract sources available it is necessary to replace or repair critical network components quickly.

(C) System Integration

Users can utilize PCs as terminals connected to a mainframe as well as workstations connected to a network. Data moves back and forth between the network and other systems, using the open standard protocol.

(D) Modems

The Office uses modems for communication with selected departments, clients, and employees. Modems will be turned off when not in use. The network administrator will activate applicable security features that are available. The senior management will approve modem controls.

The following modem controls should be implemented if permitted by hardware and software:

- Limitation of the activities that can be performed
- Auto call-back to identify dial-in users
- Passwords
- Unique operator identification
- Automatic log-off after a predetermined number of failed access attempts

5. Management of Computer Centre

a. Computer Centres shall maintain a temperature of less than 22 degree centigrade.

b. Apart from centralized AC, Window/split AC of appropriate tonnage shall be installed as backup.

c. Servers, networking equipment and any other important equipment at computer centre shall get power from online UPS.

d. The capacity of the UPS for the computer centre shall be decided by the respective IS Department.

e. Adequate safety measures shall be provided in consultation with S&EP Department.
f. Network audit, IT Security Audit (vulnerability test) and IT process audit shall be carried out once a year.
g. Physical / General Safety.

- Routers and switches etc. shall be housed in network racks.
- Location-in-charge shall be responsible for providing safety, security, proper upkeep and ambient environment for IT equipment placed at their location (e.g. A/C dust/ dirt free environment etc.)

6. Relocation of Hardware and Software

Whenever computers or computer peripherals are relocated (e.g. for maintenance, installation at different sites or storage), the following guidelines shall apply:

(i) All removable media will be removed from the computer system and kept at secure location.
(ii) Internal drives will be overwritten, reformatted or removed as the situation may be.
(iii) If applicable, ribbons will be removed from printers.
(iv) All paper will be removed from printers.

7. Purchase and Licensing of Hardware and Software

(1) Hardware and software products that contain or are to be used to enforce security, and intended for use or interface into any organisation system or network, must be verified to comply with these Information Technology Security Guidelines prior to the signing of any contract, purchase or lease.

(2) It is prohibited to knowingly install on any system whether test or production, any software which is not licensed for use on the specific systems or networks.
(3) No software will be installed and used on the system when appropriate licensing agreements do not exist, except during evaluation periods for which the user has documented permission to install and test the software under evaluation.
(4) Illegally acquired or unauthorized software must not be used on any computer, computer network or data communication equipment. In the event that any illegally acquired or unauthorized software is detected by the System Administrator or Network Administrator, the same must be removed immediately.

8. Servers Security and Usage Policy

- All the servers must be hardened. The default OEM settings like user name and passwords must be customized as per the requirements.
- Power on Passwords (BIOS Passwords) must be enabled.

- There should be Admin Bios password and user Bios password for all the servers and PG. The password must be written to the PASSWORD register. lt should be changed quarterly.
- All database servers must be kept in militarized zone and no direct/remote access from outside is allowed.
- All Web and application servers must be kept in de-militarized zone and no direct/remote access from outside is allowed.
- All default passwords in Web Server, Application Server, Database Server, must be changed or blocked lf not required.
- Only required software should be installed and other software including bundled software must be removed,
- Default web services must be removed from the web servers.
- No Remote access of servers shall be allowed for outside users; for exceptional conditions manual records for the same shall be maintained with proper approval.
- On Servers no pen drive/External drive shall be used. in exceptional condition before using external pen drive/external drive must be scanned at a sanitization PC containing antivirus other than that installed at DC/DRC and approval for the same from DVDR Security officer shall be taken and record for the same to be maintained.
- Health of Servers must be regularly monitored and record for the same is maintained. The Preventive maintenance of each server must be done once in a month and record of the same must be maintained.
- Full Back up of All Servers (including Database Servers, Application Servers, Configuration Files of each application end server of each servers) on monthly basis, must be taken on external media (like Tape Drive/ Cartridge etc.) and should be transferred to a safe location. Location must be in other building, approx. more than 2 Km apart from Data Centre building, media transfer manual record should be maintained with the handing over and taking over details.
- Shadow copy of each server on annual basis, must be taken on external media (like Tape Drive/ Cartridge etc.) and should be transferred to a safe location. Location must be in other building, approx. more than 2 Km apart from Data Centre building& media transfer. Manual record should be maintained with the handing over and taking over details.
- A password Register must be maintained which will contain all the passwords of the servers and applications like (Web Application and Database Applications and must be kept in a safe cupboard under lock and key. All the admin passwords must be changed once in a month and must be written on this register, the register should contain the signature of the person changing the password, IT Manager/DBA/DGM (IT).

