THE MAHARASHTRA STATE CO-OPERATIVE BANK LTD., MUMBAI.

INFORMATION TECHNOLOGY (IT) POLICY

DOCUMENT CLASSIFICATION: INTERNAL AND PROPRIETARY

Version: III Release: March 2015

INDEX

Sr. No.	Particulars	Page No.
1.	Information Technology System Security Policy Apex Document	3
2.	Operational Control Policy	10
3.	Backup and Restoration Policy	15
4.	Internet Access and Email Policy	19
5.	Logical Security Policy	24
6.	Network Security Policy	33
7.	Physical and Environmental Security Policy	42
8.	System Administration Policy	52
9.	Oracle Database Server Hardening	66
10.	Windows Server 2008 Hardening	70

INFORMATION TECHNOLOGY (IT) SYSTEM SECURITY POLICY – APEX DOCUMENT

DOCUMENT CLASSIFICATION: INTERNAL AND PROPRIETARY

1. BACKGROUND:

The Maharashtra State Cooperative Bank Ltd. (MSC Bank) is an Apex Co-operative Bank for the State of Maharashtra. The Bank has its registered Main Office at Mumbai. Presently, the branch network of the Bank is as follows:

Total number of units	:	Fourty Nine
Head Office	:	Mumbai
Regional Offices	:	Four (Viz. Pune, Nasik, Nagpur & Aurangabad)
Pay Offices	:	Two (viz. Nanded & Kolhapur)
Branches	:	Forty
Extension Counters	:	Three.
Divisional Offices	:	Eight

The Bank serves as a balancing centre for the surplus resources of co-operatives in the State. Besides, it provides normal banking services, which include latest ones like RTGS/ NEFT, DEMAT, SGL and various facilities for NRIs etc.

The Bank has implemented Core Banking Solution (CBS) 'OMNI' by Infrasoft Technologies in the year 2009. At present, all locations (HO, ROs, POs, and Branch Offices totaling 49) are connected to DC and DR with Primary (MPLS / Leased Lines) and Secondary (ISDN) lines for CBS

The Bank had formulated I.T. Policy in November 2011 which was approved by the Board of Directors on 21/11/2011.

However, a need to revise the existing IT Policy was felt because:

- The Bank has adopted various new IT Initiatives and the overall IT systems of the Bank have undergone various changes / updates.
- The existing IT Policy is having limited scope and is not sufficient to cover the risks / vulnerabilities associated with the changed environment.
- The Bank conducted its Information System Audit during 2013-14 and the recommendations of the ISA Report prompted revision in the existing IT Policy.

Accordingly a revised IT Policy has been framed and approved

2. OBJECTIVE OF INFORMATION TECHNOLOGY (IT) SYSTEM SECURITY POLICIES:

A. To provide direction and support for IT Systems security

B. To ensure that Bank's IT resources are appropriately protected from destruction, alteration or unauthorized access

C. To ensure that the confidentiality, integrity and availability of IT Systems of the Bank is maintained

D. To ensure that these protections are accomplished in a manner consistent with the business and work flow requirements of the Bank.

3. POLICY STATEMENT:

The Information Systems Security Policy document shall lay down various policies and control measures to

a) To protect Bank's information and Information Systems assets from destruction or disclosure, and
b) To ensure confidentiality, integrity and availability of Bank's information and Information System assets.

4. APPLICABILITY:

The IT Systems Security Policies shall be applicable to:

a) Computer hardware and peripherals used in the Bank
b) Operating, Database and application Software used in the Bank
c) Electronic data stored on standalone devices, networks, diskettes, databases, etc.
d) Network infrastructure devices
e) The Bank's Intranet and access to and data transmissions across the Internet.
f) All employees of the Bank
g) All vendors, consultants, agents or any such entity having access to Bank's I.T Systems, working in any premises or off the premises of the Bank.

5. ROLES AND RESPONSIBILITIES:

Based on the R.B. I. guidelines, the roles and responsibilities in respect of Information and Information security Systems of the Bank shall be as given in the following table.

Sr. No.	Role	Allotted to	Responsibilities
1	Information and Information systems owner	Bank's C.E.O / M.D./ Board of Directors	Approving / Reviewing the I.T. security controls Policy and Procedures.
2	Information and Information systems Custodian	Bank's I.T. officials at Head Office / R.O./Z.O	Implementing, maintaining and reviewing the I.T. Security controls for all I.T. systems in Bank as per Bank's policy.
3	Application Owners	Head of the Business department which uses the application system /s.	a) Ensuring and reviewing that the I.T. security controls are implemented and maintained as per Bank's policy in respect of application systems owned by them. b) Ensuring that logs or audit trails, as required, are enabled and monitored for the applications used by department/s under their control.

Sr. No.	Role	Allotted to	Responsibilities
4	I.S. Security Administrator / System Administrator	Bank's I.T. department official	a) Implementing I.T. security measures at branches / Head Office as per Bank's Policies and procedures document in respect of all Information Systems in the Bank. b) Ensuring and reviewing that the I.T. security controls are implemented and maintained as per Bank's policies / procedures.
5	User Manager	Bank's H.R. official	Ensuring and reviewing that the User management controls are implemented and maintained as per Bank's policy.
6	End User	All persons such as employees, auditors, Vendors, etc. who are authorized users of Bank's information systems resources as part of their job.	Complying with the I.T. security controls implemented / guidelines given as per Bank's policy.

6. DOCUMENTATION AND MAINTENANCE OF THE IT SYSTEMS SECURITY POLICIES:

This document shall be considered as the I.T. Security Apex Policy and policies documents for individual areas such as Physical / environmental security, Logical security, Network security, etc shall be prepared separately.

The IT System Security Committee members shall take decisions on the matters relating to the IT Security Policies. All such policies along with this Apex Policy document shall be termed as **Bank's IT Systems Security Policy.**

The IT Manager shall be entrusted with the responsibility of documenting and maintaining the IT Policy document.

6.1 Review of the IT Policies document:

The IT Policies /Procedures document shall be reviewed and updated annaually or as per the demands of the situations.

6.2 Approval of the IT Systems Security Policies document:

The Security Policies document as prepared / reviewed by the committee shall be presented to the board of directors for approval.

7. FREQUENCY OF INFORMATION SYSTEM AUDIT:

Information System shall be conducted every year in the following manner:

- Every alternate year – Quick Audit.
- Every alternate year of the Quick Audit – Regular Audit.

8. COMPLIANCE:

- Every employee of the Bank is responsible for complying with this policy.
- Managers are responsible for ensuring that their staff complies with this policy.
- Any employee who becomes aware of any violation or suspected violation of this policy must inform the Information Security Manager.
- Employees who violate the provisions of Security Policy and compromise IT Systems security shall be subject to disciplinary action up to and including termination of employment.

9. IMPLEMENTATION AND MONITORING OF IT SYSTEMS SECURITY POLICIES:

- For implementing various IT Security policies, procedures and guidelines also shall be formulated by the Committee.
- Monitoring of the implementation of Policies / procedures shall be done by way of internal / external IT audits. The IT Security Manager (Head Office) along with the branch managers and the I.T. team at branches shall be responsible for proper implementation of IT Security Policies.

10. COMMUNICATION OF THE IT SECURITY POLICIES TO ALL STAFF MEMBERS:

- The relevant provisions of IT Security Policy shall be communicated to all staff members.
- The staff members shall be given training regarding various measures implemented for security and their roles/ responsibilities in implementation.

OPERATIONAL CONTROLS POLICY

DOCUMENT CLASSIFICATION: INTERNAL AND PROPRIETARY

Version: 1.0

Document Control

1. OBJECTIVE

a. To ensure that the business processes / operations are standardized to avoid any kind of intentional or unintentional errors or omissions.
b. To impart guidelines for implementing adequate controls to establish such standardization of business processes / operations.

2. SCOPE:

All the business processes of the Bank.

- Banking Operations

3. POLICY STATEMENT:

The Bank shall have standardized procedures for handling IT Operations to maintain accuracy and uniformity.

POLICY DETAILS:

3.1	REVIEWING REPORTS
A	**AUDIT TRAILS:** **1.** All business and system applications used in the Bank shall generate Audit Trails of the critical processes. **2.** The frequency and authority of review of these Audit Trails shall be set based on the criticality of the operation and shall be communicated to all the users. **3.** The procedure for handling the discrepancies found in these Audit Trails shall be set. **4.** These Audit Trails shall be reviewed as per the set frequency, by the competent authority. **5.** Users shall be trained to understand and identify the discrepancies. **6.** There shall be a laid down procedure and hierarchy to report the discrepancies, if found any. **7.** Branches shall generate the following Audit Trails on daily basis • Customer Masters Updates Log **8.** Branch Managers shall review these Audit Trails on daily basis. **9.** Data Centre shall generate following Audit Trails. **8.1. Related to business applications (Separately for all the applications)** a) User Log Updates Log Parameters Updates Log (On weekly basis) b) Parameter Settings / Updates Log (On weekly basis) c) Products / scheme details Updates Log (On weekly basis) **8.2. Related to System Software: (Separately for all the software)**

	a) Database : • User Profile Log (On fortnightly basis) • Log of activities done directly into the database (On fortnightly basis) **b) Operating System:** • User Profile Log (On monthly basis) **10.** These logs shall be reviewed by the DC Head jointly with process owners wherever needed.
2	**EXCEPTION REPORTS:** a) Exceptions in various processes shall be identified and set in respective applications. b) All applications used in the Bank shall generate a report of activities overriding the set exceptions. c) Branches shall generate Exceptions Reports on daily basis from all the applications used in the branch. d) These reports shall be reviewed by the Branch Manager. e) Data Centre shall generate Exceptions Reports related to the processes handled there, on daily basis for various applications used in the Bank. f) These reports shall be reviewed by the DC Head jointly with process owners wherever needed. g) Users shall be trained about assessing the criticality of the exceptions. h) There shall be a laid down procedure and hierarchy to handle the different types of exceptions based on the criticality

3.3	SCHEDULING OF ACTIVITIES
	a) The critical activities shall be identified b) The time bound activities among these for e.g. handover from the branches, day end, day begin activities etc, shall be appropriately scheduled. c) The sequence to carry out these activities shall also be scheduled. d) Such scheduling shall be communicated with the respective process owners. e) Users shall be trained to adhere to the given schedules. f) There shall be a frequent reviewing / internal audits in the Bank to ensure that the laid down schedules are followed.

MSC BANK LTD., MUMBAI

BACKUP & RESTORATION POLICY

DOCUMENT CLASSIFICATION: INTERNAL AND PROPRIETARY

Version: 1.0

Document Control

1. OBJECTIVE

a. To ensure that the complete and accurate data of the Bank is available at all times for restoration in case of any loss or corruption of Bank's database..
b. To impart guidelines for taking Backups for safegaurding Bank's critical data / information.

2. SCOPE:

The policy covers backup and restoration.

POLICY

.

3	Backup and Restoration Policy
A	***Bank recognizes that the taking database backups of servers are critical to the viability and operations of the Bank. It is essential that certain basic standard practices be followed to ensure that data files are backed up on a regular basis.*** **Procedures** I. Bank has 11 backup tapes for the storage of backup II. Bank uses HP Data Protector backup software to support backup processes III. The team schedules full tape backups during non-production hours. IV. Backup is being stored daily on different tapes. For each day of week, one separate backup tape is assigned. After 6 days, first tape is being recycled on 1st day of week for backing up database. On 2nd day, second tape and cycle goes on every day. V. Milestone backup is being stored on some special situations like half-year end and year-end. VI. Any type of incidents / problems faced during any of the above action shall be immediately reported.
B	***The IT department is required to perform periodic test restores of the system to ensure proper functioning. The maximum interval between test restores is monthly.*** **Procedures** I. Restoration of selected backup shall be tested on Test server. II. Monthly once randomly selected backup shall be restored and tested

	ensuring the correctness and completeness of the backup. III. Before making any major changes in any system, the milestone backup shall be taken and the same shall be restored for checking the Correctness and completeness. IV. Any type of incidents / problems faced during any of the above action shall be immediately reported.
C	***A record of the all types of backup, Restoration/testing of backup and physical movements of all backup copies shall be maintained.*** **Procedures** I. All detail records with success and failure status of database backup taken, restored/tested shall be maintained II. All backup media should be labeled with pre-decided nomenclature. III. Logbook/Register shall be checked weekly by authorized personnel of Bank.
D	***Backup copies must be stored in an environmentally protected and access controlled secure offsite location.*** **Procedures** I. These media should be handled with proper care, in secure manner through reliable sources only. II. Any type of incidents / problems faced during any of the above action shall be immediately reported.

MSC BANK LTD., MUMBAI

INTERNET ACCESS AND EMAIL POLICY AND PROCEDURES DOCUMENT.

DOCUMENT CLASSIFICATION: INTERNAL AND PROPRIETARY

Version: 2.0 Dated 5th Jan 2015

1. OBJECTIVE:

a) To protect the Bank from potential threats/ vulnerabilities arising out of internet connectivity.
b) To ensure the use of MSCB's internet and email system in a secured, responsible, effective and lawful manner.

