कार्यालय-प्रधान जिला एवं सत्र न्यायाधीश, अशोकनगर म.प्र.

पृष्ठां. प्रतिलिपि क्र. Comp/161 अशोकनगर, दिनांक 20.09.2023

प्रति,

समस्त न्यायिक अधिकारी,
जिला मुख्यालय अशोकनगर तथा तहसील न्यायालय चंदेरी/मुंगावली/ईसागढ़
एवं
प्रभारी अधिकारी,
समस्त अनुभाग केंद्रीकृत फाइलिंग काउंटर
जिला मुख्यालय अशोकनगर तथा तहसील न्यायालय चंदेरी/मुंगावली/ईसागढ़

की ओर माननीय उच्च न्यायालय के ज्ञापन क्रमांक Reg(IT)(SA)/2023/1214,Date 15.09.2023 की छायाप्रति इस निर्देश सहित प्रेषित है कि अपने अधीनस्थ समस्त कर्मचारियों को विभिन्न कम्प्यूटर उपकरणों के भौतिक सुरक्षा एवं डेटाबेस क्रियाकलाप की सुरक्षा संबंधी दिशा-निर्देशों का आवश्यक रूप से पालन किये जाने हेतु निर्देशित करें ।

संलग्नः- उक्तानुसार।

प्र. प्रधान जिला न्यायाधीश
जिला एवं सत्र न्यायालय, अशोकनगर

1003 Fwd: 15/09/23

HIGH COURT OF MADHYA PRADESH

PRINCIPAL SEAT – JABALPUR

No. Reg(IT)(SA)/2023/ 1214 Jabalpur, Dated:- 15/09/2023

::MEMO::

To,

The Principal District and Sessions Judge,
All the District and Sessions Courts in the State of M.P.
District - ____________

Sub: **Regarding to ensure proper physical security and database activities.**

Ref: **Reg(IT)(SA)/2018/1574, dated: 01.11.2018 and memo no. Reg(IT)/2011/718, dated: 26.11.2011.**

JSA
AO
19-9-23

As directed, under the subject cited and with reference to above, it is to inform it is again inform to take up the matter regarding to ensure proper physical security and database activities with reference to Reg(IT)(SA)/2018/1574, dated: 01.11.2018 and communication made in this regard.

The copy of aforementioned memos is hereby enclosed for kind perusal and further necessary action at your end.

15/09/2023
(F.H. QAZI)
SPSA(SA)

Encl: As Above

HIGH COURT OF MADHYA PRADESH

PRINCIPAL SEAT – JABALPUR

No. Reg(IT)(SA)/2018/ 1574 Jabalpur, Dated:-.01 NOV 2018

:: REMINDER::

To,

The District and Sessions Judge,
All the District and Sessions Courts in the State of M.P.

Sub: Regarding to ensure the proper physical security and data base backup activities.

Ref:- This Registry memo no. Reg(IT)/2011/718, dated: 26.11.2011.

As directed, under the subject cited and with reference to above, it is to inform that recently in the Tehsil Court of Sanavad of District Mandleshwar fire was erupted out and most of the Computer hardware articles installed at the Server Room of the Tehsil Court, Sanavad of District Mandleshwar has been destroy / burnt out.

In this regard, previously this Registry vide memo no. Reg(IT)/2011/718, dated: 26.11.2011 has made communication to all District and Sessions Judges in the State of Madhya Pradesh **to follow up the computer system security and backup policy. But,** it has been observed that till date nobody has implemented the policy in this regard.

Therefore, this reminder is issued in order to have proper physical security, system administration activities, database backup activities in order to ensure the proper computer system security.

01 NOV 2018

(F.H. QAZI)
REGISTRAR (IT)(SA)

Encl: As Above

HIGH COURT OF MADHYA PRADESH : JABALPUR

MEMORANDUM

No. Reg(IT)/2011/718 Jabalpur, Dated: 26/11/11

To,

The District & Session Judge,
District & Session Court,
All District in the State of Madhya Pradesh

Subject: Implementation Computer System Security and Backup policy.

Under the subject cited above, I am to inform that Hon'ble the Computerization Committee of the High Court in its meeting dated 08/03/2011 has resolved to recommend as under :-

"The Computer System Security and backup policy is to be adopted and to be implemented in phases in the High Court, Jabalpur and its Benches at Indore and Gwalior and subordinate Courts subject to availability of resources"

Hon'ble the Chief Justice vide order dated: 5/4/2011, pleased to approve the minutes and recommendation made by the Computerization Committee.