- If any staffs are transferred, the concerned passwords must be changed.
- Firmware of the Servers should be updated with latest version as per advisory issued by the vendor from time to time. It should be at least of (n-1) version.
- All the servers must use genuine licensed operating systems , System Software's, database Software & application software, must be updated with latest compatible with running applications on that servers.
- Only used ports required by application needs to be opened and remaining ports on servers must be closed. Proper patch deployment and security provisions should be adhered for opened ports.
- Agencies responsible for maintenance of the servers , must sign non disclosure agreement with the owner of the servers for protecting and not disclosing the information outside the organization
- Servers' Operating system must be patched regularly with the latest patch release.
- Manual Technical Record for each server must be maintained in following format:

Server OEM Name	
Server Processor	
Server RAM	
Server Local Storage details	
Server Operating System Details	
Server Manufacturing year	
OEM Warranty Status	
Applications Hosted on the seryer	
Server Owner Details	
DC/DR Rack details where server is hosted	
Signature information Verified by Transmission (Owner) **Name:** **Designation:** **Department:**	**Signature information Verified by Agency** **Name:** **Designation:** **Department:**

4.22. Manual Record for each server access must be maintained in following format:

S.No.	**Date Start time and End time of activity**	**User name Designation Company Mobile No.**	**Purpose for Accessing Server**	**Details of Activity Performed**	**Details of Approval from Information Owner**	**Signature**

9. Antivirus Server Policy

- Antivirus server must be updated daily basis and all the servers must be scanned on daily basis.
- On all the servers if any eternal media is used then first external device must be scanned forcefully.
- Close monitoring of all the events reported by scanning of devices by Antivirus server.
- All the devices installed in server form area must have antivirus agent.

10. Active Directory Server Policy

- All the users (Application, Servers) created must use AD and authority of user must be controlled by AD.
- User Password change policy every month must be enforced.

- Password must be 8 character long having at least one Upper Case character one lower case character, One numeric and one special character. Password must not contain dictionary words user name.
- Change password must not be same of history of 10 passwords.
- Name of Admin user should not be Admin or Administrator. lt should be renamed as BSPTCL.

11. Computer Security Do's and Dont's

Do's:

- Create strong passwords that are at least eight characters long, and including at least a numerical value and a symbol, such as #, to foil password-cracking software. Avoid common words, and never disclose a password online.
- Always password-protect sensitive files on your computer, USB, smartphone, etc.

Losing items like phones, USB flash drives and laptops can happen to anyone. Protecting your devices with strong passwords means you make it incredibly difficult for someone to break in and steal data.

- Change your password every ninety days
- Perform regular backups of important data.

- Create a password for your files in order to protect file sharing activities.
- Physically secure your laptop
- Delete any message that refers to groups or organizations that you are not a part of.
- Download and install software only from online sources you trust.
- Never click on a link from an untrusted source.
- Close windows containing pop-up ads or unexpected warnings by clicking on the "X" button in the upper most right hand corner of that window, not by clicking within the window.
- Use antivirus software, and update it on a regular basis to recognize the latest threats. Heed ITR security alerts to download antidotes for newly circulating viruses and worms.
- Regularly update your operating system, Web browser, and other major software, using the manufacturers' update features, preferably using the auto update functionality.
- Set Windows or Mac updates to auto-download.
- Save attachments to disk before opening them. McAfee "Auto-Protect" will automatically scan your attachments if you save them to disk
- Locking your phone and computer keeps your data and contacts safe from prying eyes.
- Always report any suspicious activity to the IT team. Part of our job is to stop cyber attacks and to make sure our data isn't lost or stolen.
- All of our jobs depend on keeping our information safe. In case something goes wrong, the faster we know about it, the faster we can deal with it.

Don'ts:

- In particular the following activities are deemed unproductive by the Corporation and therefore NOT permitted: Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material & downloading the same.
- Using the computer to perpetrate any form of fraud, or software, film or music piracy
- Using the internet to send offensive or harassing material to other users.
- Downloading of music/video, playing music/video.
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such license.
- Hacking into unauthorized areas.
- Publishing defamatory and/or knowingly false material about the corporation, colleagues and/or our customers on social networking sites, blogs (online journals), wikis and any online publishing format

- Undertaking deliberate activities that waste employees effort or networked resources
- Introducing any form of malicious software into the corporate network.
- Any other action that is prohibited by law.
- Don't respond to emails or phone calls requesting confidential company information—including employee information, financial results or company secrets.
- It's easy for an unauthorized person to call us and pretend to be an employee or one of our business partners.
- Stay on guard to avoid falling for this scam, and report any suspicious activity to IT. And protect your personal information just as closely.
- When you access sensitive information from a non-secure computer, like one in an Internet café or a shared machine at home, you put the information you're viewing at risk.
- Make sure your computer is running the latest approved security patches, antivirus and firewall. And you should work in user mode, not administrator mode, whenever possible
- Don't leave printouts containing private information on your desk. Lock them in a drawer or shred them. It's very easy for a visitor to glance down at your desk and see sensitive documents.
- Keep your desk tidy and documents locked away. It makes the office look more organized, and reduces the risk of information leaks
- Don't let curiosity get the best of you.
- Always delete suspicious emails and links. Even opening or viewing these emails and links can compromise your computer and create unwanted problems without your knowledge.
- Remember, if something looks too good to be true, it probably is.
- Don't plug in personal devices like USB flash drives, MP3 players and smartphones without permission from IT.
- These devices can be compromised with code waiting to launch as soon as you plug them into a computer.
- Talk to IT about your devices and let us make the call
- Malicious applications often pose as legitimate programs, like games, tools or even antivirus software.
- They aim to fool you into infecting your computer or network.
- If you like an application and think it will be useful, contact IT to look into it for you before installing.
- No desktops/Laptops/Mobiles in any LAN shall be permitted to be connected to the Internet through attachment of any modem (Broadband / LL / Cable / PSTN), or Data card etc.