2. SCOPE AND APPLICABILITY:

a) IT assets of the MSCB which get exposed to threats and vulnerabilities of Internet Usage
b) Employees having access to the Bank's Internet resources and Bank's email system

3. POLICY STATEMENT:

The Bank shall ensure a secure connectivity to Internet and shall restrict the usage of Internet and email facility to authorized persons only, to safeguard the Bank's internal network from any threats / vulnerability arising out of internet connectivity

3.1	SECURE INTERNET CONNECTIVITY
3.1.1	***Availability of standard source of internet connectivity shall be ensured by the Bank.*** **Procedures** A. Approved standard source of Internet connectivity such as broad band, data cards etc. should be provided by the Bank to the authorized users. B. Users should not be allowed to use any other source, than the one provided by MSC Bank, to connect to the Internet. C. Bypassing Bank's network security by accessing the Internet directly by modem or other means such as PSTN, CDMA, GPRS, EDGE, and GSM etc. should be strictly prohibited.

3.1.2	***Adequate controls should be implemented to ensure physical and logical security to the internet connections of the Bank.*** **Procedures** A. The hardware such as modems, data cards etc.should be protected from physical treats of theft, loss and fire. B. Internet connectivity provided via removable media, shall be protected from loss and unauthorized usage. C. The roles / designations which need usage of Internet connectivity should be identified. Access to internet should be given strictly on "need to do" basis. **D.** Internet connectivity should be password protected.

3.2	**PROTECTION AGAINST POTENTIAL VULNERABILITIES**
	Adequate controls shall be implemented to safeguard the IT systems of MSCB from potential vulnerabilities arising out of internet connectivity such as Virus attack, Unauthorized access / hacking of bank's IT Systems, Violation of copyrights or any other unlawful usage **Procedures:-**
3.2.1	**FIREWALL:** a) A firewall of an adequate capacity should be installed by the Bank to route the internet traffic. b) Undesirable and unwanted websites should be blocked by using the web filtering feature of the firewall. c) The data traffic should be monitored in certain intervals for ensuring that the guidelines about the size and contents of internet browsing are followed.

3.2.2	**ANTIVIRUS / ANTI MALWARE / ANTI SPYWARE:** a) The Bank should have a licensed antivirus application suitable and adequate for the Bank's setup. b) The Antivirus application should be updated on daily basis by the IT team c) All the servers, desktops and laptops should be covered by such antivirus application. d) Suitable anti-malwares, anti-spywares should be installed and updated in the Bank's network. e) USB drives of maximum possible locations should be disabled.
3.2.3	**AWARENESS TRAINING TO THE USERS** **A.** Users should be made aware about various threats and vulnerabilities of getting Bank's confidential data exposed to internet. **B.** Users should be trained to take adequate cautions and controls while using the internet in the Bank **C.** Users should be instructed to use the internet strictly for official use only. **D.** Users should not be allowed to download any software from internet such as screensavers, device drivers, shareware, software patches, add-ons and updates, etc. **E.** The users should be made aware that, while downloading any software from internet, they may inadvertently download a virus and/or malicious code from the internet which may have an adverse effect on availability of resources. Also if anyone uploads, downloads or transmits commercial software or copyrighted material in violation of its copyright, the Bank and the employee may face legal charges. **F.** Users should be prohibited from disclosing / sharing any critical business data / information with any unauthorized person. **G.** Users should be instructed that the Bank's internet facilities should not be used for speculation, gambling, buy/sell shares, buy/sell articles or illegal activities.

3.3	EMAIL SECURITY AND CONTROLS
3.3.1	*Adequate controls shall be implemented to ensure effective and lawful usage of the Bank's email system.* **Procedures:** A. The Bank should have their own registered email domain name. B. Email accounts should be created of those employees who need to communicate with external entities only after written approval from General Manager of the respective department. C. Users should be restricted from using their personal email IDs other than the official IDs in any official correspondence. D. Users should be instructed :- • To have a personalized signature which should include the sender's name, job title, company name and contact number. • Not to use Internet abbreviations and characters such as smileys should be avoided while writing an email. • Not to attempt to disguise his / her identity when sending mail. • That Emails should not be sent using another person's email account E. The Bank should have the right to monitor the emails sent and receive by any user for legitimate business reasons, including checking the compliance with the E-mail policy and Industry regulations, employee performance and reasonable suspicion activities harmful to the company, at any point in time and whenever deemed necessary. F. Unrestricted usage of the facility will result in network congestion and loss of productivity. Therefore, I. Excessively large email messages or attachments should not be sent. II. Chain or pyramid messages or similar schemes should be avoided.

MSC BANK LTD., MUMBAI

LOGICAL SECURITY POLICY AND PROCEDURE DOCUMENT

DOCUMENT CLASSIFICATION: INTERNAL AND PROPRIETARY

1. OBJECTIVE

a. To ensure that only authorized persons get logical access to Bank's IT assets and any unauthorized user access is prevented.
b. To impart guidelines for taking appropriate controls for ensuring such authorized user access.

2. SCOPE:

All software applications implemented by the Bank

Operating Systems

Database Systems

Anti-virus Application

Various Business Application systems

3. POLICY STATEMENT:

Adequate logical access controls shall be implemented by the Bank to ensure that -

- Only authorized users can access Bank's information and Information Systems assets
- The integrity of Bank's data and system configurations is safeguarded from unauthorized access

POLICYDETAILS:

3.1	SECURE LOG ON PROCEDURES FOR ALL APPLICATION
	There shall be a secure logon procedure for all applications implemented in the Bank. **Procedures** A. There shall be password protected Login IDs for handling / accessing all software applications available in the Bank. B. Users should have individual Login IDs. Separate Login IDs should be created for outside support persons such as vendors. C. The Login IDs created should be unique in nature. D. The access levels allotted to Login IDs should be on 'Need to do' and 'Need to know' basis.

3.2	USER PROFILE MANAGEMENT / MAINTENANCE

There shall be a uniform process for managing and recording User Profiles for all software applications implemented in the Bank.

Procedures

A. **User Access allocation:** The access to bank's IT systems shall be given to the authorized users on '**need to know and need to do'** basis.

B. **User Profile Creation:**

a. The process owner / in-charge should initiate the request for creation of Login ID for new user for a particular application.

b. The requested Login ID should be created at the Data Centre based on the received request.

c. The Login ID should be communicated to the respective user is a secure manner.

d. An acknowledgement should be obtained from the user for accepting the Login ID.

e. The User should change the allotted password during the first logon.

C. **User Profile modification:**

a. The process owner / in-charge should request the Data Centre for any kind of modifications required in Login ID of any user. (changes in the user level, changes in working location etc.)

b. Such request should be signed by the respective User

c. The requested changes should be done at the Data Centre based on the received request.

d. The changes should be communicated to the respective user and the initiator of the request.

D. **Enabling / Disabling of Users:**

a. Users on long leave (more than 3 days) should be temporarily disabled.

b. The process owner / in-charges should communicate the Login ID of such user to the Data Centre

c. Such Login Ids should e temporarily disabled at the Data Centre.

d. Once the user is resumed back to his / her duties, again the request for enabling his / her Login ID should be sent to the Data Centre and should be executed based on the request.

E. **Deactivation of User IDs:** Login IDs of the retired, resigned or terminated employees should be deactivated on their last working day.

F. **Maintaining record of User Profiles**: A detail record of user profile creation, deletion or modification should be maintained along with users' acknowledgement.

G. **Use of privileged User IDs:** The allocation and use of privileged User IDs shall be restricted and controlled. After successful installation of systems, the default system passwords shall be changed and stored securely.

	H. **Review of User profiles and access rights:** • Logs of User Profiles and access rights of business applications should be generated and reviewed on weekly basis by the unit managers. • **Database application or operating systems user profiles should be reviewed once in a month by the IT Manager**

3.3	**PASSWORD MANAGEMENT**
	The software applications implemented in the Bank shall have password protected accesses and shall enforce strict password controls, **Procedures** **A. Password Protected Systems:** Allsystems implemented by Bank should be password protected. **B. Password Controls:** Maximum possible password controls should be built in the systems. At least following controls should be available in the systems. a) The system should enforce the user to change of fist time allotted / default password. b) The password should consist of minimum 8 characters

	c) The password should be alpha-numeric and having at least one special character such as @,#,* etc. d) The system should maintain password history and shall not allow last (2) password to be repeated. e) The password file should be encrypted one way. f) The system should enforce password change by user after periodic interval. g) Every system should provide for 'password change' facility to every user as and when required by him / her. h) The system should not accept password which is same as the User ID of the user i) The system should not accept blank passwords **C. Passwords maintenance:** a) In case, any user reports password lost / forgotten, a written application should be obtained from him / her before resetting it in the system. b) The system should enforce the user to change the allotted password during the first login after resetting the password.
3.4	**GENERAL CONTROLS (COMMON FOR ALL THE SYSTEMS)**
	Controls shall be implemented to ensure that the software applications implemented in the Bank, are adequately secured against the basic threats. **Procedures** **A. Idle Session time-out:** Inactive sessions should be shut down or locked after a

180 seconds period of inactivity.

B. Limitation on concurrent logins: The systems should be configured not to allow more than one login at the same time by a user. In cases where, for any reason, concurrent logins are required, such cases should be approved and documented by I.T. Security Committee.

C. Logs maintenance and scrutiny: For detecting unauthorized activities or system faults / failures, monitoring of logs at all systems levels should be done.

Audit logs recording user activities , exceptions etc. should be available in the system and shall be preserved for prescribed periods

In addition to the general controls, following controls specific to operating system of Servers used in the Bank should be implemented.

D. Synchronization of system clocks: Synchronization of Server clock and the client's clock and the application system clock should be ensured once in a fortnight.

E. Installation of Latest hot fixes and Service packs: Latest hot fixes and service packs shall be installed on the Servers / other computers. These patches should be tested in test environment before rolling out to the live environment.

F. Blocking of unnecessary ports and services: Unnecessary services and ports should be blocked.

a) Documentation / Backup of Operating Systems: Documentation / backup of Operating system settings should be maintained.

3.5	SECURITY AWARENESS AND RESPONSIBILITIES AMONG USERS
	Users of the Bank shall be adequately aware of the possible threats associated with the unauthorized access and controls to be implemented to address such risks. **Procedures** Users should be trained of their responsibilities for maintaining effective access controls, particularly good security practices in selection and use of passwords

MSC BANK LTD., MUMBAI

NETWORK SECURITY POLICY

DOCUMENT CLASSIFICATION: INTERNAL AND PROPRIETARY

Version - 1.0.0

1. OBJECTIVE

Protecting the network infrastructure against threats originating from external and internal networks is of prime importance to Maharashtra State Co-Operative Bank Limited (MSC BANK). Absence of proper access control protection can lead to attacks that include unauthorized access from the Internet; spread of virus, worms, malware etc. Traffic can be sniffed in transit on the network that can lead to unauthorized access to critical and sensitive information.

The purpose of this policy is to ensure authorized and secure access to MSC BANK network internally and from external networks, provide adequate redundancy for critical IT assets and establish effective management of the network infrastructure.

2. SCOPE AND APPLICABILITY

This policy and the associated guidelines apply to the employees of the MSC BANK and all personnel using the information technology resources of the MSC BANK. This includes contractors, consultants, third-party associates and any temporary employees who access MSC BANK computer networks that include LAN, WAN, Dial-up Access and data communication equipment and facilities.

3. POLICY

The MSC BANK network infrastructure should be adequately designed, managed and controlled in order to ensure the protection of the information in the network and of the supporting infrastructure.

3.1 Network Operations Department

3.1.1 A network operations department should be setup for managing MSC BANK network.

- The network engineer should report to the IT Manager on the network availability and performance.

- The network operations department should communicate any incidents in the network to the IT Manager. Any incidents which are reported should follow the Incident Management process.

3.2 Documentation

3.2.1 The network manager will be primarily responsible for maintaining an updated network diagram describing the network layout. The diagram should be updated to reflect any change in the network architecture.

3.2.2 Detailed inventory of all the network assets should be maintained by the network teams and updated to reflect any changes in the network.

3.2.3 Network team should maintain standard operating procedures for carrying out the day to day activities.

- Detailed documentation for the following should be maintained:
  - Network connectivity including switches/routers/link speeds
  - Firewalls and their associated segments
  - Application Server Details
  - IP addressing schema details
  - Access List/ Firewall Rulebase details
  - Approved software list which are authorized for usage at MSC BANK
  - VPN user list if any

3.3 Network Architecture

3.3.1.	The internal network of MSC BANK should be separated from external network using a firewall. The firewall should be configured so as to prevent any unauthorized inbound access to MSC BANK network.
3.3.2.	Intrusion prevention/detection system (IDS/IPS) should be deployed in the network for monitoring external intrusions.
3.3.3.	Internet access for all users should be controlled by a central gateway and should be routed via a proxy server.
3.3.4.	The firewall should segregate the MSC BANK network into security domains such as external, DMZ, internal etc.
3.3.5.	The default access between security domains must be none (i.e. Deny All). ▪ All communications between security domains must be authorized and controlled based on a least privilege/capability basis, as required by the assigned function of the device or application
3.3.6.	Only network administration team should have administrative access (physical and logical) to network devices. The access should adhere to the principle of least privileges and should be approved by IT Manager.
3.3.7.	All network and security devices should be accessed over a secure channel and from IP addresses approved by the IT Manager.
3.3.8.	Default Passwords of all network devices must be changed and configured as per Password Policy
3.3.9.	All network and security devices must have their internal clocks set accurately and synchronized to a MSC BANK approved time source.

