Version History

Ver. No.	*Authors*	*Date*	*Reviewers*	*Review Date*	*Release Date*
1.0	Information Technology Team	27-Aug-2018	QMF	31-Aug-2018	03-Sep-2018
2.0	Information Technology Team	02-Dec-2019	QMF	13-Dec-2019	16-Dec-2019
3.0	Information Technology Team	10-07-2020	Vincent Dsouza	10-July-2020	

Change History

Ver. No.	*Section*	*Date*	*Change Information*	*RFC No.*
1.0	All	03-Sep-2018	New Release	-
2.0	All	16-Dec-2019	Annual Release	-
3.0	All	23-01-2020	Hardening Document for Windows Included, Password Policy for Network devices mentioned. Backup retention policy mentioned	-

Table of Contents

Information Technology Process

1. Objectives

- The objective of this document is to describe the activities involved in Information Technology activities
- The objective of this document is to describe the activities related to Information Technology function

2. Scope

- This process applies to activities involved in Information Technology function
- This process applies to all activities involved in seeking assistance / help from Information Technology

3. Policy

3.1 Policy Statement

- Refer to Information Technology Policy

3.2 Framework to Support or Implement this Policy

- Refer to Information Technology Procedure

4. References to (checklists, forms, guidelines, lists, standards, templates, other processes)

Process Element	***Description***	***ID***
Checklists	NA	
Forms	Daily Monitoring Report	QMS-L4-FR-IT-01
	Email Request	Email
	Email Request for Closing / Locking / Forward Emails	Email
	Service Level Matrix for Issues	QMS-L4-FR-IT-02
	Service Level Issues Closing Report	QMS-L4-FR-IT-03
	Software Installation Request	Email
	Master List of Softwares	QMS-L4-FR-IT-04
	Anti-Virus Software Request – Desktop / Laptop / Server	Email
	Windows Hardening Document	QMS-L4-FR-IT-05
	Linux Hardening Document	QMS-L4-FR-IT-06
	Backup / Restoration Request	Email
	Data-card Installation Request	Email
	Outlook Configuration Request	Email
	Linux Evolution Configuration Request	Email
	Windows Client Addition in Domain Request	Email
	Linux Client Addition in Domain Request	Email
	Lync Installation Request	Email
	Cyberoam Firewall Configuration Request	Email
	Core Switch Basic Configuration Request	Email
	Domain Controller Configuration Request	Email
	VPN Change Management Request	Email
	ISP Change Management Request	Email
	Capacity Change Management Request	Email
	Unlock / Reset Password Request	Email

Process Element	***Description***	***ID***
	Desktop / Laptop Issue Request	Email
	HR Email for Creation of new employee and giving Access	Email
	Head of Department Email for granting access to employee for Application / Database / Network / System	Email
	HR Email for separation of employee for removing Access	Email
	Printer Configuration Request	Email
	Patch Intimation from OEM	Email
	Patch Updation using Tool	Tool
	Patch Testing Details	QMS-L4-FR-IT-07
	Network Access / Alter Request	Email
	VA Report	Vendor Report
	Change Request Form	QMS-L4-FR-MR-05
	Change Request Register	QMS-L4-FR-MR-06
	Risk Management Plan	QMS-L4-FR-MR-03
Guidelines	IT Manual	QMS-L4-GD-IT-01
	IT Asset Tags	QMS-L4-GD-IT-02
Lists	Employee Eligibility List	QMS-L4-LS-IT-01
Standards	NA	
Other Processes	Information Technology Process	

5. *Entry Criteria*

Inputs	***Source Processes***
Daily Monitoring Report	Daily monitoring of IT Activities
Email Intimation from HR	Human Resources
Email Request for Closing / Locking / Forward Emails	Human Resources / Head of Department
Issue Request - helpdesk	User Groups
Software Installation Request	User Groups
Anti-Virus Installation Request	User Groups
Hardening Documents – Windows / Linux	IT Team
Backup / Restoration Request	User Groups
Printer Configuration Request	User Groups
Datacard Installation Request	User Groups
Outlook Configuration Request	User Groups
Linux Evolution Configuration Request	User Groups
Windows Client Addition in Domain Request	User Groups
Linux Client Addition in Domain Request	User Groups
Lync Installation Request	User Groups
Cyberoam Firewall Configuration Request	IT Team
Core Switch Basic Configuration Request	IT Team
Domain Controller Configuration Request	IT Team
VPN Change Management Request	IT Team
ISP Change Management Request	IT Team
Capacity Change Management Request	IT Team
Unlock / Reset Password Request	User Groups
Desktop / Laptop Issue Request	User Groups
HR Email for Creation of new employee and giving Access	HR Team
Head of Department Email for granting access to employee for Application / Database / Network / System	Head of Department
HR Email for separation of employee for removing Access	HR Team
Patch Intimation from OEM	OEMs
Network Access / Alter Request	User Groups
Change Request Form	IT Team
Change Request Register	IT Team

6. *Responsibilities*

Role	***Responsibilities***
Head – Information Technology	• Oversee all technology operations (e.g. network security) and evaluate them according to established goals • Devise and establish IT policies and systems to support the implementation of strategies set by upper management • Analyze the business requirements of all departments to determine their technology needs • Purchase efficient and cost effective technological equipment and software • Inspect the use of technological equipment and software to ensure functionality and efficiency • Identify the need for upgrades, configurations or new systems and report to Senior Management • Coordinate and supervise team members and provide guidance • Control budget and report on expenditure • Assist in building relationships with vendors and creating cost-efficient contracts
Manager – Information Technology	• Manage information technology and computer systems • Plan, organize, control and evaluate IT and electronic data operations • Ensure security of data, network access and backup systems • Act in alignment with user needs and system functionality to contribute to organizational policy • Identify problematic areas and implement strategic solutions in time • Audit systems and assess their outcomes • Preserve assets, information security and control structures
Executive – Information Technology (System Administrator / Database Administrator / Network Administrator)	• Install and configure software and hardware • Manage network servers and technology tools • Set up accounts and workstations • Monitor performance and maintain systems according to requirements • Troubleshoot issues and outages • Ensure security through access controls, backups and firewalls • Upgrade systems with new releases and models • Build an internal wiki with technical documentation, manuals and IT policies

7. *Process Description*

Information Technology Team is involved in the following activities:

- Daily Monitoring
- Email Id Creation Process
- Email ID Closing / Locked / Forward
- Response Time Matrix
- List of IT Asset Tag Categories
- IT Asset Tag Category
- Employee Eligibility Table
- Software Installation
- Anti-virus Installation
- Operating System Hardening
- Backup Restoration
- Printer Configuration on Windows
- Data Card Installation
- Microsoft Outlook Configuration
- Linux Evolution Configuration
- Add Windows Client in Domain

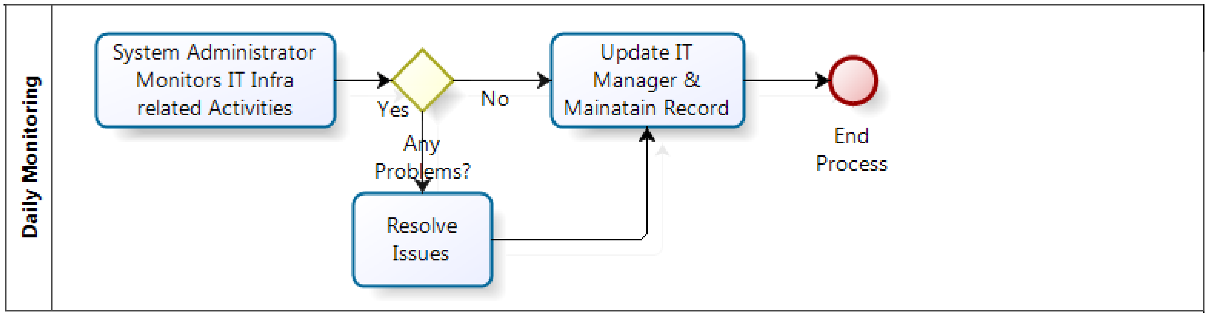
- Add Linux Client in domain
- Lync Installation
- Configuration Cyberoam Firewall
- Core Switch Basic Configuration
- Configuration of Domain Controller
- Server Security – Hardening
- VPN Change Management Process
- ISP Change Management Process
- Capacity Management Process
- Password Management Process
- Desktop Process
- Access Control
- Patch Management
- Network Management

Overview Diagram

Refer to individual activity process flow diagrams.

Information Technology IT Manual

7.1 Daily Monitoring


Daily Monitoring
System Administrator Monitors IT Infra related Activities
Yes
Any Problems?
No
Update IT Manager & Mainatain Record
End Process
Resolve Issues

- The System Administrator will monitor all IT infra related things during the day as mentioned below.
- In case of issues found, the same is addressed by the System Administrator and keeps the Manger IT informed of the same.
- System Administrator will provide Daily Monitoring Report mail every morning after doing a health check of servers and also confirming all the application are working fine.