Therefore, it is request to follow up the Computer System Security and Backup policy as per the **enclosed document** and **Annexure**.

26.11.11

(SUBHASH KAKDE)
REGISTRAR GENERAL

Encl : As Above

1 ✓

Security and Data Backup Guidelines for stand-alone Computers and Computers connected to networks of High Court of M.P. and sub-ordinate Courts.

The Information Security Program for the High Court and its Sub-Ordinate Courts can be broken into specific stages as follows:

(a) Adoption of a security policy.
(b) Security risk analysis
(c) Development and implementation of an information classification system.
(d) Development and implementation of the security standards manual.
(e) Implementation of the management security self-assessment process.
(f) On-going security programme maintenance and enforcement
(g) Training.

A security policy defines the rules that regulate how the High Court of M.P. manages and protects its information's and computing resources to achieve security objective. One of the policy's primary purpose in detecting signs of intrusion is to document important information assets and the threats to those assets that the High Court of M.P., chooses to address.

Preparation of procedures includes the action necessary to observe systems and networks for signs of unexpected behavior, including intrusion. Observation can take the form of monitoring. inspecting and auditing. From these procedures, all concerned parties are able to determine the operational steps they need to take to comply with policy. These steps will thereby uphold the security of High Court of M.P. information and networked systems.

Security policies and procedures that are documented, well known, and visible enforced establish expected user behavior and serve to inform users of their obligations for protecting computing assets. Users include all those who access, administer, and manage computer systems and have authorized accounts in the systems. They play a vital role in detecting signs of intrusion.

I. Physical Security

1. Effective physical security procedures should be in place to deny access to unauthorized persons in the Server Room .
2. Adopt effective physical access control procedures for entering into the organization. Biometric physical access security systems should be installed to control and audit access to the operational site. Need-based access should be allowed to personnel to different parts of the operations area. Personnel authorized for limited physical access should not be allowed to gain unauthorized access to restricted area within the operational site.
3. UPS (Uninterrupted Power Supply) should be used to prevent corruption of data and software due to power supply

26.11.11

Reference: This document has been taken and modified from source : Computer Emergency Response Team (CERT-IN)

fluctuation. Proper grounding of the power supply & system should be ensured.

4. Where necessary, hardware/software security locks should be procured and installed on PCs as a protection against unauthorized access.
5. Physical protection technologies such as shielding could be use to protect against unauthorized monitoring, eavesdropping of electronic emations coming from computing equipment.
6. Security procedures should be adopted to prevent any installation of unauthorized hardware like a modem, removable media, boot device, etc. which could be used for either gaining access to the system of copying data from the system.

II. System Administration.

1. The root/administrator password should be known to only one designated responsible officer. Root/Administrator login should only be allowed from the console and not through the network.
2. While installing the Operating system, only the minimal set of services & applications required by the user should be installed/enabled. Some of the utilities/programs that are enabled by default like Guest user account, file sharing, default passwords, sample networking programs, etc. must be disabled.

   Preferable, the configuration principle of ***'deny first, then allow'*** should be practiced. That is, turn off as many services and applications and services as possible and then selectively turn on only those that are absolutely essential.
3. Password should be used and periodically changed (at least once in a fortnight) and should not be shared with anyone to prevent access to unauthorized persons. A **password should have at least 8 characters** and should be a combination of upper and lower case alphabets, numerals and special characters.
4. Audit Trail/System-event Log files give information regarding all activities performed on the system. These files should be enabled and checked regularly by the officer-in-charge to find out any unusual/doubtful activity.
5. The designated System Incharge should routinely check the relevant files to ensure no unauthorized account with 'super user' permissions exist.
6. Access rights to sensitive data should be restricted. Service like ftp and telnet on servers should be disabled.
7. Every individual user should have a separate account for which he/she should be individually responsible. A single account should not be shared / used by multiple users. Access permission for each account should be restricted according to the user's requirement.
8. Software Maintenance Tools should be kept in the custody of the System Incharge . Care should be taken that service engineers of external agencies are not able to copy any data from the system.
9. Maintenance or rectification of faults in the computer system should be carried out under proper and close supervision. In case of maintenance of hardware by an

26.11.11

external agency, a responsible officer should invariably be present throughout such maintenance. It should be ensured that no data file/program is copied and taken by the maintenance engineer. The users themselves should preferably do the maintenance of software.