3.4	**WAN Access**
3.4.1.	Access control list (ACL) should be implemented on all perimeter devices that connect to the external networks.
3.4.2.	ACLs on the perimeter devices should block access to all ports except for the ports approved by InfoSec Team. Ports that are known to be vulnerable to virus/worms or any attacks should be blocked.
3.4.3.	Network administration team is responsible for blocking of ports. Network administration team should use MPLS for WAN links which has got its own security features.
3.5	**Segregating Server and User Segments**
3.5.1	Critical multi-user application servers should be separated from the user segments by a firewall.
3.5.2	The firewall should restrict user access from any network to only essential ports on the respective servers.
3.6	**Demilitarized Zone (DMZ)**
3.6.1	All Internet facing servers such as web server, email gateway, antivirus gateway should be segregated from the internal server segment through a firewall.
3.7	**Redundancy**
3.7.1	The network redundancy requirements should be assessed and adequate redundancy should be built into critical network devices and network links.
3.7.2	Redundant link should have the same level of security as the primary link. ▪ If the primary link offers encryption and firewall protection, the secondary link should also have similar security level.
3.7.3	Network device configuration and firewall device configuration should be backed up, as per the Backup Policy.

3.8	**External or Third Party Connections**
3.8.1	The Third Party or External connectivity link requests should be approved by Head of Business of the department.
	▪ External networks include connections to customers, IT service providers and subsidiary companies.
	▪ Network operations department should asses the security risks associated with the connection in consultation with the IT Manager.
3.8.2	External network should be separated from MSC BANK network through access control devices.
3.8.3	Any connectivity to third party with any point within the MSC BANK network over Internet should be encrypted and authenticated as per the Remote Access Policy
3.9	**VPN Connectivity**
3.9.1	VPN connectivity should be authorized for users only after explicit approval from IT department.
3.9.2	Users with VPN privileges should be authenticated to ensure that unauthorized users are not allowed access to MSC BANK internal network, as per Remote Access Policy.
3.9.3	The IT Team should conduct periodic reviews of the VPN users.
3.10	**Change Control**
3.10.1	Any change in the internal network architecture or network connectivity should follow the Change Management Policy.
3.10.2	Any change to the network shall be carefully planned based on business system requirements and current and projected trends in MSC BANK's information processing capabilities to avoid potential bottlenecks.

3.11 Logging and Monitoring

3.11.1 All network systems must have security related event logging. Log files generated must never be overwritten or deleted until they are backed up in off-line storage. Log files must, at a minimum, record login failures, remote access (e.g. ftp/sftp, telnet, http/https, ssh, rdp etc.), account lockouts and administrator actions

3.11.2 The network logs should be accessible only to network team.

3.11.3 The devices should be monitored for system utilization and performance.

- The parameters that should be checked are:
  - Bandwidth Utilization
  - CPU and memory utilization in the device
  - Hard disk space utilization

3.11.4 The Network team must review the log files on a daily basis. Log files of administrator activities, network traffic & critical device.

3.12 Vendor Support

3.12.1 Security Feature, service levels and management requirements of all network services should be identified and documented in the service agreement with the network service providers.

3.12.2 The network vendors should be audited for assessing the security measures implemented.

3.12.3 The ability of the network service provider to manage agreed services should be monitored through SLA.

3.13 Security Review

3.13.1 Security analysis of the network including hardening review should be conducted once a year.

3.14 Decommissioning of Network Asset	
3.14.1	Network assets should be decommissioned only after approval from network manager and IT head.
3.14.2	Decommissioning should be done as per the Media Handling Policy.

4. EXCEPTION

Exceptions to provisions of IT Security Policy should be agreed on a case-by-case basis, upon request made by the information owner. The steps for seeking exception approval are as follows:

4.1 A requestor seeking an exception to the Information Security Policy should assess the risks and identify compensating controls so that the risks are managed to an acceptable level. Additionally, the requestor should fill the Exception form and take approval from business /department head.

4.2 The business/department head should review the form with regards to the justification and supporting documents for the exception request. If the risk is acceptable the Business/Department Head should sign-off on the Exception Form.

4.3 Post sign-off from Business/Department Head, the requestor should submit the request for exception to the Chief Information Security Officer (CISO). The CISO should record the decision on the Exception Form and sign-off on the same.

4.4 All exceptions are valid for a period of one year after which, fresh exception approval should be sought for all unresolved issues.

The CISO should review all exceptions, every year, for validity and continued relevance.

5. ROLES AND RESPONSIBILITIES

Roles	Responsibilities
HOD	The heads of departments should be responsible for providing appropriate approvals on request.
IT Team	IT team should be responsible for auditing the implementation of the policy
End users	End users should be responsible for abiding by this policy
Network Team	Network Team should be responsible for implementing and executing the procedures mentioned in this document.

MSC BANK LTD., MUMBAI

PHYSICAL AND ENVIRONMENTAL SECURITY POLICY AND PROCEDURE DOCUMENT

DOCUMENT CLASSIFICATION: INTERNAL AND PROPRIETARY

Version: 2.0

1. OBJECTIVE

a) To provide reasonable physical and environmental security to Bank's IT assets to ensurethat these assets are protected from any unauthorized access and environmental threats
b) To impart guidelines on physical protection of the IT assets of MSC BANK from damage, unauthorized access and environmental factors.

2. SCOPE AND APPLICABILITY

a) The employees of the MSC BANK and any person using the information technology resources of the MSC BANK.
b) All IT assets of the MSC Bank

3. POLICY

All IT assets of MSC BANK shall have appropriate physical access controls in place to protect these assets from unauthorized access and environmental threats/hazards.

3.1	PHYSICAL ACCESS CONTROL
A	***The premises of all the branches, head office and ATMs shall have security vigilance / monitoring around the clock.*** **Procedures** VII. A security guard should be available at all branches, ATMs, Data Centre, and DR Site of the bank VIII. CCTV monitoring should be available on all the branches, ATMs, Data Centre and DR Site of the bank
B	***A system to detect physical intrusion shall be in place.*** **Procedures** V. A burglar alarm should be in place to detect any physical intrusion on all the branches, ATMs, Data Centre and DR Site of the bank

C	***IT Assets of the Bank shall be protected from unauthorized physical access*** **Procedures** **1. Common precautions:** IV. All the critical IT Assets such as servers and communications equipment should be located in locked rooms. V. Entry to the server room / data center should be restricted to unauthorized personnel through the use of lock and key / number pads / swipe cards / biometric controls keys etc. VI. In the open for public areas like branches, IT assets should be so placed to restrict direct accessibility by the customers. VII. Adequate insurance cover should be available to all IT assets against theft 2. **Additional precautions for Bank's Employees:** a) A list of persons authorized to enter restricted area should be maintained b) Each employee should wear an identification badge to gain access to the premises. The badge should have a photo of the employee and should indicate his employee ID. 3. **Additional precautions for Vendors:** a) Only authorized persons should be given access to the Server Room/DC and DR. b) Maintenance staff should be adequately trained not to cause any disturbance to the setup.

	c) Vendors should be accompanied by any one authorized staff member of the Bank. 4. **Additional precautions for Visitors:** a) A visitors' log should be maintained to record all the visits to the server room / data center. b) Visitors should record details of their possessions (e.g., Data cards, removable media) in a register, before entering the Data Centre and the Security personnel should verify the possessions at the time of their exit. . c) Public tours of the Server Room/DC and DR and the other major computer and communications facilities should be prohibited, unless approved by appropriate authority. d) The visitor should be accompanied by at least one person from the technology group and preferably the data center in-charge during the visit
E	***Adequate physical protection shall be provided to handheld it equipment like laptops, tabs etc.*** **Procedures** I. The custody of the handheld IT equipment should be kept with the IT Center. II. In case of carrying such equipment, off premises, following procedure should be followed. a. Written approval from competent authority should be obtained **b.** The details should be entered in register such as Asset number and description, name of the person carrying the equipment, allotted duration and reason for such allotment etc. III. There should be an adequate insurance for the laptops and portable computers, which are allowed to taken off-premises.

	IV. Virus controls must be enabled to protect MSC Bank resources. V. Information processing equipment and media containing highly restricted and confidential data should not be left unattended in public places. VI. Portable computers containing sensitive data should be carried as hand luggage when traveling. VII. Registers should be updated when the equipment are submitted.

3.2	ENVIRONMENTAL THREATS AND CONTROL
1	***Adequate Controls Shall Be Implemented To Protect Bank's It Assets From The Potential Hazard Of FIRE*** **Procedures:** **FIRE PREVENTION:** 1) To minimize potential damage from smoke and fire, kitchen facilities (IF ANY) should be located away from (including not directly above or below) the server and communications facilities. 2) Adequate cooling and humidity should be maintained in the Server Room/DC and DR using precision air conditioners. 3) The Server Room/DC and DR should be free from: • Excessive heat • Inflammable material such as stationery, packaging material etc. • Dust / litter / discarded papers etc. 4) The Server room /data centre should be constructed with fire resistant materials and it should remain structurally stable when there is a fire. It is necessary to ensure that fireproofing extends to ceilings and raised floors 5) Printers should not be placed in the Server Room / DC. 6) The UPS batteries should be stored in separate room with adequate ventilation and cooling. 7) Electric wiring of the Server Room / DC should be checked once in six months. Record of such testing should be kept.

	FIRE DETECTION 1) The Server Room/DC and DR should be equipped with adequate smoke / fire detection system. 2) These systems should be tested once in six months. Record of such tests should be maintained. **FIRE FIGHTING:** 1) The DC and DR should be equipped with suitable fire fighting / suppression system. 2) All the branches and ATMs should be equipped with suitable fire extinguishers of adequate number and capacity. 3) The fire extinguishers should be maintained regularly to ensure adequate pressure and gas quantity. 4) Training should be given to all staff members on the use of the fire extinguisher system once a year.
2	***Adequate Controls Shall Be Implemented To Protect Bank's It Assets From The Potential Hazard Of FLOOD AND WATER SEEPAGE*** **Procedures** 1) Server Room/DC and DR should not be installed in basement. 2) To minimize the potential water damage, rest room and kitchen facilities should not be located next to or above Server Room/DC and DR. 3) Server Room/DC and DR should be facilitated with raised flooring. 4) Adequate controls to prevent any water seepage from ceiling, windows etc. should be implemented such as sealing of windows. Waterproofing of the ceiling etc. 5) Seepage detectors should be planted in the DC / DR.

3.3	OTHER CONTROLS
1	***Uninterrupted and adequate power supply to all the it systems shall be ensured*** ***Procedures:*** 1) Uninterrupted power supply (UPS) machines should be installed for all computing and supporting equipment. The UPS should have adequate capability to continue the power supply to allow for an orderly shutdown of the system. *2)* In areas susceptible to outages of power, generators should be provided to ensure working of servers and all business critical workstations 3) For Server Rooms in DC / DR generator Backup should be provided to support precision air conditioners. *4)* Backup power facilities should be monitored and tested on weekly basis to ensure its functioning.
2	***Secured cabling / electrical fittings shall be available for the IT Assets of the Bank*** **Procedures** 1) Cables connecting computing equipment and other support equipment should be neatly organized and tagged. 2) All electrical wiring and LAN cabling should be structured / concealed cabling, network cabling should be protected from unauthorized interception or damage. 3) Circuit breakers of appropriate capacity should be installed to protect the hardware against sustained increase in power. 4) An overall diagram of the electrical layout including detailed physical network diagrams showing cable routings and terminations should be maintained and should be readily available with the Administration Department. *5)* Electrical mains should be properly guarded against accidental / unauthorized access.

	6) Electric mains should be equipped with ground earthing to protect all computer systems.
3	***Adequate controls shall be implemented to protect Bank's IT assets from the potential damage by RODENTS:*** **Procedures** 1) Regular Pest Control should be undertaken for the Server Room/DC and DR. 2) Eating / drinking in the Server rooms of DC and DR should be strictly prohibited. 3) Server Room should be kept clean and litter free.
4	***Adequate maintenance shall be provided to all IT equipment of the Bank to ensure smooth functioning.*** **Procedures:** 1) Information processing equipment should be maintained in accordance with the vendor/manufacturer's recommended service intervals and specifications. 2) Only authorized personnel should perform repairs and servicing of information processing equipment. 3) Records should be maintained of all repairs, maintenance, faults and suspected faults on information processing resources. 4) All information processing equipment should be covered under an appropriate insurance cover against hardware, theft, damage or loss. 5) IT Assets should be kept in clean and dust-free environment
5	***Adequate controls shall be implemented to provide security to the Server Room in DC / DR*** ***Procedures:*** 1) The Server Room/DC and DR should not be identified by external signs, notices or maps as this may attract the attention of unauthorized individuals. 2) Eating**,** Drinking or smoking should be strictly prohibited in the Server

	Room/DC and DR and a notice to this effect should be displayed in the respective areas. 3) **Emergency Lighting:** In the server room /data centre, automatic emergency lighting should be provided for use during power outages *4)* Physical emergency procedures should be clearly documented. MSC Bank personnel should be trained in appropriate behavior in emergencies. *5)* Contact numbers of concerned persons in case of emergencies should be displayed in the Server Room/DC and DR.

MSC BANK LTD., MUMBAI

SYSTEM ADMINISTRATION POLICY

AND

PROCEDURES FOR IMPLEMENTING THE POLICY

DOCUMENT CLASSIFICATION: INTERNAL AND PROPRIETARY

Version: 2.0

1. OBJECTIVE:

c) To ensure secure and smooth working of IT infrastructure

d) To impart guidelines for taking appropriate controls to establish such secure and smooth working of IT Infrastructure.