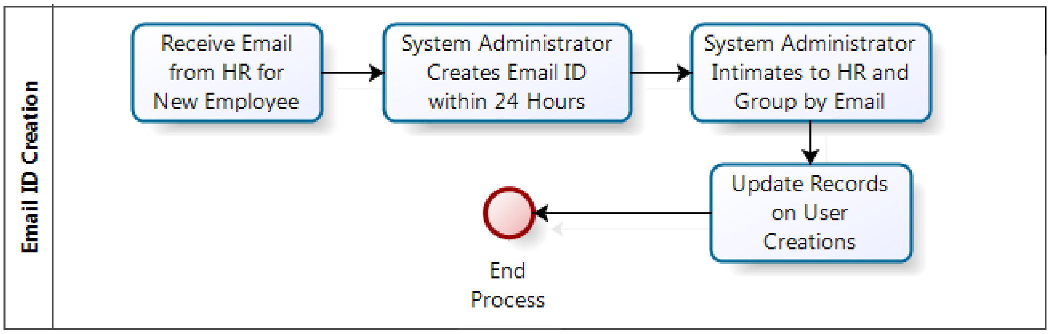
Category	Committed Time in Hours	Priority
Network Troubleshooting	2	High
Email Troubleshooting	2	High
Server Troubleshooting	2	High
Application Software installation / Troubleshooting	4	Medium
Application Software troubleshooting	4	Medium
Printer installation / Maintenance	4	Medium
Hardware installation / Troubleshooting	6	Medium
OS installation / Troubleshooting	6	Medium
Documentation	6	Medium
Miscellaneous	8	Low

Email Account Configuration	24	Medium
Asset Installation	48	Medium

Daily monitoring format

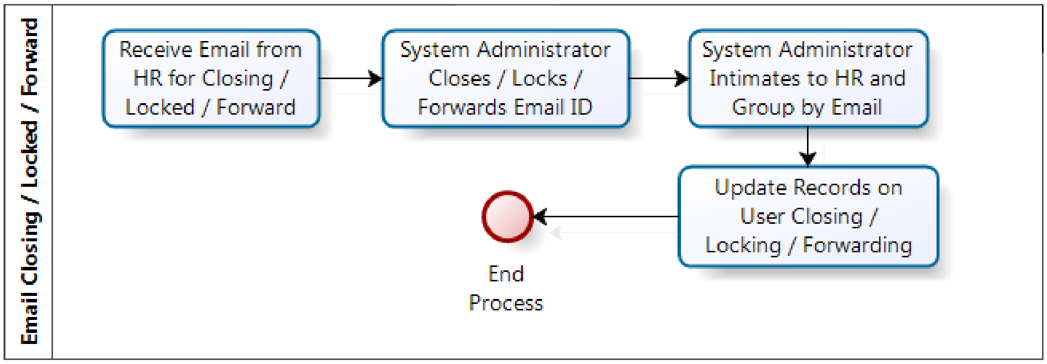
Sr. No.	Daily Activity	Activity Description	Standard Time
1	Backup Server	Data Backup	30
		Service Check	10
		Space Utilization	10
		Log Check	15
		Connectivity Check	5
2	Firewall	Service Check	10
		Space Utilization	10
		Log Check	15
		Connectivity Check	5
3	Antivirus (VMWARE)	Service Check	10
		Space Utilization	10
		Log Check	30
		Antivirus Update Check	30
		Connectivity Check	5
4	Domain Controller	Service Check	10
		Space Utilization	10
		Log Check	15
		Connectivity Check	5
5	ISP Connection Links	Internet	10

7.2 *Email ID Creation*


Email ID Creation
Receive Email from HR for New Employee
System Administrator Creates Email ID within 24 Hours
System Administrator Intimates to HR and Group by Email
Update Records on User Creations
End Process

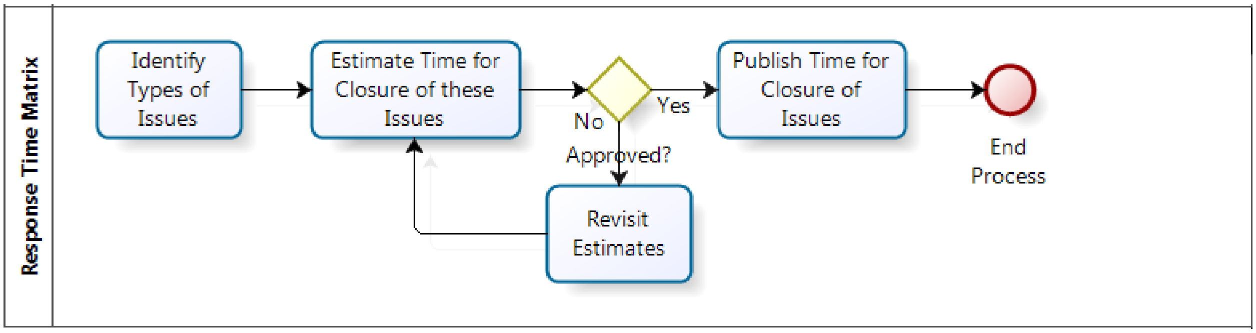
- HR sends email to IT Department to create Email creation for New Employees
- On receipt of the above, the System administrator will create the user within 24 hours
- The System administrator will follow the procedure for creation of user id as per IT Manual
- Once the user is created, Sys Admin will send a mail to HR and cc to System Administrator group informing about the mail ID creation.
- The user creation details will be updated on the User Creation Record.
- Refer IT Manual for screenshots

7.3 *Email ID Closing / Locked / forward*


Email Closing / Locked / Forward
Receive Email from HR for Closing / Locked / Forward
System Administrator Closes / Locks / Forwards Email ID
System Administrator Intimates to HR and Group by Email
Update Records on User Closing / Locking / Forwarding
End Process

- HR team would send an email to the IT Team for user email id closing / locked
- Based on the email, the user id is locked or closed based on the request if the email is required to be forward or closed request
- Once the respective e-mail is either closed or locked, the same to be updated in the MIS report
- In case, the E-mail ID is forwarded the same to be confirmed for closed / locked.
- Refer IT Manual for screenshots

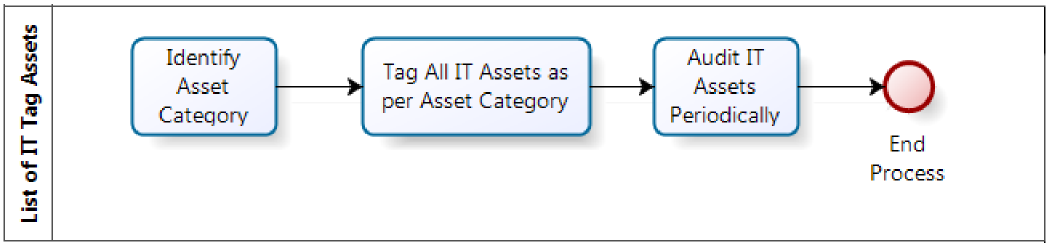
7.4 *Response Time Matrix*



- As per the Helpdesk process, we commit a response time to every ticket. The following are the various types of the issues and the corresponding are the response time. The IT infra team will work hard to ensure that all issues is responded within the committed response time.
- Refer IT Manual for screenshots
- In each IT Audit the issues and the response time will be re-looked to make necessary recommendations

Sr. No.	Type of Issue	Response time
1	Network Issues	1 hours
2	Printer Issues	3 hours
3	Hardware Issues	2 hours
4	Software Issues	4 hours
5	OS Installation	5 hours

7.5 *List of IT Tag Assets*


List of IT Tag Assets
Identify Asset Category
Tag All IT Assets as per Asset Category
Audit IT Assets Periodically
End Process

- Following are the list of IT Asset and their corresponding TAG Category.
- Refer IT Manual for screenshots
- During the Audit the Categories are reviewed and ensure all the additional asset categories are included.
- Asset Tag Categorization as follows:

XX-CIPL-<Location>-<Serial Number>

XX – Category of Asset (DT-Desktop, LT-Laptop, PR-Printer, SW-Network Switch, TP-Tape Drive / USB Drive, FW – Firewall)
CIPL – Clover Infotech Pvt. Ltd.
<Location> **-** JBR-JB Nagar Mumbai, PUNE-Pune Office)
<Serial Number> **-** Continuous Serial Number