10. Damaged hard disk should not be released even after it has been replaced by a new one. Such hard disks may be destroyed or zero-filled.
11. Downloading of software (*both source and binary*) from public sources (freeware/shareware) should generally not be allowed. If downloaded, it should not be executed on the online system before ascertaining that it is not a security threat. The user's authority to download and/or install software should be defined.
12. Use of pirated and unlicensed software or other software which are not allowed are strictly prohibited.
13. Firewall along with anti virus should necessarily be setup for restricting the unauthorized access.
14. All used draft memos, reports, carbons, unused printouts, etc. should be destroyed.

III. Anti-Virus

1. In order to protect the system/valuable data from viruses, virus infection checks should be incorporated in the boot-sequence of the system. Anti-virus software should be installed on all system in the M.P. High Court and subordinate Courts. Mechanism for regular upgrades for the anti-virus software to check for new viruses is formulated as per **"*Annexure-A.*"**
2. Program disks should not be loaned out as these may be returned with virus. If however, it becomes unavoidable, only a copy and not the original disk should be loaned.
3. Take enough precautions against computer viruses be not allowing any removable storage media (like floppies) for use without scanning for the viruses.
4. Computer games and other Trojan programs could be one of the main carriers of computer viruses and an unsuspecting easy medium for an intruder to break into the computer system. Playing computer games is prohibited.

IV. Backup

1. The Store Incharge/Computer Technicians should maintain a proper register for proper accounting of removable storage media already issued by it and which it will be issuing to computer users in future. The data backup is to be done in the format as per enclosed in "***Annexure –B***".
2. The Store Incharge / Computer Technician in the M.P. High Court should supply blank removable storage media like CD for computers users only against a written requisition duly signed/countersigned by the reporting officer.
3. The store section incharge should undertake a census of all removable storage media (like CD, DVD etc) issued by them. All removable storage media should be serially numbered and labeled with a sticker of the section /

26.11.11

department on the media so as to distinguish them from media brought from outside.

4. All removable storage media available for issue should also be serially numbered and labeled.
5. Before deleting a sensitive file from a storage media, some useless or junk information should be over-written on the file to prevent restoration of sensitive data by an unauthorized user.
6. Removable storage media should not be kept in table drawers, it should be kept in locks.
7. The safe custody of every used removable storage media should be the personal responsibility of the concerned user.
8. Damaged an unusable removable storage media (like CD – Compact Disk) should be broken and destroyed as applicable to the weeding out of paper based files and an entry to this effect made in the register.
9. Copying of information from the hard-disk/ CD should be done under the authorization of the reporting officer. It is preferable to use write-once-read-many media (such as CD-ROM) rather than media that can be re-written.
10. During transportation, removable storage media should be carried in appropriate mail-boxes to save these from damage.
11. As far as possible, removable storage media containing classified information should not be carried outside of the building. If at all it has to be taken outside the office building, its movement should be with the prior approval of the officer-in-charge. A record of the movement giving full details like date/time of it being taken out, Serial number, name of the officer taking it out, purpose, date and time of its return, etc. should be maintained.

V. Secret/Confidential

1. Top secret and secret information should not be stored on computers. Necessary information should be stored only on external media like PEN drive / External Hard Disk Drive with password protection and encryption.
2. Top Secret/Sensitive data should ideally be stored on external media in an encrypted form. These media along with the media containing encryption/decryption algorithm, if being used, should be kept at a highly secured place as applicable to Top Secret/Classified Paper based files of similar classification.
3. Top Secret information should not be permanently stored on the hard disk of a computer. If and when such top secret and sensitive information is processed on the computer, the information should be immediately to the password protected the processing is over, and should be copied on copied on a removable media.
4. Confidential information should be saved on the stand-alone system only. Such a system should be physically secured. The system should not be connected to any Wide Area Network (WAN) or Local Area Network (LAN) or to the Internet. This system should not have any terminal connected to it.