2. SCOPE AND APPLICABILITY:

Following IT Systems related functions are covered under this policy

A. SYSTEM MAINTENANCE
B. ANTI-VIRUS ADMINISTRATION
C. IT ASSETS VENDOR MANAGEMENT
D. CHANGE MANAGEMENT
E. VERSION CONTROL
F. INCIDENT MANAGEMENT
G. ASSETS CONTROL
H. HANDHELD ASSETS CONTROL

3. POLICY STATEMENT:

"The Bank shall maintain a secure and smooth working of the entire IT infrastructure to enable uninterrupted business processes and to ensure integrity, availability and confidentiality of the Business Information and IT Assets"

POLICY DETAILS:

3.1	IT SYSTEMS MAINTENANCE
3.1.1	***The Bank shall ensure smooth functioning of its IT Assets*** **Procedures** A. All IT Assets should IT equipment should be kept in clean and dust-free environment. B. Critical IT Assets should be stored in maintained temperature and humidity to avoid excessive heat. C. Timely Maintenance activities for all IT Assets should be ensured. D. The IT Assets should be maintained in accordance with the vendor/manufacturer's recommended service intervals and specifications. E. Only authorized personnel should perform repairs and servicing of IT Assets. F. Regular Pest Control should be undertaken for the Server Room/DC and DR. **ROUTINE MAINTENANCE ACTIVITIES:** In addition to the above, routine activities for better performance of the existing hardware and software shall be undertaken periodically such as A. Disk cleanup and fragmentation of servers and other desktops

	B. Removing of redundant and unwanted data/ information from important storage drives. C. Data Purging and Archiving as and when needed D. Imparting various trainings to the users after assessing the needs etc
3.1.2	***Timely support to IT Assets shall be ensured in case of breakdowns*** **Procedures** A. The critical IT assets such as all servers, routers, networking switches, air conditioners of DC/DR, generator set and UPS should be either under warranty or under comprehensive AMC (Annual Maintenance Contract) with an authorized vendor/ dealer B. All business applications should be either under warranty or under comprehensive AMC (Annual Maintenance Contract) with respective vendors. C. All the systems software such as Operating system, Database, Anti-virus application etc. shall be under comprehensive AMC (Annual Maintenance Contract) with authorized vendors/ dealers. D. Other important components such as fire extinguishers, fire alarm system, smoke detectors, attendance recording devices etc. should be either under warranty or under comprehensive AMC (Annual Maintenance Contract) with respective vendors. E. The Bank may appoint a person / firm for miscellaneous repairs of other than above listed hardware / software on call basis
3.1.3	***Smooth and effective working of outsourced IT activities / functionalities shall be ensured***

	Procedures A. While outsourcing any IT Activity / functionality, the vendor selection should be done as per the Vendor Selection policy of the Bank B. A detail Service Level Agreement (SLA) for all involved parties should be executed. C. The SLA should be measurable. It means the important parameters in the SLA such as uptime assurance, problem resolution period etc. should have been clearly mentioned in terms of units or percentage. D. Also the SLA should cover the escalation matrix. E. The SLAs should be renewed as and when required to keep it valid. F. Performances of outsourced vendors should be tracked based on the incidences violating the SLA terms. G. Taking appropriate penal actions as per the SLA terms is at the Bank's discretion.

3.2	ANTI VIRUS ADMINISTRATION
	Adequate, suitable and updated Anti-virus protection shall be ensured to all IT Assets, by the Bank. **Procedures:** A. The Bank should have adequate number of licenses of suitable anti- virus application to cover all servers, desktops, laptops of the Bank. B. The Bank should have a dedicated server for anti-virus application. C. The anti-virus console /server should update the application directly from the internet as and when the updates are available.

	D. The client machines should update the latest virus definitions from the console as soon as the client machine is connected with the intranet. E. Removable media (CDs/ DVDs/ any USB device) scan should be set to Automatic Scan, so that any such media (CDs/ DVDs/ any USB device) should not be browsed unless scanned for threats. F. The logs of anti-virus application should be reviewed once in a fortnight for scrutinizing the details of quarantined / deleted items for its sources and frequency. Efforts to remove source of such items should be taken and recorded. G. A random test of at least ten clients should be done once in a month to test the correctness of program update. Such test should be recorded with results. H. Users should be made aware about the related security threats and controls thereof.

3.3	IT ASSETS VENDOR MANAGEMENT
3.3.1	***Selection of vendor for IT Assets shall be based on defined criterions.*** **Procedures:** Annexure: Vendor Selection Policy. Mention the reference number.
3.3.2	***A detail record of vendor related documentation shall be preserved and updated. All the activities done by the vendors***

	shall be recorded **Procedures:** A. The original documents of Service level contract / AMC should be maintained by the IT Team. It should be ensured that all these documents are renewed on timely basis and remain valid. B. All visits and activities of vendors should be recorded in the Vendor Registers
3.3.3	***Only authorized persons from the vendor company shall be given access to the MSC Bank's IT Assets*** **Procedures:** A. While granting access to persons from vendor companies, their ID card should be verified B. Vendor activities should be closely monitored and they should not be left alone with Bank's IT assets. Authorized person from the IT team should always accompany the vendor during their visits. C. List of all authorized vendor companies with name of contact person and contact numbers etc. should be made available to all Branches. The same should also be displayed in the server rooms and Data Centre. D. All communication to vendors should be done using only:- • Vendor's Registered address • Vendor's Registered telephone numbers • Vendor's Registered email ID
3.3.4	***Adequate precautions shall be taken to ensure that sensitive data is not exposed to the vendors, while they are given access to the IT Assets of the Bank*** **Procedures:** A. Before any hardware item is handed over to the vendor for taking out of Bank's premises, it should be ensured that the equipment does not contain sensitive data B. **Check if the Bank needs to share its data with OMNI for any reason.**
3.3.5	***The performance of the vendors shall be monitored to ensure***

	compliance with the terms and conditions of Service Level Agreement. **Procedures:** A. The performance of Vendors should be monitored frequently to ensure that the SLA terms are followed. B. Penal actions should be taken as determined in the SLA in case the non-compliance / deviation is beyond the level of acceptance.

3.4	CHANGE MANAGEMENT
3.4.1	***Formal procedures for Change/patch, management shall be laid down for making any changes to the IT systems.*** **Procedures:** A. Changes to any existing IT Asset (hardware / software) should be made only when there is a valid business reason to do so. B. A Business case for change/s to the hardware / software should be prepared by the IT team. C. The change request should be submitted to the competent Authority for a careful study and analysis and approval. D. Changes should be done and effected only after the approval from the competent authority is received. E. Changes to the hardware / software system should be implemented after extensive and successful testing. F. The tests should be carried out on a separate system (test environment) and not on live systems. G. A detail record of changes made in hardware / software should be maintained

3.4.2	***Necessary controls shall be implemented during migrating to a new system to ensure accuracy and completeness of the data.*** **Procedures:** A. While migrating to new systems accuracy of the migrated data should be ensured by branch officials. B. Before migrating to new system entire backup of the old system should be taken and kept in the custody of branch manager. C. If the old system and data should be preserved with restricted physical and logical accesses.

3.5	**VERSION CONTROL**
3.5.1	***Uniform version of all software, throughout the Bank shall be ensured. A formal procedures shall be laid down for controlling the versions of software.*** **Procedures:** • Versions of software should be properly numbered. • Changes to the software versions should be done by the IT Team. • A proper record of version changes should be maintained. • A list of authorized software with latest version should be readily available with the IT Team and all Branches

3.6	INCIDENT MANAGEMENT
	Standard procedures for identifying, reporting and handling IT related incidents shall be defined and circulated among the IT Team of the Bank. *An incident is defined as an attempted or successful unauthorized access, use, disclosure, modification or destruction of any IT asset, causing any disturbance in the smooth functioning of the business. Examples of information security incidents include (but are not limited to):* • *Attempts (either failed or successful) to gain unauthorized logical access to a system or its data.* • *Unwanted disruption or denial of service.* • *Changes to any IT asset without the owner's knowledge, instruction, or consent.* **Procedures:** A. Any IT Security related incident should be handled by the Incident Response Team (IRT) comprising of IT members as well as members from Operational Departments. B. A list of all the IRT members with their contact numbers and roles and responsibilities should be sent to all branches of the Bank. This list should also be displayed in Server Rooms. C. **The bank needs to form detail methods for handling all types of incidents. Check if they have anything. If not, it will be a very big exercise. As good as BCP / DRP**

3.7	ASSETS CONTROL
3.7.1	***CATEGORIZATION AND LABELING OF ASSETS*** 1) All the IT Assets of the Bank shall be categorized based on the prices. Assets pricing below Rs.5,000/- such as sound cards / video cards / CDs / DVDs / pen drives etc., shall not be considered for tracking. There shall be a separate procedure for handling the movement of these assets. 2) The assets to be tracked, shall be listed and this list shall be updated as and when there are additions or disposal of such assets. This list shall contain details such as: a) **ID Number**: All IT Assets shall be labeled with unique identification number. b) Asset Name c) Current Location d) Designated owner e) New Location f) New owner g) Locations of Sensitive Data
3.7.2	***TRACKING OF ASSETS*** The purpose of tracking an asset is to provide a physical protection to the asset against unauthorized use, theft or loss. There shall be a laid down procedure for movement of any IT Asset. 1) When an asset is acquired, an ID will be assigned for the asset and its information shall be entered in the asset-tracking database. 2) The ownership of the assets shall be defined 3) In case of movement of an Asset, there shall be a written requisition authorized by the AGM. 4) Along with the movement of the asset, the tracking database shall be updated.

	5) The changed ownership shall be updated in the database 6) The tracking database shall be reviewed once in every three (3) months for ensuring the completeness and correctness of it. 7) There shall be a random inspections of the IT assets to ensure that those are properly labeled
3.7.3	***TRACKING OF LOW VALUE IT ASSETS:*** 1) The miscellaneous IT Assets such as sound cards / video cards / CDs / DVDs / pen drives etc. shall be recorded separately. 2) The ownership of these assets shall be given to a separate person and the responsible person shall keep a record of movement of these assets. 3) Such record shall be inspected once in every three months by the IT Head to ensure the correctness and completeness of the same. 4) The handling of such assets shall be secure and the responsible person shall ensure that the movement of these assets is among the authorized users only.
3.7.4	***DISPOSAL OF ASSETS*** An asset disposal is a special case. Any asset shall be checked for sensitive data and such data shall be removed prior to disposal. The manager of the user of the asset must determine what the level of maximum sensitivity of data stored on the device is. Below is listed the action for the device based on data sensitivity according to the data assessment process. • Low (Sensitive) - Erase the data using any means such as reformatting or degaussing. • Medium (Confidential) - The data must be erased using an approved technology to make sure it is not readable using special high technology techniques. • High (Secret) - The data must be erased using an approved technology to make sure it is not readable using special high technology techniques.

3.8	HANDHELD ASSETS CONTROL (LAPTOPS / HANDHELD COMPUTERS ETC)
3.8.1	***RECORD:*** 1) The Bank shall have a detail record of all the hand held devices. 2) All such devices shall be identified with unique identity number. 3) All such devices shall be labeled properly with the unique identity number. 4) All accessories of such devices such as charges/ adaptors etc. shall also be labeled with the UID of the parent device.
3.8.2	***STORAGE AND OWNERSHIP*** 1) All the handheld devices shall be stored in the IT Department and the ownership of all these devices lies with the IT Department. 2) All these devices shall be adequately insured against theft and loss.
3.8.3	***ALLOTMENT OF THESE DEVICES:*** 1) Responsibility of allotment of these devices shall be restricted to a team of two or three persons from the IT Department. 2) The allotment shall be done based on a written requisition, authorized by competent authority. 3) Acknowledgement and personal guarantee for taking due care in handling these devices shall be obtained before allotment. 4) The record shall be updated after any such allotment
3.8.4	***LOGICAL ACCESS SECURITY OF THESE DEVICES*** ***The Bank shall ensure maximum logical security to these devices.*** 1) All these devices shall be secured with adequate and updated Anti-virus 2) All these devices shall be password protected. These passwords shall be changed at the time of allotment and also at the time of re-depositing. 3) BIOS password and administration rights shall not be provided to any users.

	4) Personal firewall shall be installed on each such device to restrict unauthorized access. 5) In order to prevent sensitive data being read from a Laptop that has been stolen, an encryption program for secure storage of information shall be activated in all the laptops moving out of the premises. User shall be given basic training in using the encryption programs that are used on Laptop. 6) All the communications between different networks shall route through Virtual Private Network (VPN) and not routed through public network. 7) Users of these devices shall take frequent backups.
3.8.5	***PHYSICAL SECURITY OF THESE DEVICES*** Employees using a laptop shall ensure due care in handling these devices outside the office. The following points to be considered: 1) Such devices shall not be left unattended. 2) Adequate physical security shall be ensured all the time 3) These devices shall be protected from environmental threats such as dust, excessive heat, and radiation with suitable measures such as using protective equipment. 4) These devices shall be protected from other threats such as virus, malwares etc. by taking adequate precautions

MSC BANK LTD., MUMBAI

ORACLE DATABASE SERVER HARDENING POLICY

DOCUMENT CLASSIFICATION: INTERNAL AND PROPRIETARY

Version - 1.0.0

Oracle Database Server Hardening

1) **Restrict administrative privileges/roles granted to user:** We should not provide more privileges than necessary. We should enable only those privileges actually required to perform necessary jobs efficiently. We have revoked DBA role from oracle user and granted required privileges to oracle users. Developers and testers must not have direct access to production databases.