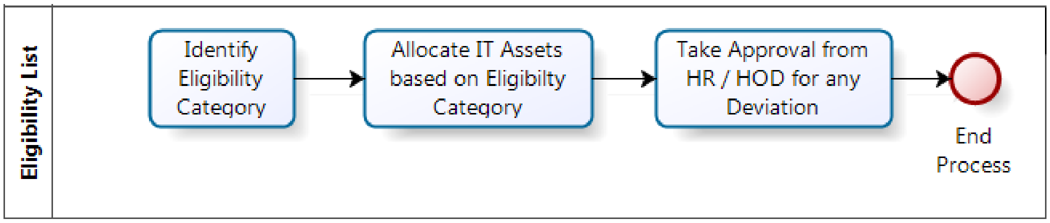
IT asset tag category

Asset Category	**Asset TAG**
Desktop	DT-CIPL-JBR-001
Laptop	LT-CIPL-JBR-001
Printer	PR-CIPL-JBR-001
Network Switch	SW-CIPL-JBR-001
Tape Drive / USB Hard Drive	TP-CIPL-JBR-001
Firewall	FW-CIPL-JBR-001

IT asset are tagged with the following information:

Type	Description
Classification :	Restricted/ Confidential/ Internal/ Public
Contact No :	
Location :	

7.6 *Employee Eligibility list*

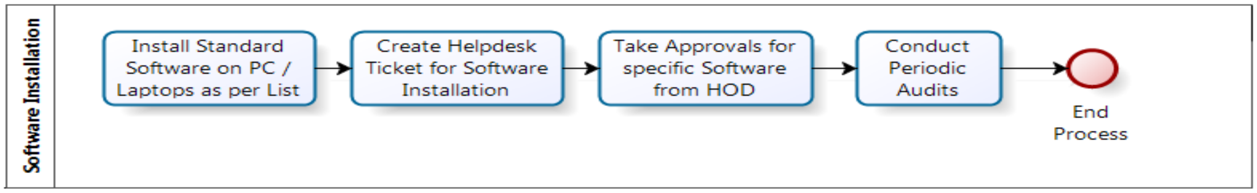

Eligibility List
Identify Eligibility Category
Allocate IT Assets based on Eligibilty Category
Take Approval from HR / HOD for any Deviation
End Process

- All allotment of IT asset to employee's should be done in line with the below mentioned eligibility.
- In case of deviation, the same should be communicated by the HR or Functional Manager
- Refer IT Manual for screenshots

Employee eligibility table

Sr. No.	Employee Level	IT equipment entitlement / eligibility
1	M1	Desktop
2	M2	Desktop
3	M3	Laptop or Desktop depending on need basis
4	M4	Laptop
5	M5	Laptop
6	M6	Laptop
7	M7	Laptop
8	M8	Laptop

7.7 *Software Installations*


Software Installation
Install Standard Software on PC / Laptops as per List
Create Helpdesk Ticket for Software Installation
Take Approvals for specific Software from HOD
Conduct Periodic Audits
End Process

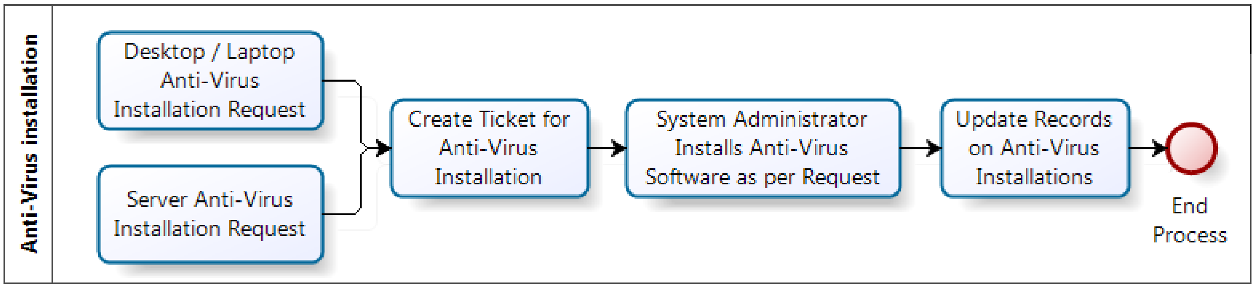
All software installation should be done as per the instructions given below.

- Any change in upgrade, the SOP for the same needs to be updated
- In case of any new Software purchased, same needs to be updated and approved in the standard software list.
- All Software across the organization is standardized. The same is listed as below.
- Audit should bring out whether the SOP is followed and recommend best practices.
- The individual requiring the same with the prior approval of the supervising manager or HR in case of new joinees initiates any request for Software installation.
- All requests for Software installation will be executed as a part of Helpdesk ticket number. The same is updated once it is completed
- Refer IT Manual for screenshots
- List of Softwares as follows:

Approved Software Versions

Sr. No	Product	Versions				Purchase Due Date	Vendor Info
1	MS Office	2003	Professsional	Standard			
2	MS Office	2010	Professsional	Standard			
3	MS Office	2012	Professsional	Standard			
4	MS Office	2013	Professsional	Standard	365 Pro		
5	MS Office	2016	Professsional	Standard	365 Pro		
6	MS Visio	2003	Professsional	Standard			
7	MS Visio	2010	Professsional	Standard			
8	MS Visio	2016	Professsional	Standard			
9	MS Project	2003	Professsional	Standard			
10	MS Project	2010	Professsional	Standard			
11	MS Project	2016	Professsional	Standard			
12	MS OneNote	2003					
13	MS OneNote	2010					
14	MS OneNote	2016					
15	MS Publisher		All versions				
16	Windows OS	XP	All versions				
17	Windows OS	7	All versions				
18	Windows OS	8	All versions				
19	Windows OS	8.1	All versions				
20	Windows OS	10	All versions				
21	Windows Server	2003	All versions				
22	Windows Server	2010	All versions				
23	Windows Server	2012	All versions				
24	MAC OS		All versions				
25	JAVA		All versions				
26	Oracle		All versions				
27	SQL		All versions				
28	Dot Net		All versions				
29	Chrome		All versions				
30	FireFox		All versions				
31	IE Explorer		All versions				
32	Adobe PDF		All versions				
33	Cute PDF		All versions				
34	Adobe Acrobat Writer		All versions				
35	Adobe Photoshop		All versions			04-Feb-17	Best Buy
36	Corel Draw		All versions			Trail Version	
37	Team Viewer		All versions			Trail Version	
38	Ginger		All versions				
39	Cisco Webex		All versions			Feb-17	Web Con IT Solution Pvt Ltd
	SSL Certifcates for the below						
40	https://cloverinfotech.co.in/Pay/Logon.aspx					Feb-17	Geo Trust
41	https://iconnect.cloverinfotech.in/adrenalin/					Feb-17	Geo Trust
42	https://email.cloverinfotech.com:8443/					Jul-17	Rapid SSL
43	https://mail.cloverinfotech.com:8443/					Sep-17	Rapid SSL
44	https://cloverinfotech.co.in/Pay/Logon.aspx					Feb-17	Geo Trust
	https://cloverinfotech.co.in:8180/CloverQMS/					Jul-17	RApid SSL - JNR
45	Zimbra connector for Outlook		All versions				
46	MS Visual Studio and its components		All versions				
47	Adobe Reader		All versions				
48	Adobe Writer		All versions				
49	Adobe Photoshop		All versions				
50	Corel Draw		All versions				
51	Cisco Web Ex		All versions			Feb-17	Web Con IT Solutions
52	Skype for Business and Standalone		All versions				
53	Ginger (Spell Check for marketing team)		All versions				
54	Tight VNC		All versions				
55	Spark		All versions				
56	Tata Photon Plus		All versions				
57	Airtel Internet Dongle		All versions				
58	CD burner XP		All versions				
59	Citrix Receiver		All versions				
60	Ammy Admin		All versions				
61	AnyDesk remote software		All versions				
62	Command Shell		All versions				
63	Other applications & Plug-ins apart from the ones mentioned above which are would be required for Application development use only from time to time						

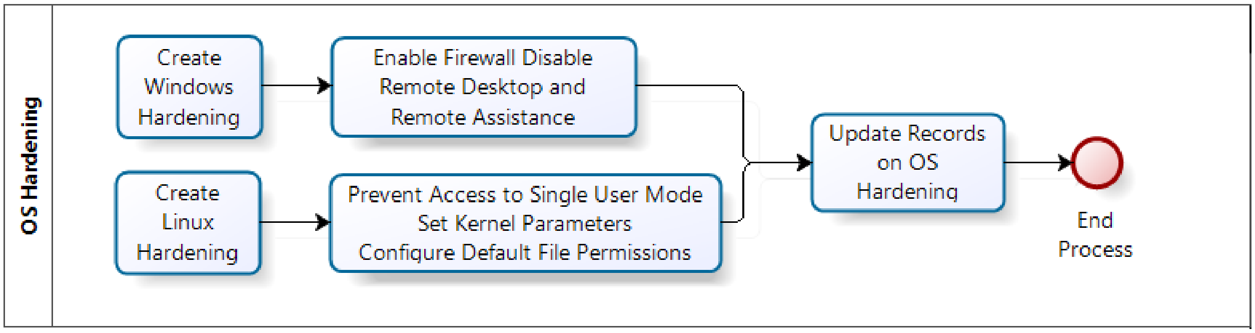
7.8 Anti-Virus & Ant- Malware Software installation


Anti-Virus installation
Desktop / Laptop Anti-Virus Installation Request
Server Anti-Virus Installation Request
Create Ticket for Anti-Virus Installation
System Administrator Installs Anti-Virus Software as per Request
Update Records on Anti-Virus Installations
End Process

All Anti-Virus installation should be done as per the instructions given below.