26.11.11

Reference: This document has been taken and modified from source : Computer Emergency Response Team (CERT-IN)

5. If classified data/programs are stored in the hard disk of the computer, the concerned person should ensure adequate safe guard against unauthorized access to the computer system.
6. Authenticity of the sender should be verified before exchanging classified information.
7. Internet mail should not be used for exchanging classified information.
8. Periodical verification of character & antecedents of computer personnel handling critical functions should be carried out.

VI Physical and Operational Security

Fire protection

(1) Combustible materials shall not be stored within hundred meters of the operational site.

(2) Automatic fire detection, fire suppression systems and audible alarms as prescribed by the Fire Brigade or any other agency of the Central or State Government shall be installed at the operational site.

(3) Fire extinguishers shall be installed at the operational site and their locations clearly marked with appropriate signs.

(4) Periodic testing, inspection and maintenance of the fire equipment and fire suppressions systems' shall be carried out.

(5) Procedures for the safe evacuation of personnel in an emergency shall be visibly pasted / displayed at prominent places at the operational site. Periodic training and fire drills shall be conducted.

(6) There shall be **no eating, drinking or smoking in the operational site**. The work areas shall be kept clean at all times.

Environmental Protection

(1) Water detectors shall be installed throughout the operational site and shall be connected to audible alarms.

(2) The temperature and humidity condition in the operational site shall be monitored and controlled periodically.

(3) Personnel at the operational site shall be trained to monitor and control the various equipment and devices installed at the operational site for the purpose of fire and environment protection.

(4) Periodic inspection, testing and maintenance of the equipment and systems shall be scheduled.

Physical Access

(1) Responsibilities round the clock, seven days a week, three hundred sixty five days a year for physical security of the systems used for operation and also actual physical layout at the site of operation shall be defined and assigned to named individuals.

26.11.11

(2) Biometric physical access security systems shall be installed to control and audit access to the operational site.

(3) Physical access to the operational site at all times shall be controlled and restricted to authorized personnel only. Personnel authorized for limited physical access shall not be allowed to gain unauthorized access to restricted area within operational site.

(4) Dual control over the inventory and issue of keys during normal office hours to the Data Centre shall be in place. An up-to-date list of personnel who possess the keys shall be regularly maintained and archived for a period of three years.

(5) All individuals, other than operations staff, shall sign in and sign out of the operational site and shall be accompanied by operations staff.

(6) Emergency exits shall be tested periodically to ensure that the access security systems are operational.

(7) All opening of the Data Centre should be monitored round the clock by surveillance video cameras system.

VII. Information Management

SYSTEM ADMINISTRATION

(1) The Registrar General, High Court of M.P., shall designate a properly trained "System Administrator" who will ensure that the protective security measures of the system are functional and who will maintain its security posture.

(2) The responsibility to create, classify, retrieve, modify, delete or archive information must rest only with the System Administrator.

(3) Any password used for the system administration and operation of trusted services must not be written won (in paper or electronic form) or shared with any one. A system for password management should be put in place to cover the eventualities such as forgotten password or changeover to another person in case of System Administrator leaving the Office. Every instance of usage of administrator's passwords must be documented.

(4) Periodic review of the access rights of all users must be performed.

(5) The System Administrator must promptly disable access to a user's account if the user is identified as having left the Data Centre, changed assignments, or is no longer requiring system access. Reactivation of the user's account must be authorized in writing by the System Administrator.

(7) The System Administrator must take steps to safeguards classified information as prescribed by its owner.

(8) The System Administrator must authorize privileged access to users only on a need-to-know and need-to-do basis and also only after the authorization is documented.

(8) Criteria for the review of audit trails/access logs, reporting of access violations and procedures to ensure timely management action/response shall be established and documented

26-11-'11

(9) All security violations must be recorded, investigated, and periodic status reports compiled for review by the management.

(10) The System Administrator together with the system support staff shall conduct a regular analysis of problems reported to and identify any weaknesses in protection of the information.

(11) The System Administrator should ensure that no generic user is enabled or active on the system.

Prevention of Computer Misuse

(1) Prevention, detection, and deterrence measures shall be implemented to safeguard the security of computers and computer information from misuse. The measures taken shall be properly documented and reviewed regularly.

(2) High Court of M.P., shall provide adequate information to all persons, including management, systems developers and programmers, end users, and third party users warning them against misuse of computers.