2) **Set default_tablespace to non-SYSTEM tablespace for user accounts:** At the time of creation of new database, we have set default_tablespace to non-SYSTEM tablespace for user accounts

3) **Database Level Audit trails should be enabled on Oracle Database Servers:** Auditing is a method of recording database activity as part of database security. It allows the DBA to track user activity within the database. The audit records will provide information on who performed what database operation and when it was performed. We have set the Auditing parameter on the Oracle Databases and the Parameter of AUDIT_SYS_OPERATIONS is changed from None to DB.

4) **UTL Packages should be restricted to DBA and Authorized Database Users only:** Revoked Execute Permission from role PUBLIC for UTL Packages

5) **Default Oracle Listener Port should be changed for Oracle Database Server :** Oracle Default Listener Port i.e 1521 has been changed and we have set the other than Default Port for Oracle Database Servers.

6) **Apply latest CPU patches provided by Oracle:** Oracle issues a Cumulative Patch Update (CPU) or Patch Set Update (PSU) every quarter that fixes number of security vulnerabilities. It is imperative to keep the Oracle database instance at the latest patch

level. While creating a new Oracle database instance make sure you install the latest security patch. Oracle database security patches are cumulative, so you need to install only the latest patch update. We have applied latest CPU patches on Oracle Database Servers.

7) **Default Password of OS user of Oracle Database Server should be changed periodically:** We are changing Default Password of OS user of Oracle Database Servers in 90 days.

8) **Backup and Archive logs retention Policy:** Last 7 days, Oracle RMAN Backup will be kept in Oracle Database Servers and afterword that backup will become obsolete . We are deleting obsolete backup. Archive logs retention policy is set for 7 days.

9) **Test backup and restore procedures regularly :** Backups should be verified by performing recoveries to ensure backups function properly. Every Month, We are restoring CBS Production Database Backup on CBS Test Database Server.

10) **Review log files periodically:**

Oracle generates several log files and many of them can provide useful information to assist in auditing and securing the database. Automated or manual review of these log files on a daily/weekly basis should be one of the key responsibilities of a database administrator.

Alert. log - Chronologically records messages and errors arising from the daily database operation. Also, there are pointers to trace files and dump files. Monitor alert log periodically for ORA- type errors.

This log file is stored under background_dump_dest specified in init.ora or spfile.

listener. log -The logfile shows a timestamp, command issued, and result code. If an Oracle error is returned, it will include the error message. The default directory is $ORACLE_HOME/network/admin.

11) **Backup Database:** Backup and recovery of your Oracle database is important to protecting data from corruptions, hardware failures, and data failures. Presently, we are taking Export backup and RMAN Backup for the Oracle Database Servers. Also, We are taking backup on tape and tape backup is testing on Test Database Server periodically.

12) **Maintain disaster recovery and standby database**

Oracle Data Guard: It enables you to use either a physical standby database (Redo Apply) or a logical standby database (SQL Apply), or both, depending on the business requirements. A physical standby database provides a physically identical copy of the primary database, with on-disk database structures that are identical to the primary database on a block-for-block basis. The database schema, including indexes, is the same. A physical standby database is kept synchronized with the primary database by applying the redo data received from the primary database through media recovery.

MSC BANK LTD., MUMBAI

WINDOWS SERVER 2008 HARDENING

DOCUMENT CLASSIFICATION: INTERNAL AND PROPRIETARY

Version - 1.0.0

Windows Server 2008 Hardening

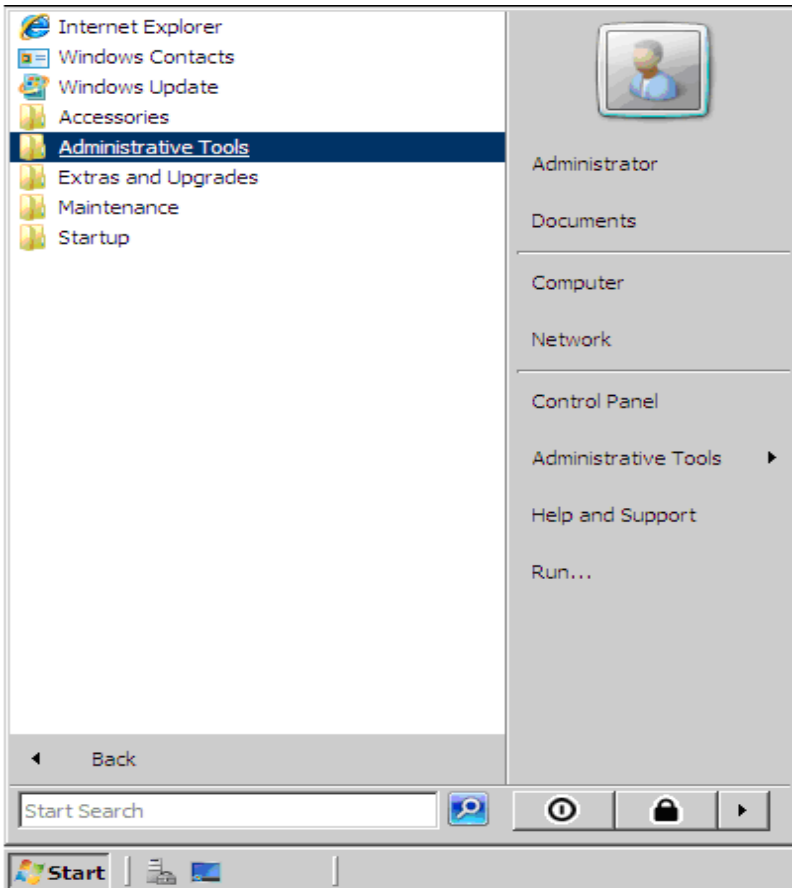
1. Configure a Security Policy:

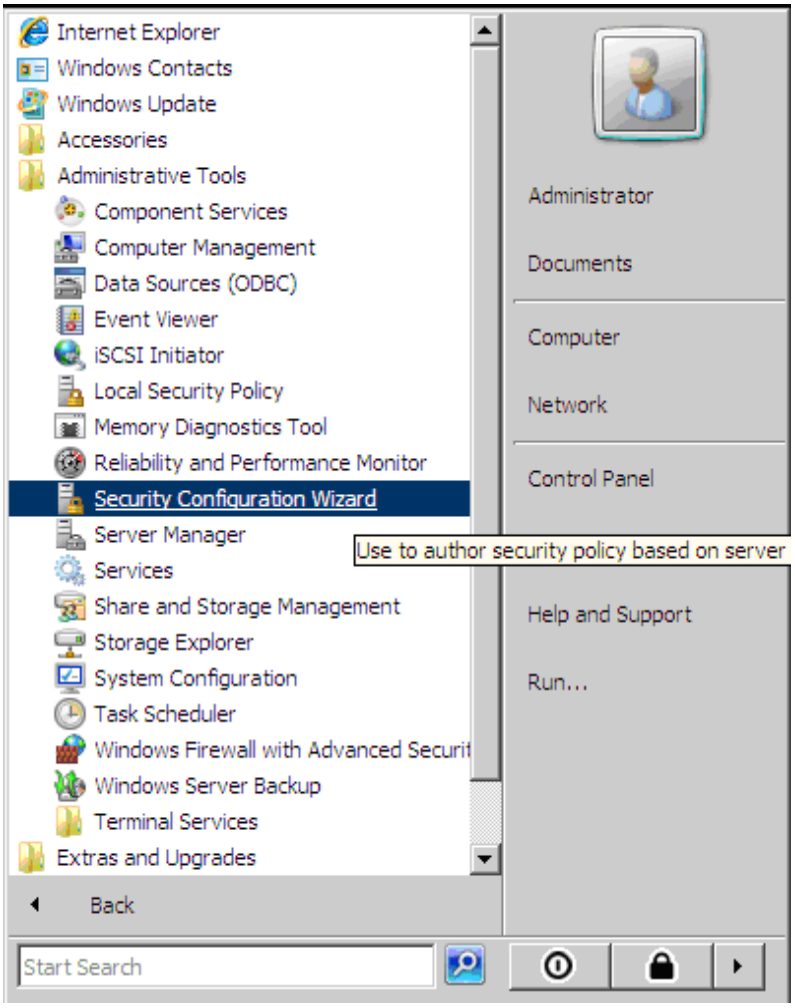
Install Security Configuration Wizard through Add and remove windows components which detect ports and services, and configure registry and audit settings according to the server's role.

- Disable unnecessary services based on the server role
- Remove unused firewall rules and limit existing firewall rules.
- Define restricted audit policies.

For Configuring the Secuirty Policy wizard Go to **Start --> Programs --> Administrative Tools**

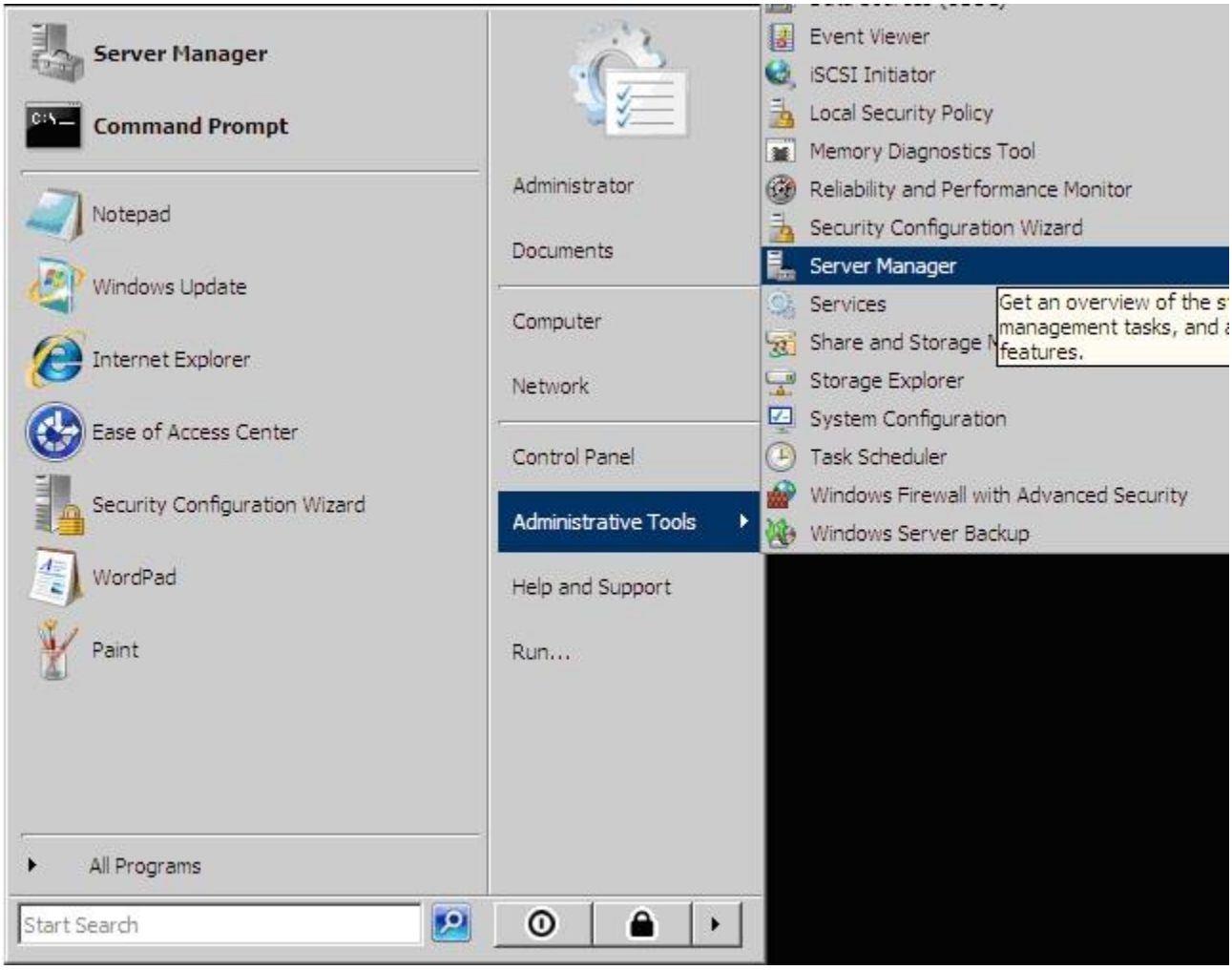
--> secuirty Configuration Wizard.




Internet Explorer
Windows Contacts
Windows Update
Accessories
Administrative Tools
Component Services
Computer Management
Data Sources (ODBC)
Event Viewer
iSCSI Initiator
Local Security Policy
Memory Diagnostics Tool
Reliability and Performance Monitor
Security Configuration Wizard
Server Manager
Services
Share and Storage Management
Storage Explorer
System Configuration
Task Scheduler
Windows Firewall with Advanced Securit
Windows Server Backup
Terminal Services
Extras and Upgrades
Back
Start Search
Administrator
Documents
Computer
Network
Control Panel
Use to author security policy based on server
Help and Support
Run...