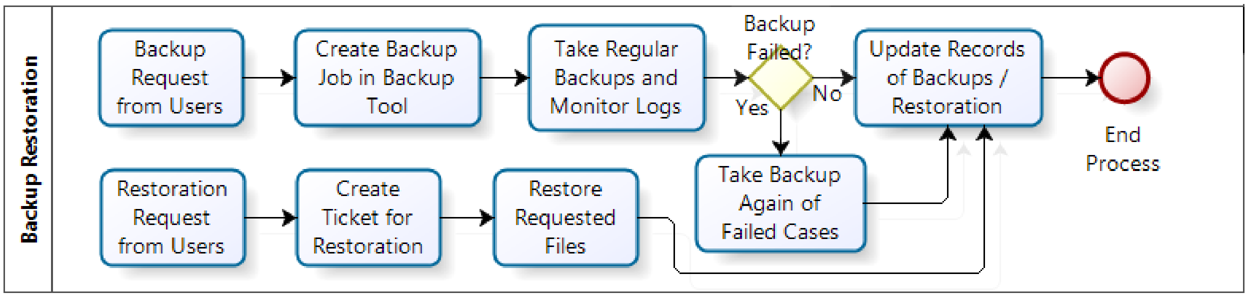
- Anti-Virus Software should be installed on all Desktops / Laptops
- Anti-Virus Software should be installed on all Servers
- All requests for Software installation will be executed as a part of Helpdesk ticket number
- Update all records related to installation of Anti-Virus
- Download daily signatures received from Service Providers
- Update signatures on all Desktops / Laptops / Servers
- Identify Desktops / Laptops / Servers not updated with latest signatures and update manually
- Refer IT Manual for screenshots

7.9 Operating System Hardening


OS Hardening
Create Windows Hardening
Enable Firewall Disable Remote Desktop and Remote Assistance
Create Linux Hardening
Prevent Access to Single User Mode Set Kernel Parameters Configure Default File Permissions
Update Records on OS Hardening
End Process

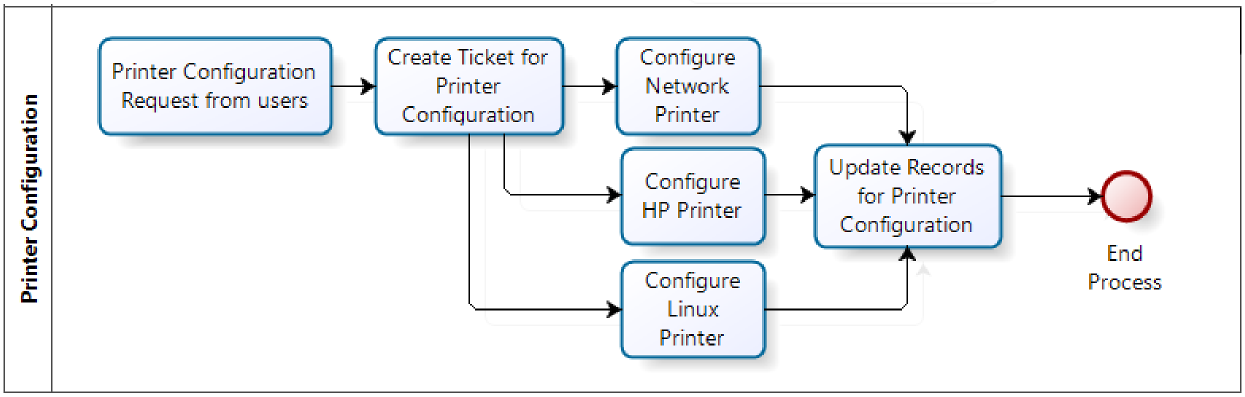
- Create Hardening Document for Windows Operating System with following parameters:
    - Enable Firewall Disable
    - Remote Desktop and Remote Assistance
- Create Hardening Document for Linux Operating System with following parameters
    - Prevent Access to Single User mode
    - Set Kernel Parameters
    - Configure Default Parameters
- Update all records related to OS Hardening
- Refer IT Manual for screenshots

7.10 Backup Restoration


Backup Restoration
Backup Request from Users
Create Backup Job in Backup Tool
Take Regular Backups and Monitor Logs
Backup Failed?
Yes
No
Update Records of Backups / Restoration
End Process
Take Backup Again of Failed Cases
Restoration Request from Users
Create Ticket for Restoration
Restore Requested Files

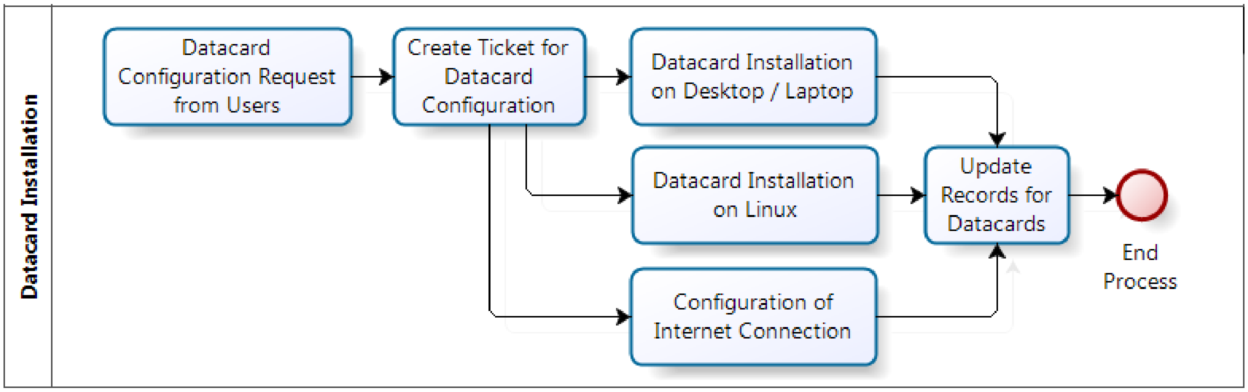
- Receive Request from Users for backup of files / folders
- IT Team creates batch job in Backup Tool
- IT Team takes regular backups based on the time defined
- IT Team checks logs of backups
- IT Team takes backup of failed cases again and updates backup records
- Receive Request from Users for restoration of file / folder
- IT Team creates ticket for restoration. Backup Restoration to be done once a year between July - Sept
- IT Team restores requested file / folder and share with Users
- IT Team sends email to Users to update status
- IT Team updates restoration records
- Refer IT Manual for screenshots
- Backup to be conducted on daily & monthly basis of different hard drives.
- Backup Retention Policy is for 6 months.

7.11 Printer Configuration


Printer Configuration
Printer Configuration Request from users
Create Ticket for Printer Configuration
Configure Network Printer
Configure HP Printer
Configure Linux Printer
Update Records for Printer Configuration
End Process

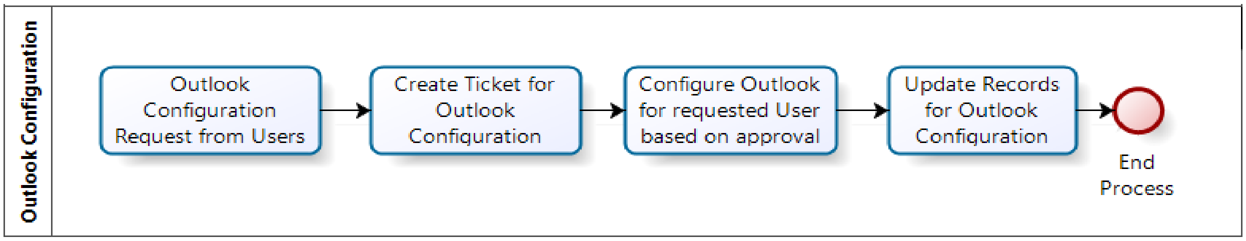
- Receive Request from Users for Printer Configuration for Network / HP / Linux Printer
- IT Team creates ticket for Printer Configuration based on the approval
- IT Team configures the requested printer and update records
- Refer IT Manual for screenshots

7.12 Datacard Installation


Datacard Installation
Datacard Configuration Request from Users
Create Ticket for Datacard Configuration
Datacard Installation on Desktop / Laptop
Datacard Installation on Linux
Configuration of Internet Connection
Update Records for Datacards
End Process