(3) Effective measures to deal expeditiously with breaches of security shall be established. Such measures shall include:

i. Prompt reporting of suspected breach :

ii. Proper investigation and assessment of the nature of suspected breach :

iii. Secure evidence and preserve integrity of such material as relates to the discovery of any breach ;

iv. Remedial measures.

(4) All incidents related to breaches shall be reported to the System Administrator for appropriate action to prevent future occurrence.

(5) Procedure shall be set-up to establish the nature of any alleged abuse and determine the subsequent action required to be taken to prevent its future occurrence. Such procedure shall include :

i. The role of the System Administrator / Hardware Technicians.

ii. Procedure for investigation ;

iii. Areas for security review ; and

iv. Subsequent follow-up action

Password Management

(1) Certain minimum quality standards for password shall be enforced. The quality level shall be increased progressively. The following control features shall be implemented for passwords:

(i) Minimum of eight characters without leading or trailing blanks;

(ii) Shall be different from the existing password and the two previous ones;

(iii) Shall be changed at least once every ninety days; for sensitive system, password shall be changed at least once every thirty days; and

(iv) Shall not be shared, displayed or printed.

26-11 17

Reference: This document has been taken and modified from source : Computer Emergency Response Team (CERT-IN)

(2) Password retries shall be limited to a maximum of three attempted logons after which the user ID shall then be revoked; for sensitive systems, the number of password retries should be limited to a maximum of two.

(3) Passwords which are easy-to-guess ***(e.g. user name, birth date, month, standard words etc.)*** should be avoided.

(4) Initial or reset passwords must be changed by the user upon first use.

(5) Passwords shall always be encrypted in storage to prevent unauthorized disclosure.

(6) All passwords used must be resistant to dictionary attacks and all known password cracking algorithms.

Privileged User's Management

(1) System privileges shall be granted to users only on a need-to-use basis.

(2) Login privileges for highly privileged accounts should be available only from Console and terminals situated within Console room.

(3) An audit trail of activities conducted by highly privileged users shall be maintained for two years and reviewed periodically at least every week by operator who is independent of System Administrator.

(4) Privileged user shall not be allowed to log in to the computer system from remote terminal. The usage of the computer system by the privilege user shall be allowed during a certain time period.

(5) Separate user IDs shall be allowed to the user for performing privileged and normal (non-privileged) activities.

(6) The use of user IDs for emergency use shall be recorded and approved. The passwords shall be reset after use.

User's Account Management

(1) Procedures for user account management shall be established to control access to application systems and data. The procedures shall include the following :

(i) Users shall be authorized by the computer system owner to access the computer services.

(ii) A written statement of access rights shall be given to all users.

(iii) All users shall be required to sign an undertaking to acknowledge that they understand the conditions of access.

(iv) Where access to computer services is administered by service providers, ensure that the service providers do not provide access until the authorization procedures have been completed. This includes the acknowledgement of receipt of the accounts by the users.

(v) A formal record of all registered users of the computer services shall be maintained.

(vi) Access rights of users who have been transferred, or left the Organization shall be removed immediately.

26-11-11

(vii) A periodic check shall be carried out for redundant user accounts and access rights that are no longer required.

(viii) Ensure that redundant user accounts are not re-issued to another user.

(2) User accounts shall be suspended under the following conditions:

(i) When an individual is on extended leave or inactive use of over thirty days. In case of protected computer system, the limit of thirty days may be reduced to fifteen days by the System Administrator.

(ii) Immediately upon the termination of the services of an individual.

(iii) Suspended or inactive accounts shall be deleted after a two months period. In case of protected computer systems, the limit of two months may be reduced to one month.

26.11.11

"ANNEXURE – A"

SECURITY OF THE COMPUTER SYSTEMS FROM VIRUSES

1.0 Introduction:

What is a Computer Virus ?

Computer viruses are data destructive programs written with the intent of copying and spreading the destruction to other computers and programs.

2.0 Computer virus types

Virus are classified depending on how they infect the computer systems on a network and they are of the following types.

2.1 Boot Viruses

They attack the boot record, the master boot record, the File Allocation Table (FAT), and the partition table of a computer hard drive. They generally propagate from an infected diskette placed in the disk drive of a computer while it starts or otherwise. Joshi and Michelangelo are examples of boot sector viruses.