2. **Disable or Delete Unnecessary accounts:**

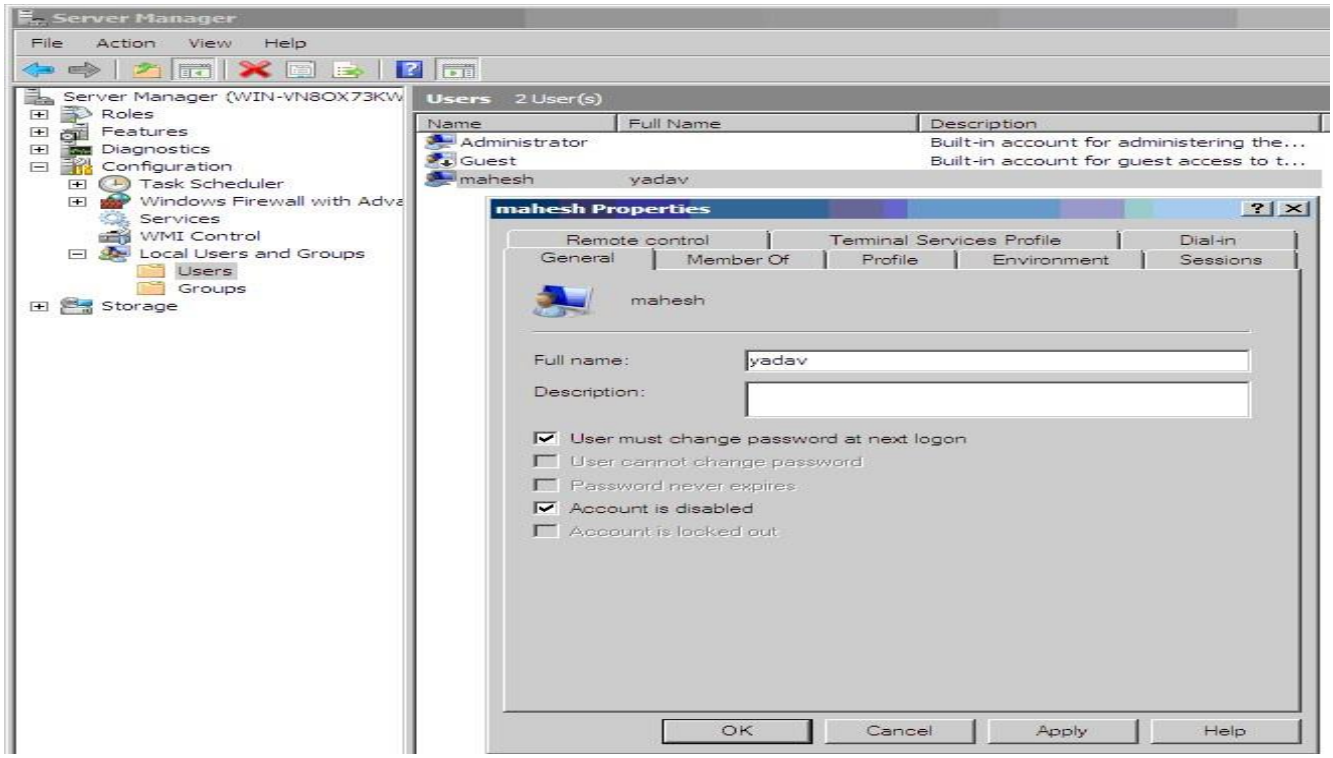
Attackers often gain access to servers through unused ports and services. So block the unused ports, protocols and by disabling services that are not required. During installation by default the Administrator, Guest and Help Assistant are created. As a security expertise the administrator account should be disabled to make it more difficult for an attacker to gain access. Both Guest and Help Assistant accounts should be disabled at all times.



or Disabling or deleting the accounts: Go to **Start -->programs --> Administrative Tools --> Server**

Manager Configuration --> Local Users and Groups --> users

Right click on the user --> properties --> check for the account is disabled

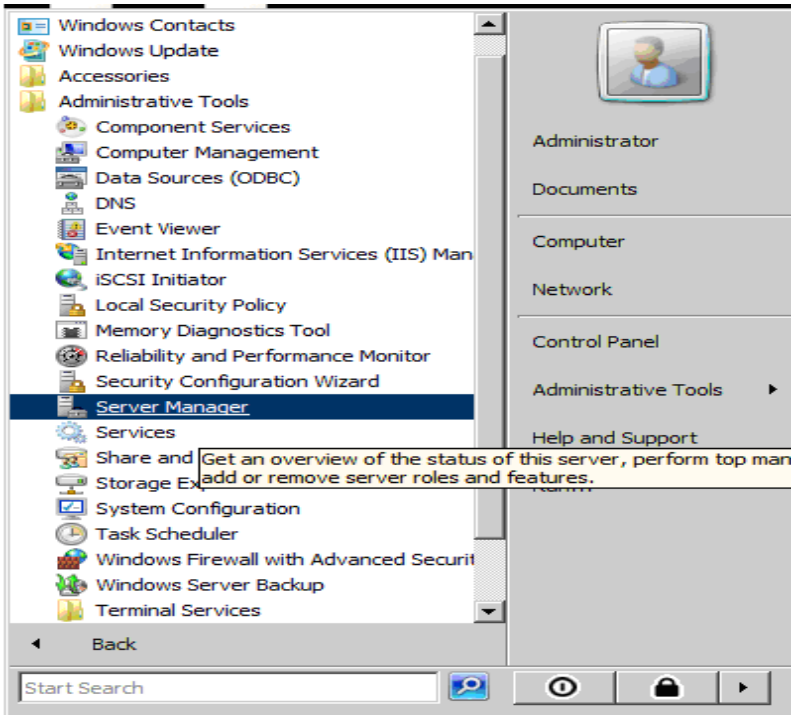


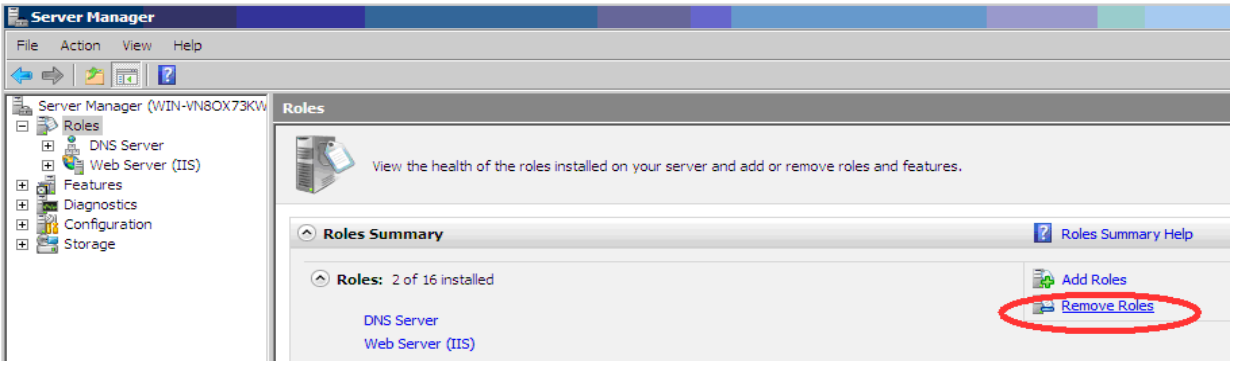
3. Uninstall Unnecessary applications or roles:

The number of applications installed on the servers should be role related. It is a good idea to test these applications out in a separate environment before deploying them on the production network. Some applications make use of service backdoors, which can sometimes compromise the overall security of the server.

For uninstalling the unnecessary application: Go to **start --> programs --> Administrative tools**

--> Server manager --> Roles --> Click remove roles



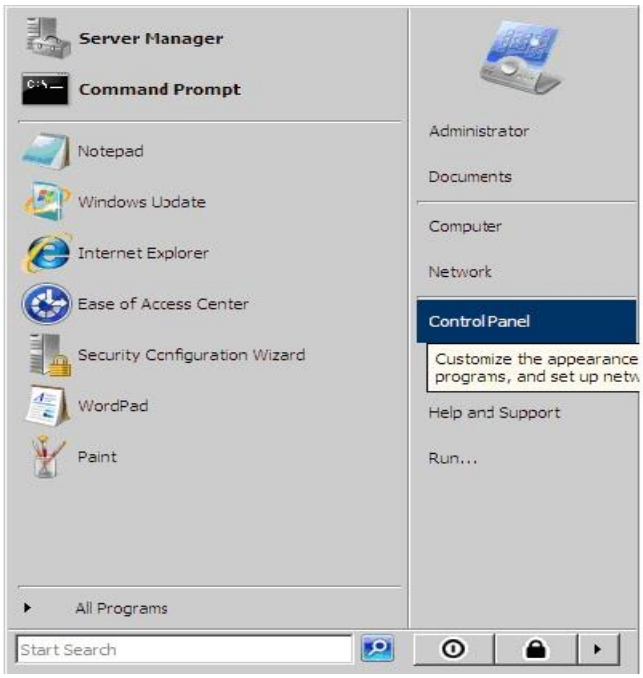


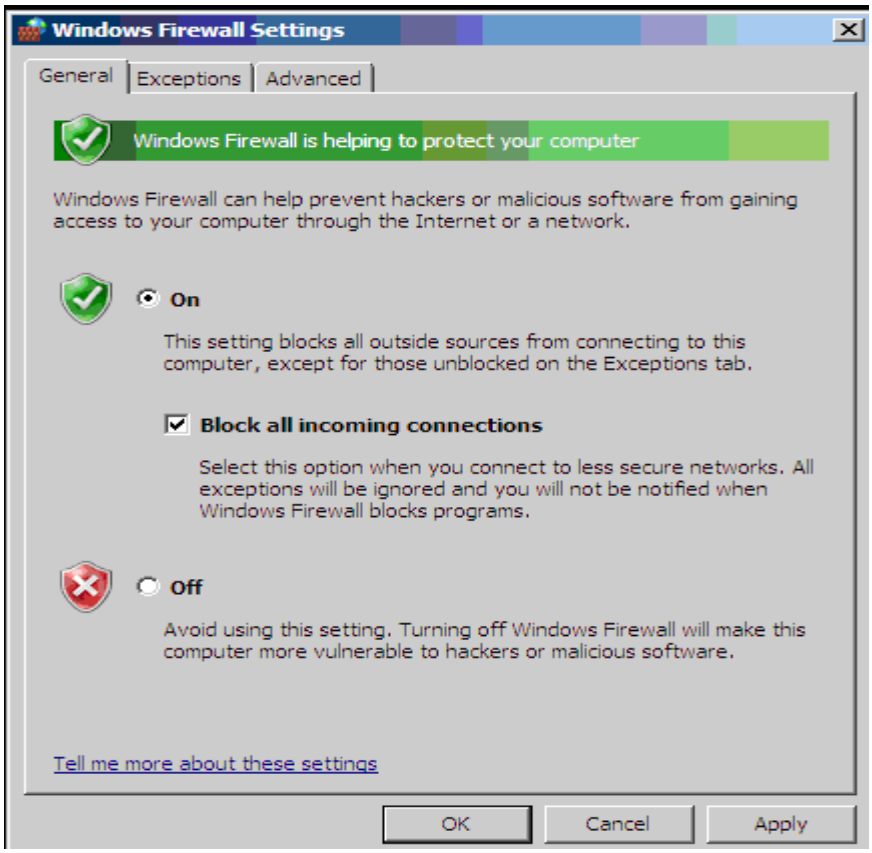
4. Configure the windows 2008 firewall:

Windows 2008 server comes with a built in firewall called the Windows Firewall with Advanced Security. As a security best practice, all servers should have its own host based firewall. Bi- directional firewall which filters the outbound traffic as well as inbound traffic. IPSEC encryption configurations are integrated into one interface. Using the advance rules you can build the firewall rules using Windows Active Directory objects, source & destination IP addresses and protocols.