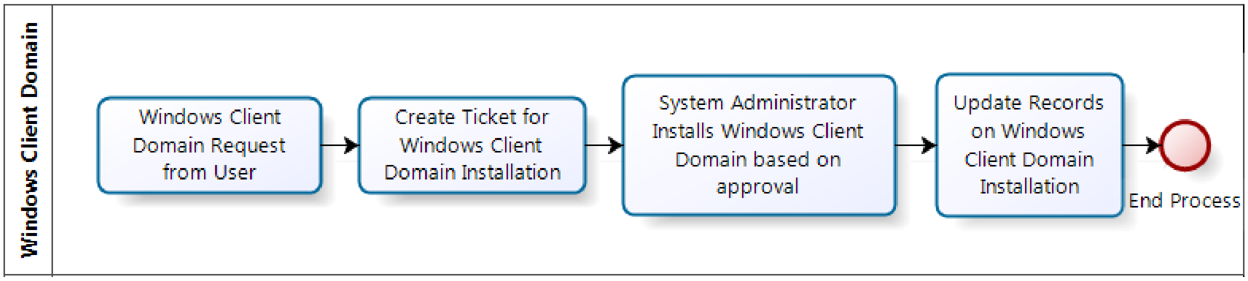
- Receive Request from Users for Datacard installation for Desktop / Laptop / Linux / Internet Connection
- IT Team creates ticket for Datacard installation based on the approval
- IT Team configures the requested Datacard and update records
- Refer IT Manual for screenshots

7.13 Microsoft Outlook Configuration


Outlook Configuration
Outlook Configuration Request from Users
Create Ticket for Outlook Configuration
Configure Outlook for requested User based on approval
Update Records for Outlook Configuration
End Process

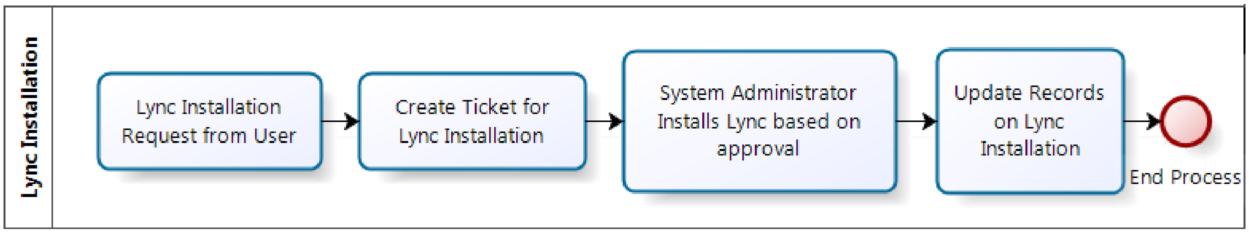
- Receive Request from Users for Outlook Configuration for Desktop / Laptop
- IT Team creates ticket for Outlook Configuration based on the approval
- IT Team configures Outlook for requested User and update records
- Refer IT Manual for screenshots

7.14 Add Windows Client in Domain


Windows Client Domain
Windows Client Domain Request from User
Create Ticket for Windows Client Domain Installation
System Administrator Installs Windows Client Domain based on approval
Update Records on Windows Client Domain Installation
End Process

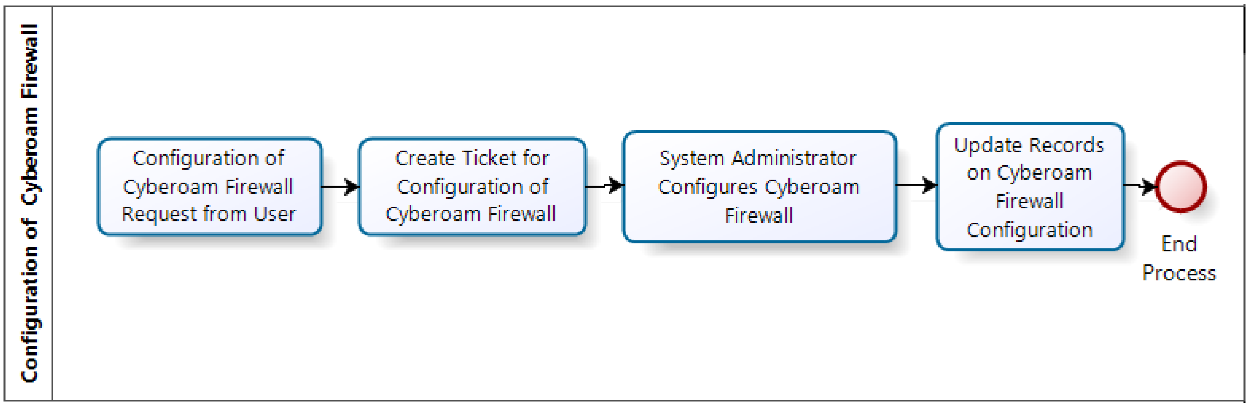
- Receive Request from Users for Windows Client Domain Installation
- IT Team creates ticket for Windows Client Domain installation based on the approval
- IT Team installs Windows Client Domain for requested User and update records
- Refer IT Manual for screenshots

7.15 Lync Installation


Lync Installation
Lync Installation Request from User
Create Ticket for Lync Installation
System Administrator Installs Lync based on approval
Update Records on Lync Installation
End Process

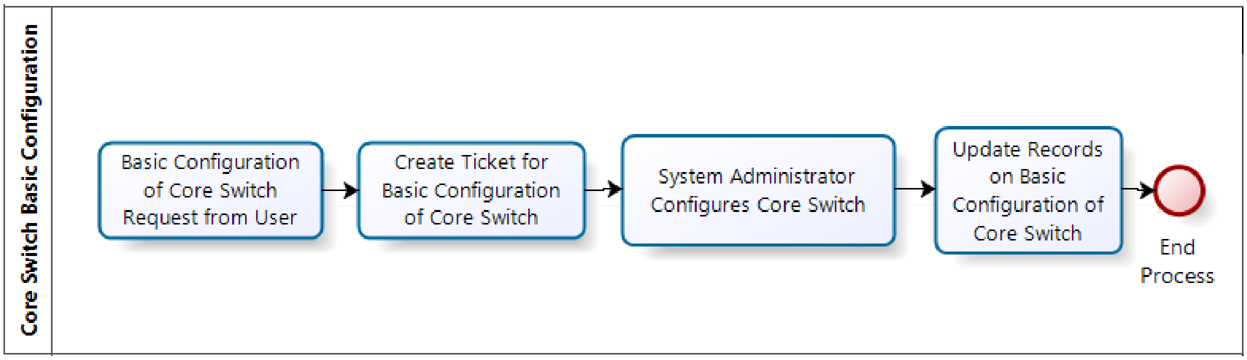
- Receive Request from Users for Lync Installation
- IT Team creates ticket for Lync installation based on the approval
- IT Team installs Lync for requested User and update records
- Refer IT Manual for screenshots

7.16 Configuration of Cyberoam Firewall


Configuration of Cyberoam Firewall
Configuration of Cyberoam Firewall Request from User
Create Ticket for Configuration of Cyberoam Firewall
System Administrator Configures Cyberoam Firewall
Update Records on Cyberoam Firewall Configuration
End Process

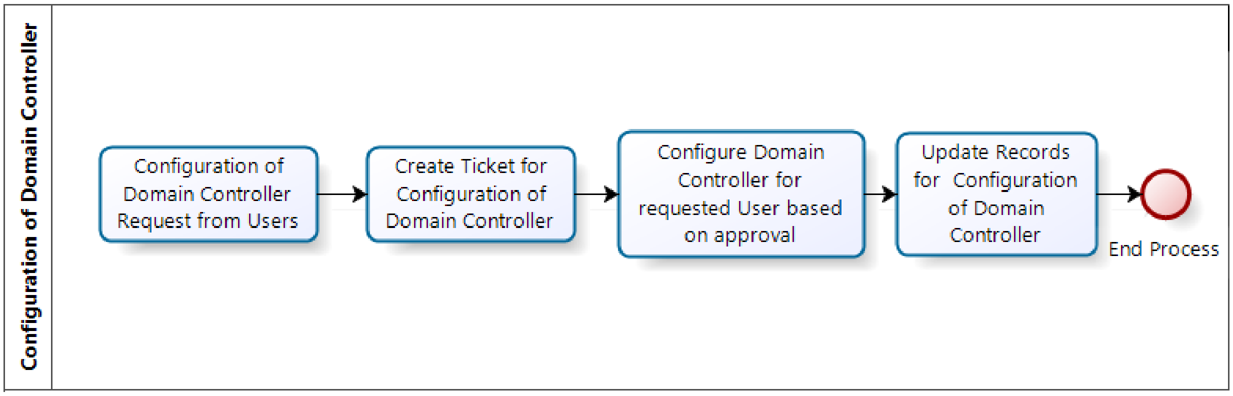
- Receive Request from Users for Configuration of Cyberoam Firewall
- IT Team creates ticket for Configuration of Cyberoam Firewall based on the approval
- IT Team Configures of Cyberoam Firewall for requested User and update records
- Refer IT Manual for screenshots