2.2 File Viruses (Trojan Horse)

Trojan horse, also called RAT (remote access Trojan or remote access trapdoor) are examples of file virus. They attack program files (e.g. .exe; .com; .sys, .drv; .ovl; .scr etc.) by attaching themselves to executable files. The virus waits in memory for users to run another program and use the event to infect and replicate.

2.3 Macro virus

These virus attach programs that runs macros. Most common are in Microsoft word documents. These virus starts when a document or a template file in which it is embedded is opened by an application. Example : Melissa.

2.4 Stealth Viruses

These disguise their actions and can be passive or active. Passive viruses can increase the file size yet present the size of the original thus preventing detection, while active ones attack the anti virus software rendering them useless. Example : Tequila.

2.5 Multipartite Viruses

These have characteristics of both the boot and program viruses.
Example : Natas

2.6 Encrypted virus

These have built in encryption software code that mask the viral code making it difficult to identify and detect the virus.
Example : Cascade

26.11.11

Reference: This document has been taken and modified from source : Computer Emergency Response Team (CERT-IN)

2.7 Polymorphic Viruses

These are growing rapidly and have a inbuilt mechanism that changes the virus signature.
Example : SMEG

2.8 Worms

A worms is a independent program that reproduces by copying itself from one system to another usually over a network. They infiltrate legitimate programs and alter of destroy data. Unlike other virus worms cannot replicate itself.

2.9 Logic Bombs

Logic Bombs are programs that are triggered by a timing device such as a date or an event and are highly destructive.

3.0 Symptoms of a Infected Computer

The following are common symptoms of a computer infected with a virus:

1. *The computer fails to start*
2. *Programs will not launch or they fail when simple commands are performed*
3. *Names of files are changing or become unreadable*
4. *File contents change or are no longer accessible*
5. *Unusual words or graphics appear on the screen*
6. *Hard disks are formatted*
7. *Variations occur in computer performance, such as slowing down in loading or operation*

4.0 Need for eradication of Virus :

Some viruses are deliberately designed to damage files or otherwise interfere with computer's operation, while others don't do anything but try to spread themselves around. But even the ones that just spread themselves are harmful. Since they (generate a lot of traffic and slow down the network leading to the denial of critical services) damage files and may cause other problems in the process of spreading. This may cause loss to individuals/organizations which may be massive. Hence, the need for eradication of viruses.

5.0 Deployment of Antivirus :

1. For Laptop and Standalone Machine, Desktop Antivirus with latest Update should be installed.
2. In a networked environment, an antivirus server should be deployed and all the workstations should have the corresponding antivirus client. It is recommended that all these clients be configured from the central antivirus server for routine tasks such as updation of antivirus signatures, scheduled scanning of the client workstations. The management of the client workstations should be done centrally from the antivirus server in order to have a centralized monitoring of all the activities.
3. Identify all the possible entry points in the network through which a virus attach is possible and all the traffic entering the network through these points should be routed via an

26.11.11

antivirus gateway application for monitoring all the types of traffic flowing through the network, whether be it HTTP (HYPER TEXT TRANSFER PROTOCOL), FTP (FILE TRANSFER PROTOCOL), SMTP (SIMPLE MAIL TRANSFER PROTOCOL) or POP3 (POST OFFICE PROTOCOL). This ensures that the risk of any virus entering the network by any means is greatly reduced.

4. Application based Antivirus should be installed for applications like MS-Exchange, Lotus Notes etc.

6.0 Integration of Antivirus with Other Tools

1) Content Filtering:
Mobile Malicious Code like unsigned ActiveX, MIME, java applets are routes of possible virus infection. Content Filtering should be used for protocols like HTTP/SMTP/POP3/FTP. Antivirus Software is to be integrated with Content Filtering Software.

2) Firewall :
A firewall with Antivirus support will give additional security for the network.

7.0 **Best Practices** :

The suggested best practices for keeping computers free from a possible virus attack.