For configuring the windows 2008 firewall: Go to **Start --> Control Panel -**

-> Windows Firewall --> Change Settings



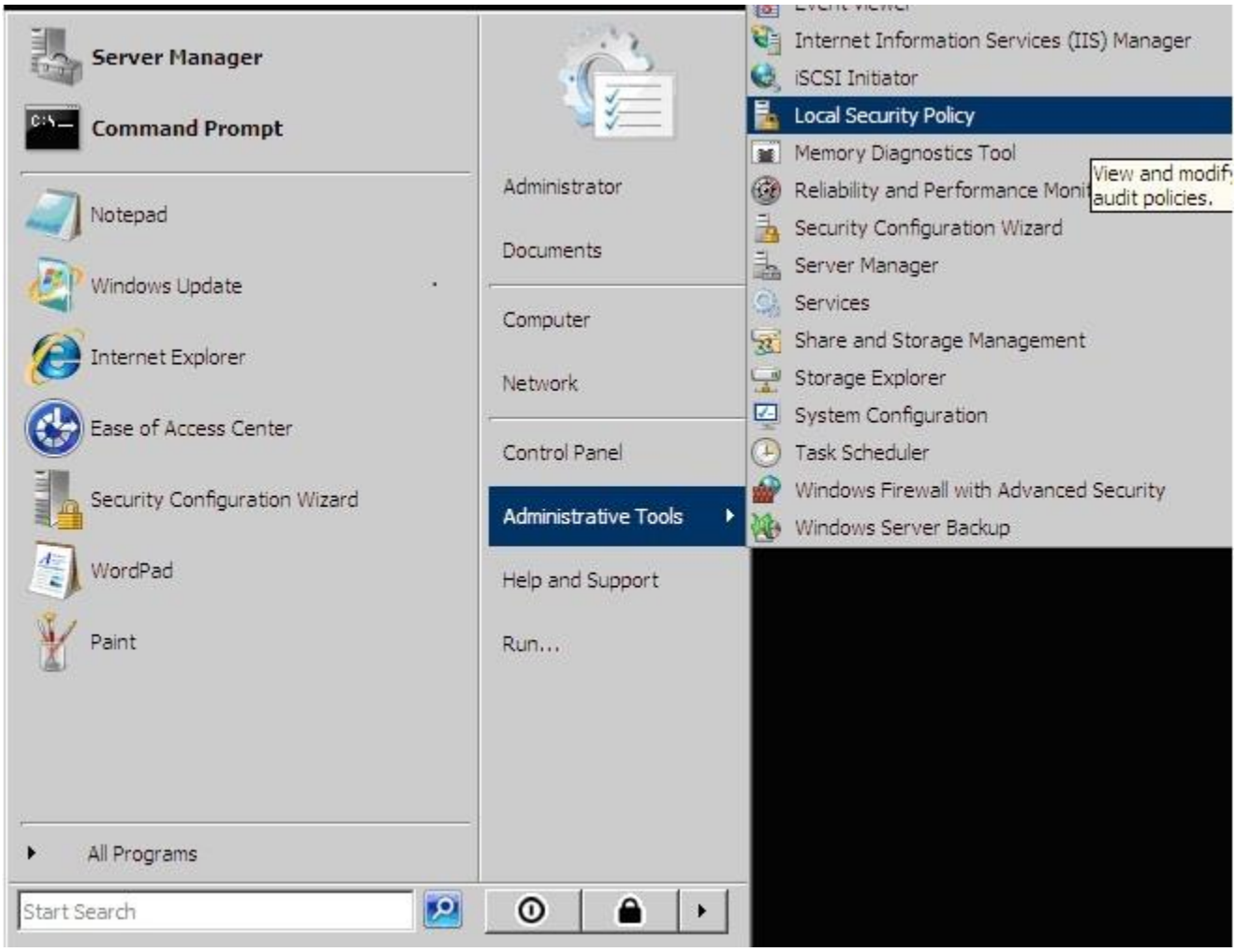


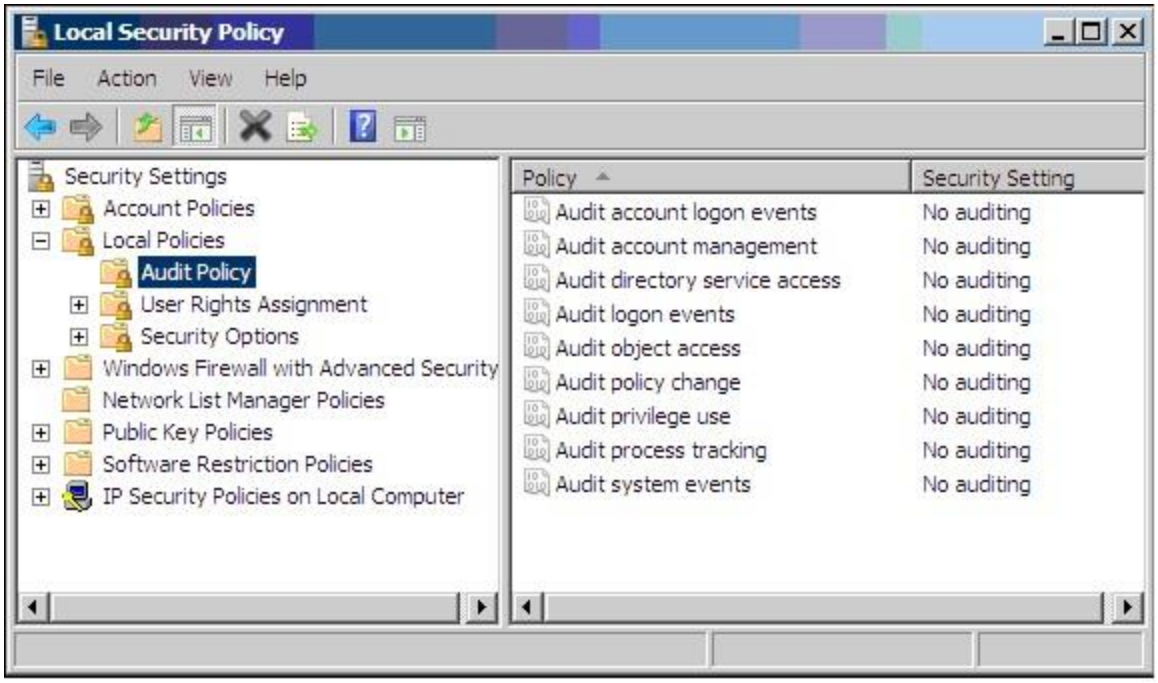
5. Configure Auditing:

The following events should be logged and audited.

- Audit account logon events
- Audit account management
- Audit directory service access
- Audit logon events
- Audit object access
- Audit policy change
- Audit privilege use
- Audit process tracking
- Audit system events

For Configuring the Auditing: Go to **Start --> Control Panel --> Administrative Tools --> Local Secuirty policy --> Secuirty Setting --> Local policies --> Audit policies**




Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
IP Security Policies on Local Computer
Policy
Security Setting
Audit account logon events
No auditing
Audit account management
No auditing
Audit directory service access
No auditing
Audit logon events
No auditing
Audit object access
No auditing
Audit policy change
No auditing
Audit privilege use
No auditing
Audit process tracking
No auditing
Audit system events
No auditing

6. Disable Unnecessary shares:

Unnecessary shares create a threat to critical servers. So it is necessary to disable the unnecessary shares. This can be done using the following command: Net share

This will display a list of all shares on the server. If there is a need to use a share, system and security administrators should configure the share as a hidden share and harden all NTFS and Share permissions.

C:\Documents and Settings>net share

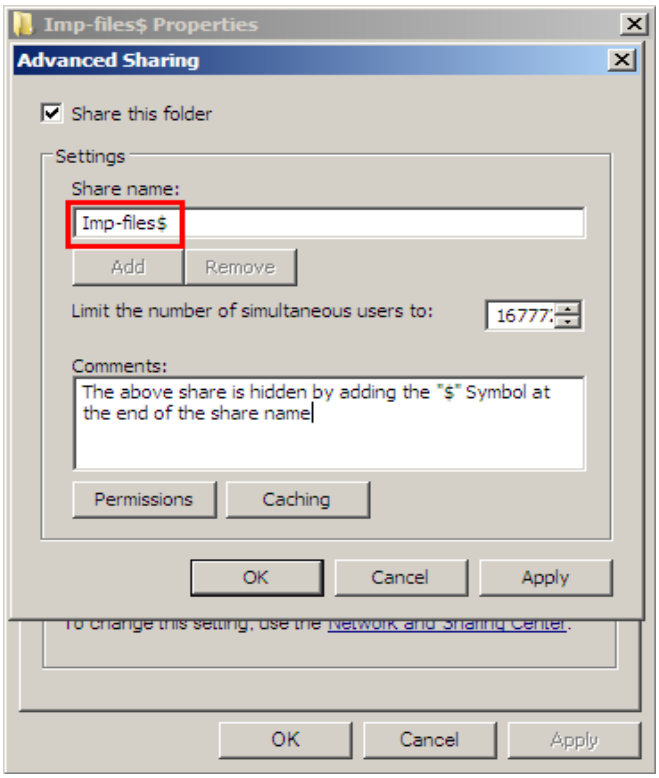
Share name Resource Remark

ADMIN$ C:\WINDOWS Remote Admin

C$ C:\ Default share

IPC$ Remote IPC

In order to create a hidden share, put a $ (Dollar) sign after the share name. The share will still be accessible; however it will not be easily listed through the network. Example: Accounting$



7. Configure Encryption:

According to industry standards, the servers require host sensitive information to make use of the encryption system. Windows Server 2008 provides a built in whole disk encryption feature called BitLocker Drive Encryption (BitLocker) which protects the operating system and data stored on the disk. To install BitLocker, select it in Server Manager or type the following at a command prompt:

C:\ServerManagerCmd -install BitLocker –restart

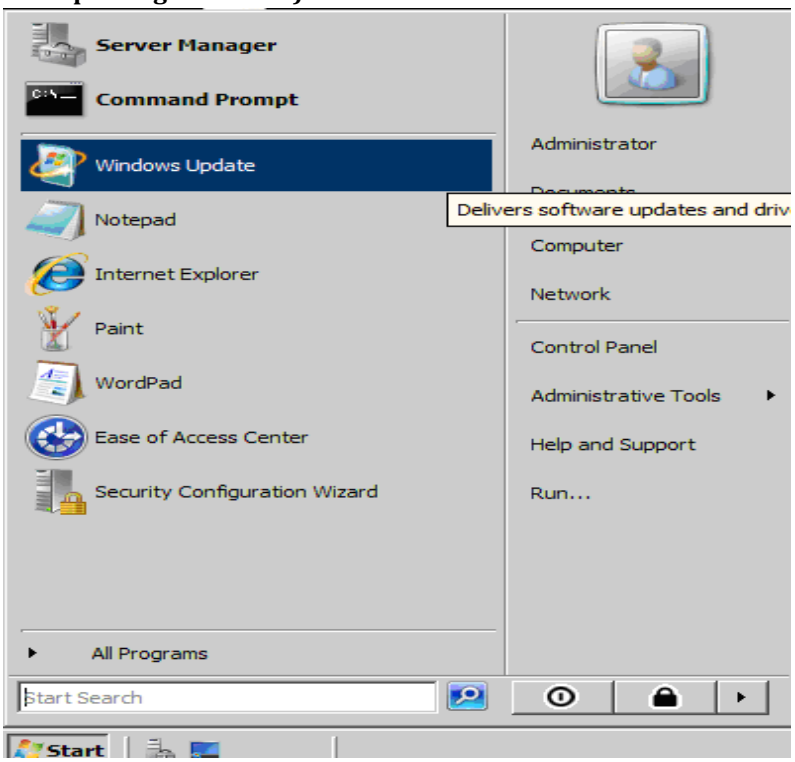
For Configuring the Encryption on 2008 server: Go to **Start --> Programs --> Administrative Tools --> Server Manager --> Features --> Bit locker** (It will be accessed only when active directory gets installed in windows server 2008)

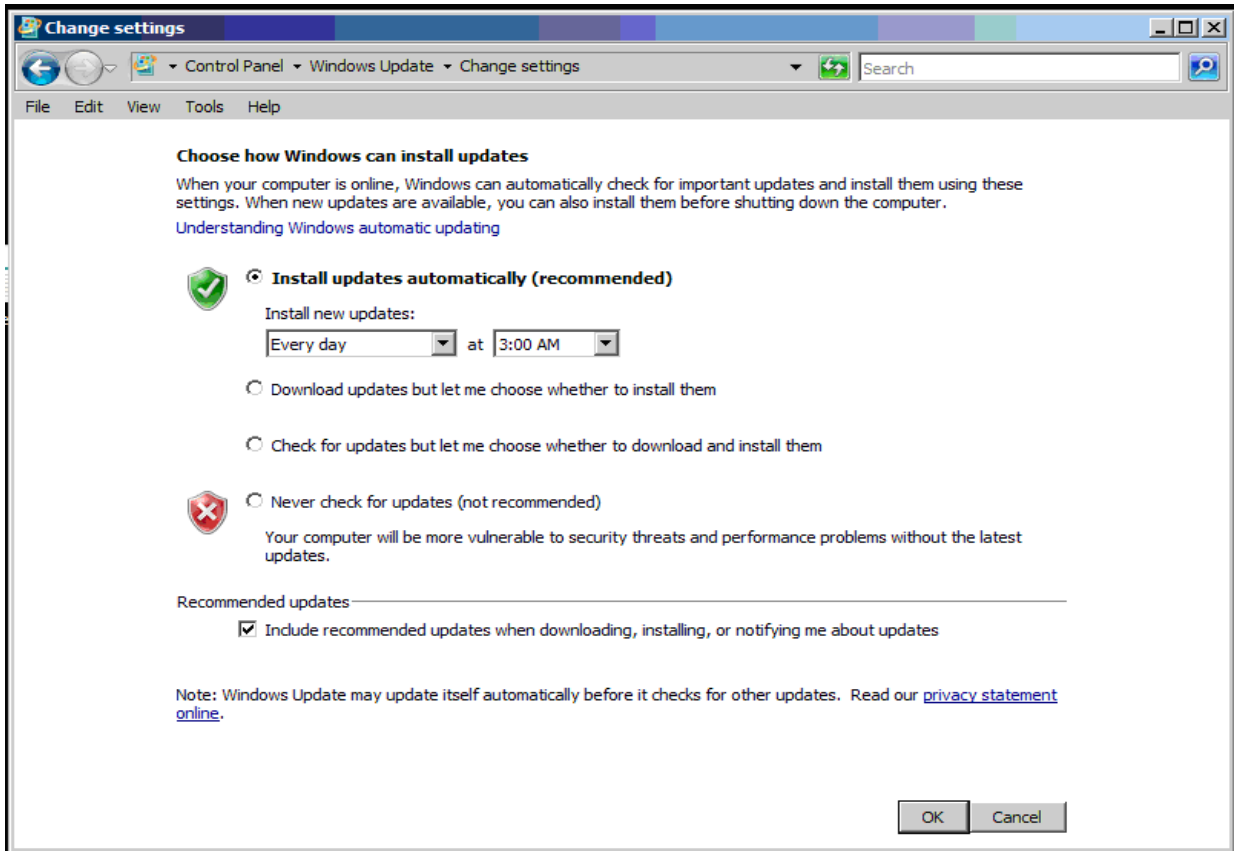
8. Windows Updates and Patches:

Updates and Patches are key elements for hardening a server. The system and security expertise should be constantly updating and patching their servers against vulnerabilities. Administrators should periodically check the vendor's websites for updates. Windows Server Update Services (WSUS) provides a software update service for Microsoft Windows operating systems and other Microsoft software.