7.17 Core switch basic configuration


Core Switch Basic Configuration
Basic Configuration of Core Switch Request from User
Create Ticket for Basic Configuration of Core Switch
System Administrator Configures Core Switch
Update Records on Basic Configuration of Core Switch
End Process

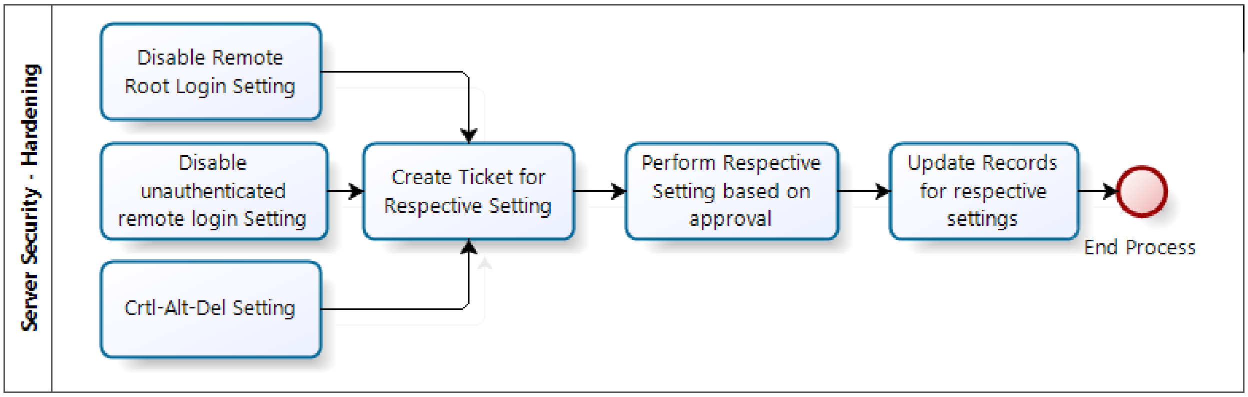
- Receive Request from Users for Core Switch Basic Configuration
- IT Team creates ticket for Basic Configuration of Core Switch based on the approval
- IT Team Configures of Core Switch for requested User and update records
- Refer IT Manual for screenshots

7.18 Configuration of Domain Controller


Configuration of Domain Controller
Configuration of Domain Controller Request from Users
Create Ticket for Configuration of Domain Controller
Configure Domain Controller for requested User based on approval
Update Records for Configuration of Domain Controller
End Process

- Receive Request from Users for Configuration of Domain Controller
- IT Team creates ticket for Configuration of Domain Controller based on the approval
- IT Team Configures of Domain Controller for requested User and update records
- Refer IT Manual for screenshots

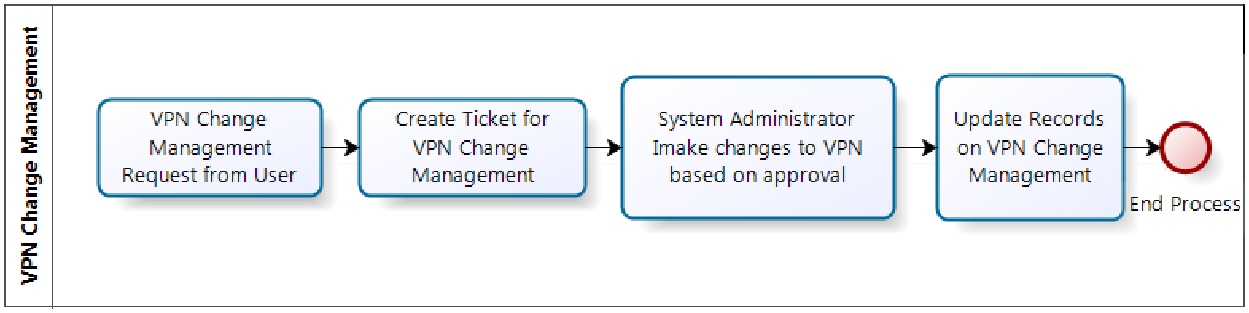
7.19 Server Security – Hardening


Server Security - Hardening
Disable Remote Root Login Setting
Disable unauthenticated remote login Setting
Crtl-Alt-Del Setting
Create Ticket for Respective Setting
Perform Respective Setting based on approval
Update Records for respective settings
End Process

- Receive Request from Users for specific purpose.
- IT Team sets the details as per request
- Hardening document is attached.

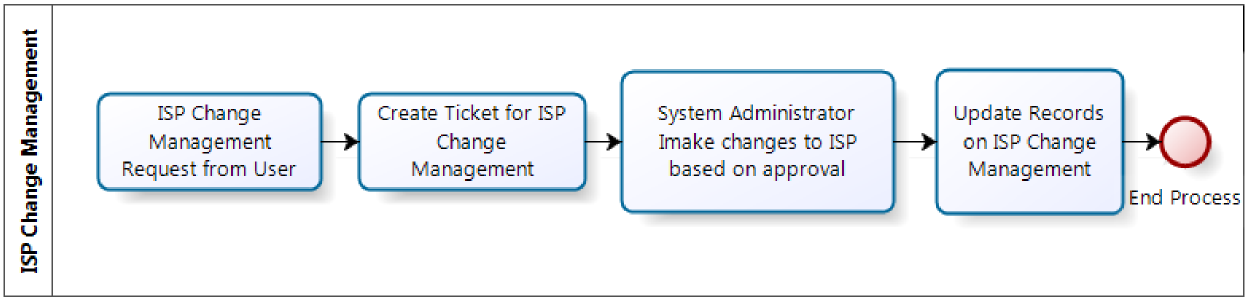
Hardening Script.pdf

7.20 VPN Change Management Process


VPN Change Management
VPN Change Management Request from User
Create Ticket for VPN Change Management
System Administrator Imake changes to VPN based on approval
Update Records on VPN Change Management
End Process

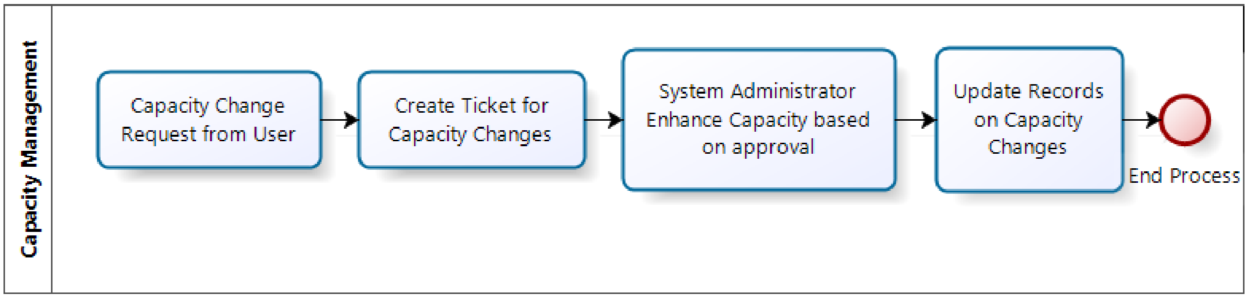
- Receive Request from Users for VPN Change Management Process
- IT Team creates ticket for VPN Change Management Process based on the approval
- IT Team make changes for VPN for requested User and update records
- Refer IT Manual for screenshots

7.21 ISP Change Management Process


ISP Change Management
ISP Change Management Request from User
Create Ticket for ISP Change Management
System Administrator Imake changes to ISP based on approval
Update Records on ISP Change Management
End Process

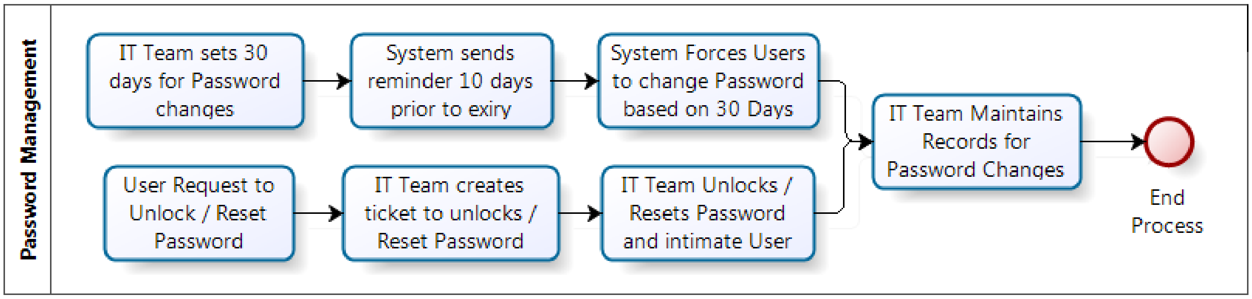
- Receive Request from Users for ISP Change Management Process
- IT Team creates ticket for ISP Change Management Process based on the approval
- IT Team make changes for ISP for requested User and update records
- Refer IT Manual for screenshots