1. A good anti-virus product should be chosen for the Computers . A centralized server based antivirus system is suggested for an organization with a computer network.
2. The latest version of the antivirus with the latest signature is required to be loaded in all the machines of the machines of the organization. This is important as new and more potent viruses are discovered every day and even a few months old anti virus program may be ineffective against newer viruses.
3. For standalone PC's the antivirus software loaded into PC should be automatically enabled for checking viruses.
4. For a networked environment there must be a central server to check for viruses' in all the machines automatically.
5. The following schedule is suggested for a full scan of the PC's/
   a. Severs: Daily
   b. Workstations : Daily

   Schedule the operation when there is least human interaction with the work stations.
6. The antivirus software should auto-update virus signatures automatically from the service providers, as and when an update of signature or virus engine is available.
7. External media (CD's and DVD's) is one of the most potent medium for transmission of viruses', hence it must not be used in the network except for a few per determined PC's.
8. Anti-virus logs should be maintained for a period of 7-15 days or as determined by the policies of the organization. Ideally a weekly analysis of the logs should be done to obtain an infection profile of viruses and the machines infected.
9. Unneeded services should be turned off and removed. By default many operating systems install auxiliary services that are not

26.11.11

critical e.g. an FTP(File Transfer protocol), telnet or a web server. These services are avenues to attack. If these services are stopped, blended threats have less avenues of attack and the system administrator has a fewer services to maintain.

10. Enforce a password policy. Complex password makes it difficult to crack password files on compromised systems/computers. This helps to prevent damage when a computer is compromised.
11. The mail server is one of the easiest routes for virus attack through e-mail attachments. Mail server should be configured to block or remove email that contains attachments that are commonly used to spread viruses, such as ***.vbs, . bat, .exe, .pif, and .scr files.***
12. To prevent spamming to mails in the organization, mails only authenticated by users in organizations should be allowed.
13. Do not allow mails from servers that have an open relay, the data base of such servers can be accessed from various sties like mail-abuse . org.
14. All employees must be made aware of the potential threat of viruses and the various mechanisms through which they propagate.
15. Employees must be trained not to open attachments unless they are expecting them.
16. Do not allow user to execute software downloaded from internet unless certified safe by system administrator.
17. The latest patches for web browsers have to apply or else simply visiting a compromised web site can cause infection.
18. If a blended threat exploits one or more network services, disable, or block access to, those services until a patch is applied.
19. Always keep patch level up-to-date, especially on computer that host public services and are accessible through the firewall. Such as HTTP (HYPER TEXT TRANSFER PROTOCOL), FTP (FILE TRANSFER PROTOCOL),, mail and domain naming services
20. Since all online viruses arrive from the internet, a good antivirus software should be loaded at the logical gateway of the network.
21. In the case of a virus attack the following steps are required to be taken .
    - a. The network share of the machine has to be stopped
    - b. The contact person for cleaning the machine of virus has to be notified.
    - c. There must be a mechanism where an authorized expert/work station is notified automatically in case of a virus attack.

22. The notified expert should perform the following action on the infected work station.
    - a. Determine the type of virus
    - b. Isolate all infected systems and floppy disks
    - c. Try to clean the infected file
    - d. In case of failure above the file should be deleted from the work station.
    - e. In case of failure above the work station should be removed from the network and remedial action taken.
    - f. Remedial action may include reformatting depending on the severity of the problem and as per specific policy of the Organization.

26.11.11

Reference: This document has been taken and modified from source :
Computer Emergency Response Team (CERT-IN)

: Backup Schedule :

Backup Type	Periodicity	Days
Database backup	Daily	Every Day
Database backup (Application)	Daily	Every Day
Database backup (letters and general orders)	Fortnightly	
Cleaning up of unwanted files and directories	Fortnightly	As per requirement and condition
Server passwords of the server room	Fortnightly	activity (1st and 15th)

26.11.11

Server Data . '. Backup

Register -A

S.No	Server Name	Original Location	Size of Data	Date/Time of Backup	Media used for taking backup	Backup taken by	Signature

25.11.11

Page No.

Se: er Patch/ Software Installation Register - B

S.N	Server Name	Patch / Software nstalled	Location of Patch/software	Backup taken of patch Yes / No?	If Yes, then media used for taking backup	Signature

Page No.

26.11.10

Emergency Repair Disk -ERD

S.No	Server Name	Original Location	Size of Data On ERD	Date/Time of ERD	Media used for taking backup	ERD created by	Signature

Page No.

26.11.11

Server / Application Error / Problem Call Register

S.No	Server Name	Problem /Error Occurred	Date/Time of Problem	Steps taken to solve the problem	Problem solved on	Turn Around time taken to solve the problem	Signature

26.11.11