The Windows automatic updates service should be configured to use WSUS Server.

For updating manually Go to: Start –> Windows Update **(Make sure Automatic Updates is turned ON if not updating via WSUS)**




Change settings
Control Panel ▸ Windows Update ▸ Change settings
Search
File Edit View Tools Help
Choose how Windows can install updates
When your computer is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also install them before shutting down the computer.
Understanding Windows automatic updating
Install updates automatically (recommended)
Install new updates:
Every day
at
3:00 AM
Download updates but let me choose whether to install them
Check for updates but let me choose whether to download and install them
Never check for updates (not recommended)
Your computer will be more vulnerable to security threats and performance problems without the latest updates.
Recommended updates
Include recommended updates when downloading, installing, or notifying me about updates
Note: Windows Update may update itself automatically before it checks for other updates. Read our privacy statement online.
OK
Cancel

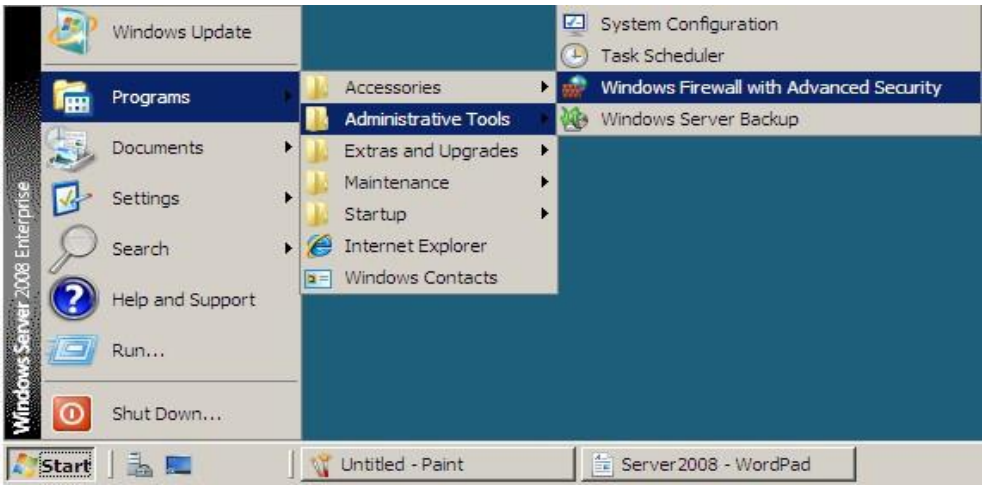
9 A System Software

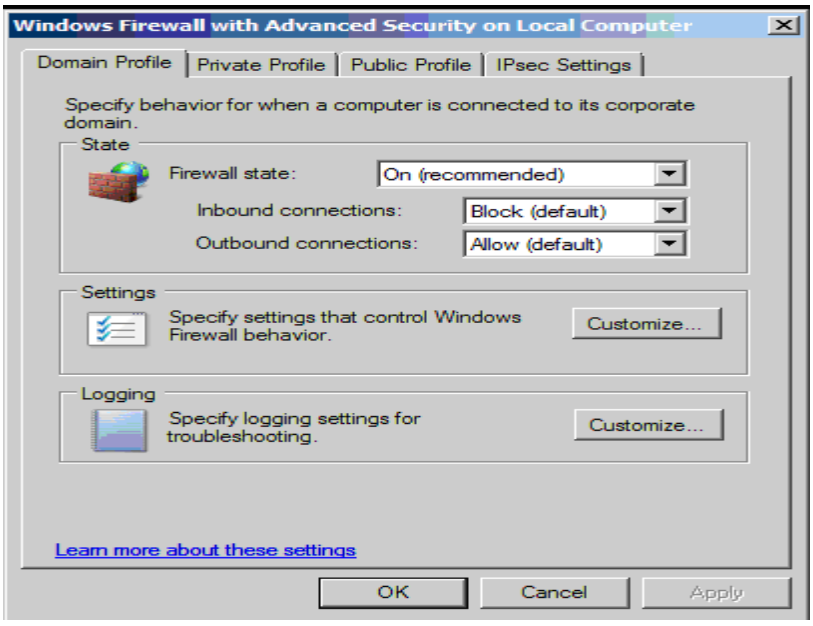
The following system level applications should be installed.

- Install Enterprise License Antivirus on each newly built server.
- Other software's as per requirement of respective application request

9. Least Privilege:

Server services should not be configured using enterprise wide administrator accounts.

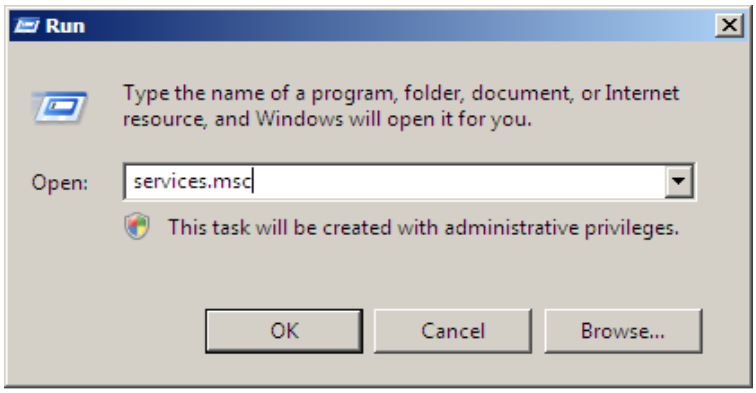


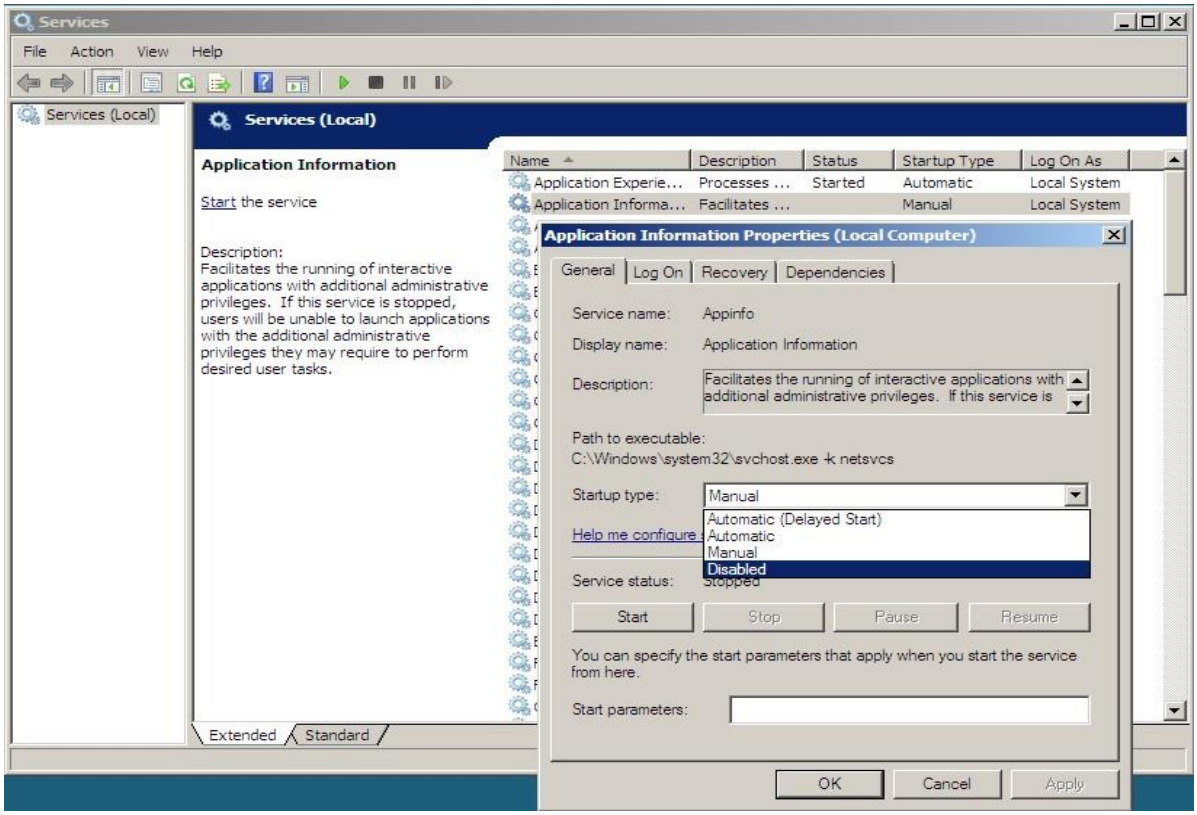


10. Disable Automatic Services:

Here are all the services are disabled that were set to automatic startup. By disabling these services you can limit attack surface area which can prevent or limit exploitation of the server.

For Disable Automatic services Go to: **Start --> run --> Services.msc --> Disable unneeded services**





11. Disable Remote Registry:

This service allows registry access to authenticated remote users. Even though this is blocked by the firewall and ACLs this service should be turned off if you have no reason to allow remote registry access.

For Disabling the remote registry Go to: **Start --> Control Panel --> Windows firewall --> ON**

If you have Corporate network follow the below steps:

Click Start – RUN --> Type "regedit" and press enter -->
Navigate to

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecureP ipeServers

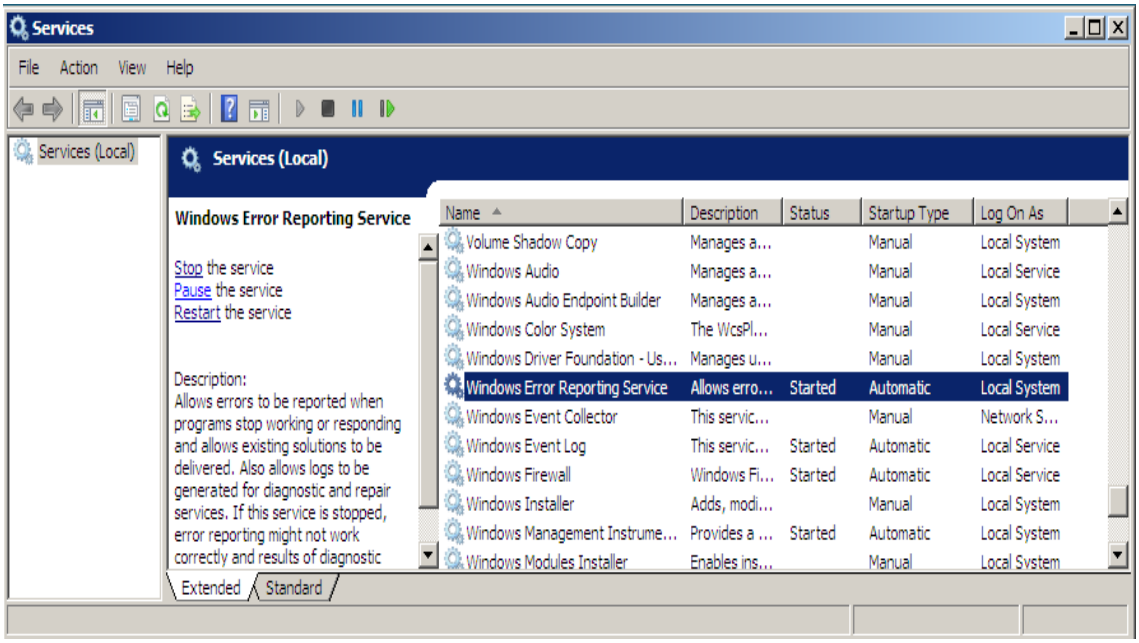
Select "winreg" and click Edit, Select "Permissions"

Select appropriate users/groups & appropriate permission like "Read" or "full Control". Click OK and exit.

12. Windows Error Reporting Service:

Windows Error Reporting (WER) is a set of Windows technologies that capture software crash data and support end-user reporting of crash information. Through Winqual services, software and hardware vendors can access reports in order to analyze and respond to these problems. WER technologies are implemented in Windows XP, Windows Server 2003, and later.

Go to: Start --> programs --> Administrative tools -> server manager -- > Configuration --> Local users and groups.


Services
File Action View Help
Services (Local)
Services (Local)
Windows Error Reporting Service
Stop the service
Pause the service
Restart the service
Description:
Allows errors to be reported when programs stop working or responding and allows existing solutions to be delivered. Also allows logs to be generated for diagnostic and repair services. If this service is stopped, error reporting might not work correctly and results of diagnostic
Name
Description
Status
Startup Type
Log On As
Volume Shadow Copy Manages a... Manual Local System
Windows Audio Manages a... Manual Local Service
Windows Audio Endpoint Builder Manages a... Manual Local System
Windows Color System The WcsPl... Manual Local Service
Windows Driver Foundation - Us... Manages u... Manual Local System
Windows Error Reporting Service Allows erro... Started Automatic Local System
Windows Event Collector This servic... Manual Network S...
Windows Event Log This servic... Started Automatic Local Service
Windows Firewall Windows Fi... Started Automatic Local Service
Windows Installer Adds, modi... Manual Local System
Windows Management Instrume... Provides a ... Started Automatic Local System
Windows Modules Installer Enables ins... Manual Local System
Extended
Standard