7.22 Capacity Change Management Process


Capacity Management
Capacity Change Request from User
Create Ticket for Capacity Changes
System Administrator Enhance Capacity based on approval
Update Records on Capacity Changes
End Process

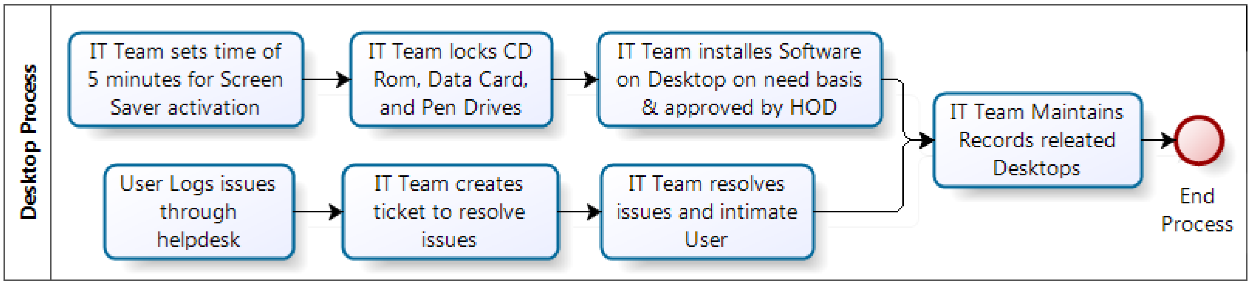
- Receive Request from Users for Capacity Changes
- IT Team creates ticket for Capacity Changes based on the approval
- IT Team make changes for Capacity Changes for requested User and update records
- Refer IT Manual for screenshots
- Capacity Planning is done on yearly basis and details are maintained

7.23 Password Management Process


Password Management
IT Team sets 30 days for Password changes
System sends reminder 10 days prior to exiry
System Forces Users to change Password based on 30 Days
User Request to Unlock / Reset Password
IT Team creates ticket to unlocks / Reset Password
IT Team Unlocks / Resets Password and intimate User
IT Team Maintains Records for Password Changes
End Process

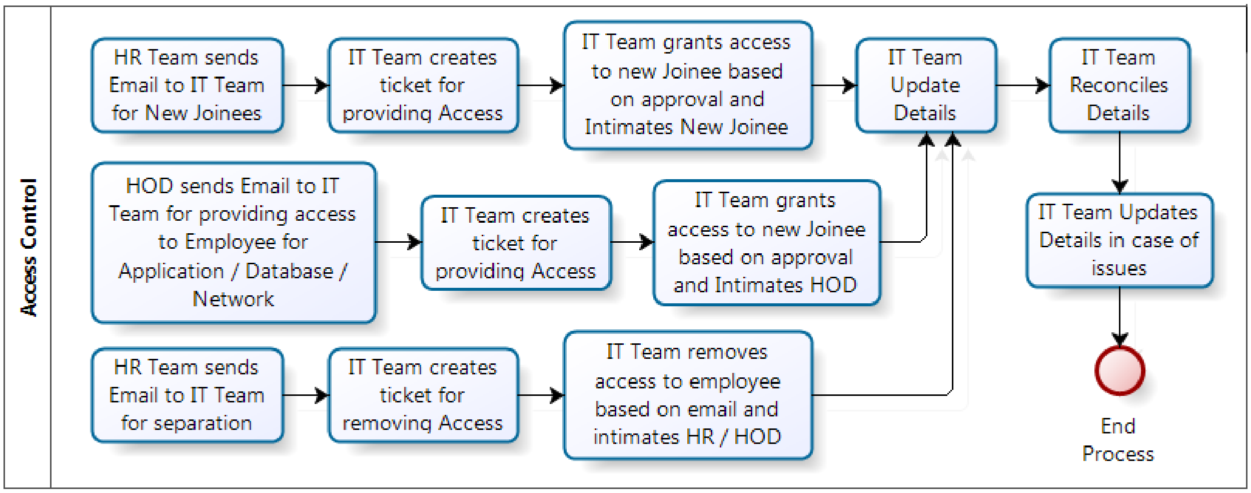
- All access to end-user in the form of application login and System login will have Password provided as a first level of security.
- All Servers at the Administrator level will have password provided as a first level of security.
- The end-user will maintain passwords as per the guidelines.
- All server level passwords will be created and maintained by the IT Administrator as per SOP.
- All server level passwords will remain with IT Administrators and one copy of the same will be provided to the IT Head in a sealed envelope.
- In case of the non-availability of IT Team, the passwords can be obtained through IT Head.
- All passwords will have to be changed once in a month with minimum password strength of 9 characters.
- Individual user will have intimation 10 days prior to change password.
- In case the passwords are shared in emergency, the responsible person should ensure the password is changed immediately.
- Individual's failing to change password, will lose the right to access the data after the specified period.
- At the server level the pop in of intimation to change password will appear at the end of every 30 days.
- Super Admin password, server passwords and domain passwords policy will remain the same as applicable as per group policy which is 30 days
- Password age is 30 days
- Password remembered is last 3
- User send request for Unlock / Reset password to IT Team
- IT Team creates ticket for Unlock / Reset password based on approval
- IT Team Unlocks/Resets password and intimate the User
- IT Team maintains the records of Password changes
- This policy is applicable for servers, network devices and workstations.

7.24 Desktop Process


Desktop Process
IT Team sets time of 5 minutes for Screen Saver activation
IT Team locks CD Rom, Data Card, and Pen Drives
IT Team installes Software on Desktop on need basis & approved by HOD
User Logs issues through helpdesk
IT Team creates ticket to resolve issues
IT Team resolves issues and intimate User
IT Team Maintains Records releated Desktops
End Process

- Ensure that user should change their password, in case the same is shared with another user in case of emergency.
- IT Administrator to ensure that the desktop password is changed monthly.
- When the user leaves his desk, the automatic screen saver password configuration should lock the personal computer after 5 minutes.
- The user should not access any external devices like CD Rom, Data Card, and Pen Drives etc. without the prior permission of the Functional Manager. This is to prevent virus attacks and data theft.
- The Screen Saver password will automatically appear on the screen if the desktop is not in use for more than 5 minutes.
- User should adhere to the specified (as per the policy) email template/settings to ensure standardization across the organization
- All the software's / versions on the desktops should be as per the standards / SOPs.
- Any Specific software installation on personal computer will have to be approved by Functional Manager and verified by IT Head.
- User send request for any issues related to Desktop to IT Team through helpdesk
- IT Team creates ticket to resolve issues related to Desktop
- IT Team resolves issues related to Desktop and intimate the User
- IT Team maintains the records of Desktop Issues

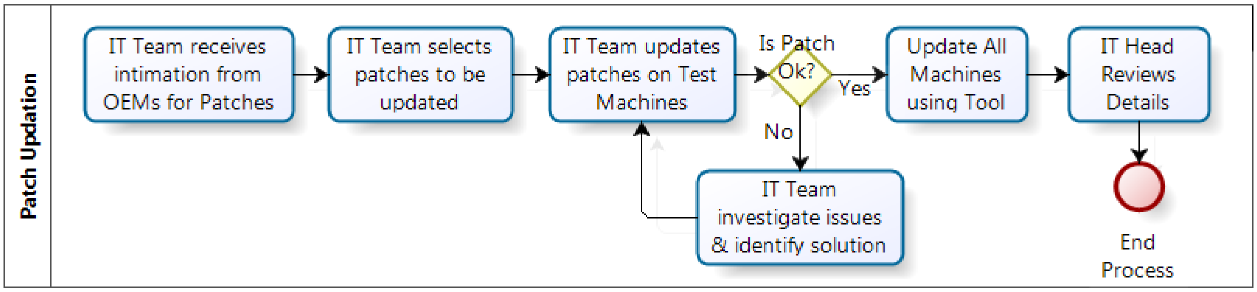
7.25 Access Control


Access Control
HR Team sends Email to IT Team for New Joinees
IT Team creates ticket for providing Access
IT Team grants access to new Joinee based on approval and Intimates New Joinee
IT Team Update Details
IT Team Reconciles Details
HOD sends Email to IT Team for providing access to Employee for Application / Database / Network
IT Team creates ticket for providing Access
IT Team grants access to new Joinee based on approval and Intimates HOD
IT Team Updates Details in case of issues
HR Team sends Email to IT Team for separation
IT Team creates ticket for removing Access
IT Team removes access to employee based on email and intimates HR / HOD
End Process

- IT Team creates Standard user profiles for user and policy management.
- User Registration and De-Registration at all levels will be defined and monitored as per the set SOP.
- All Privileges are granted to users as per the defined roles and responsibility and the same will be listed in the SOP.

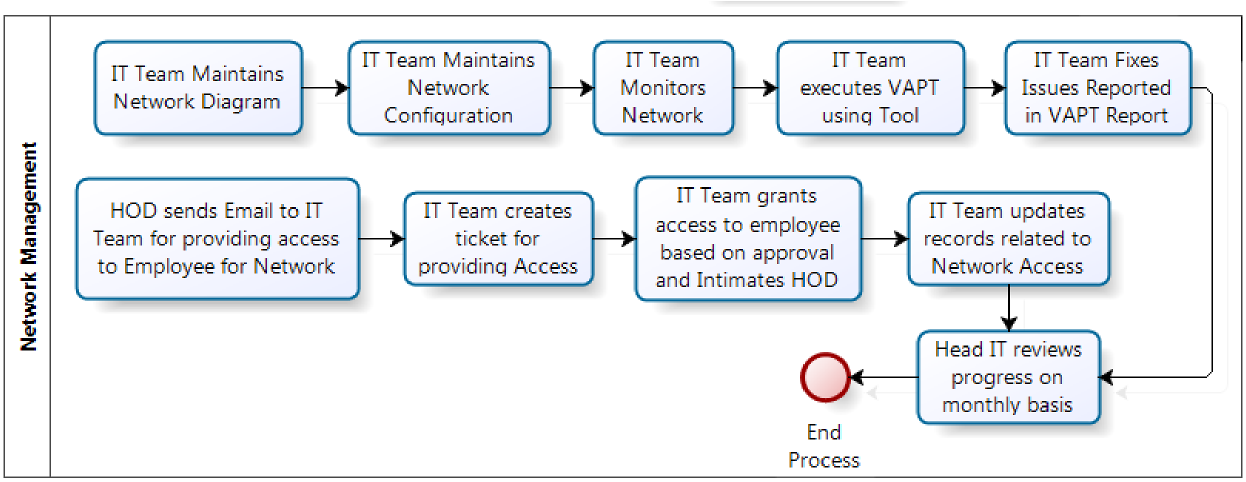
- Network Access controls will be set and monitored by each location System Administrator as per the SOP.
- This is applicable to LAN as well as Wireless Access
- The area of IT infrastructure especially the access to the Server Room is restricted.
- Anyone including the Vendor representative who wants to go to the server room should have necessary written approval from the IT Manager and should be accompanied by an IT Administrator.
- The details of persons entering the Server room should be entered in the register, which is maintained for the same. The information contained in the register should include name, reasons, time in, time out and necessary approval details.
- Person entering the Server Room should not carry media where data / image can be transferred for example – pen drive, Laptop, floppy, CDs, etc. without prior written approval from IT - Manager.
- The maintenance of the server room as to the upkeep will be as per the SOP laid down for this purpose.
- HR Team sends email for New Joinees for creation of User Access
- IT Team creates ticket to create access to New Joinees
- IT Team provides access to respective server and intimate User
- Head of Department sends email for employees to give / alter access to respective Applications / Server / Network / Database based on the requirement
- IT Team creates ticket to provide / alter access to employees
- IT Team provides / alters access to respective employee and intimate Employee / Head of Department
- HR Team sends email for separation of employee
- IT Team creates ticket to remove access of employee
- IT Team removes access of employee and intimate HR Team
- IT Team maintains the details of Administrator Access separately
- IT Team changes the Password in case de-registration of any Administrator
- IT Team reviews / reconciles of all activities related to providing / removing access to employee on monthly basis
- IT Team updates the details in case of any disturbances

7.26 Patch Management


Patch Updation
IT Team receives intimation from OEMs for Patches
IT Team selects patches to be updated
IT Team updates patches on Test Machines
Is Patch Ok?
Yes
No
Update All Machines using Tool
IT Head Reviews Details
IT Team investigate issues & identify solution
End Process

- Servers: All critical Infrastructures to be patched based on severity on quarterly basis.
- These calls be patched offline or via a patch management server.
- Workstations to be classified as back office and development machines.
- All back-office workstations to be patched based on severity
- All development workstation to be patched after taking relevant approvals from the department manager as this could affect the training environment
- IT Team receives intimation from OEMS for patch updates
- IT Team identifies which patches to be updated
- IT Team updates patches on test machine in test environment and maintains details
- IT Team updates patches on all machines based on the result of Test Environment using Patch updation tool
- IT Team maintains records of all patch updation
- IT Head reviews status of Patch updation on monthly basis

7.27 Network Management


Network Management
IT Team Maintains Network Diagram
IT Team Maintains Network Configuration
IT Team Monitors Network
IT Team executes VAPT using Tool
IT Team Fixes Issues Reported in VAPT Report
HOD sends Email to IT Team for providing access to Employee for Network
IT Team creates ticket for providing Access
IT Team grants access to employee based on approval and Intimates HOD
IT Team updates records related to Network Access
Head IT reviews progress on monthly basis
End Process

- Configuration of network related devices should be as per the SOP.
- Basic firewall rules need to be implemented
- TCP/IP protocols should be standardized as per location
- IP forwarding should be done only with prior approval of IT Manager
- Network diagram of entire organization including local and remote site should be in place.
- Any changes to network diagram should have prior approval of IT Manager / IT Head
- Updated Network diagram should be available with IT team
- External network connections should be as per SOP.
- VA should be done after office hours or off time.
- VA tools should be kept in secure place and should be used only after management approval.
- VA should be conducted once a year between Oct – Dec quarter cycle and reports to be prepared for the same
- VA shall include the scope, objective and conclusion summary with detailed IP scope in the report
- The VA report shall have vulnerability representation against each IP
- Firewall Assessment to be conducted once a year between Oct – Dec quarter cycle and reports to be prepared for the same
- Head of Department sends email to IT Team for employees to give / alter access to Network based on the requirement
- IT Team creates ticket to provide / alter access to employees
- IT Team provides / alters access to respective employee and intimate Employee / Head of Department
- IT Team maintains details of the updating of Network Access in the Network Diagram.
- Network Password to be changed once in every 30 days.
- Backup to be taken as per backup policy and firewall configuration backup can be maintained on emails.

7.28 Cryptography Procedure

- CIPL shall implement cryptographic controls supporting legislative, contractual, statutory and business requirements, only if deemed necessary.
- Compliance with Legal Requirements shall also be established.
- Data shall be transferred on the media using proper encryption which is to be sent to other locations.
- Proper precaution shall be taken during transit.
- Details shall be maintained for transfer on media.

7.29 Key Management / Generation

- Product team shall generate keys for the products for installation.
- These keys shall be shared only with concerned members for installation

8. Quality Mechanisms

- Monthly Review Report
- Access Control Logs
- VA Report Review
- Patch Review Report
- Critical Incident Report Review
- Change Management Register Review
- Backup Report Review

9. Quality Objectives

Sr. No	*Objectives*	*Responsibility*	*Frequency of Measurement*	*Reporting of Measurement*	*Target to Achieve*
1	Email Services Availability	IT Head	Monthly	Uptime Monthly Report	98%
2	Internet Services Availability	IT Head	Monthly	Uptime Monthly Report	98%
3	Access Control Logs Review	IT Head	Monthly	Security Logs Report	100%
4	VA to be conducted yearly	IT Head	Yearly	VA Report	100%
5	Backup of Information	IT Head	Daily / Weekly / Monthly	Backup Report	100%
6	Critical Incident Report	IT Head	Monthly	Incident Report	98%
7	Change Management Report	IT Head	Monthly	Change Management Register	98%

10. Identified Risk

- All risks identified for the process will be recorded into the Risk Management Plan (RMP)
- Risks will be reviewed and monitored as per the agreed schedule

11. Exit Criteria

Outputs
• Daily Monitoring Report • Email Request • Email Request for Closing / Locking / Forward Emails • Service Level Matrix for Issues • Service Level Issues Closing Report • Software Installation Request • Master List of Softwares • Anti-Virus Software Request – Desktop / Laptop / Server • Windows Hardening Document • Backup / Restoration Request • Printer Configuration Request

Outputs
• Datacard Installation Request
• Outlook Configuration Request
• Windows Client Addition in Domain Request
• Lync Installation Request
• Cyberoam Firewall Configuration Request
• Core Switch Basic Configuration Request
• Domain Controller Configuration Request
• VPN Change Management Request
• ISP Change Management Request
• Capacity Change Management Request
• Unlock / Reset Password Request
• Desktop / Laptop Issue Request
• HR Email for Creation of new employee and giving Access
• Head of Department Email for granting access to employee for Application / Database / Network / System
• HR Email for separation of employee for removing Access
• Patch Intimation from OEM
• Manual Patch Updation
• Patch Testing Details
• Patch Review Sheet
• Network Access / Alter Request
• VA Report
• Change Request Form
• Change Request Register