

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	02-Nov-2020	QMF	06-Nov-2020	10-Nov-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 Review	-
3.0	All	02-Nov-2020	Annual Review	-

Table of Contents

1.	Objectives	3
2.	Scope	3
3.	Policy	3
3.1	Policy Statement	3
3.2	Framework to Support or Implement this Policy.....	3
4.	References to (checklists, forms, guidelines, lists, standards, templates, other processes).....	3
5.	Entry Criteria.....	5
6.	Responsibilities.....	6
7.	Process Description	6
7.1	Daily Monitoring	7
7.2	Email ID Creation	9
7.3	Email ID Closing / Locked / forward.....	9
7.4	Internet Procedure	9
7.5	Response Time Matrix.....	11
7.6	List of IT Tag Assets	12
7.7	Employee Eligibility list.....	13
7.8	Software Installations	13
7.9	Anti-Virus Software installation.....	16
7.10	Operating System Hardening	16
7.11	Backup Restoration	17
7.12	Printer Configuration	17
7.13	Datacard Installation	18
7.14	Microsoft Outlook Configuration	19
7.15	Add Windows Client in Domain	19
7.16	Lync Installation	19
7.17	Configuration of Cyberoam Firewall	20
7.18	Core switch basic configuration.....	20
7.19	Configuration of Domain Controller.....	20
7.20	Server Security – Hardening	21
7.21	VPN Change Management Process.....	21
7.22	ISP Change Management Process	21
7.23	Capacity Change Management Process.....	22
7.24	Password Management Process.....	22
7.25	Desktop Process	23
7.26	Access Control.....	23
7.27	Patch Management	25
7.28	Network Management.....	25
7.29	Network Time Synchronization	26
7.30	Cryptography Procedure	26
7.31	Key Management / Generation	26
8.	Quality Mechanisms.....	26
9.	Quality Objectives	26
10.	Identified Risk	27
11.	Exit Criteria	27

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

Process Element	Description	ID
	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
	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 & PT 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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

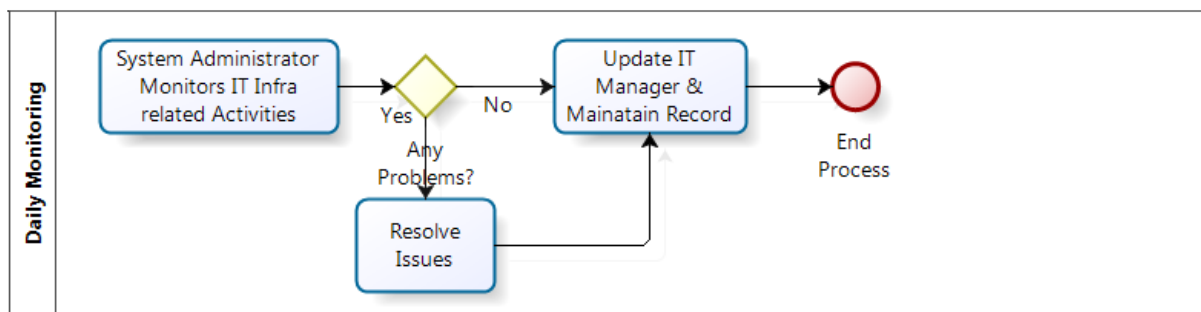
- Employee Eligibility Table
- Software Installation
- Anti-virus Installation
- Operating System Hardening
- Backup Restoration
- Printer Configuration on Windows
- Data Card Installation
- Microsoft Outlook Configuration
- Linux Evolution Configuration
- Add Windows Client in Domain
- Add Linux Client 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



- 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.

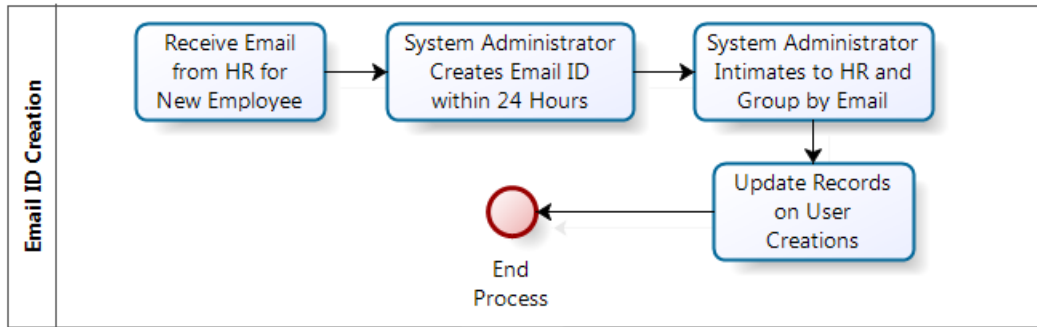
- System Administrator will provide Daily Monitoring Report mail every morning after doing a health check of servers and also confirming all the application are working fine.

Helpdesk Category	Committed Time (in Hours)	Priority
Hardware Troubleshooting	4	High
Email Account Administration	4	High
Network Configuration / Troubleshooting	4	High
OS Configuration / Troubleshooting	4	High
Printer Configuration / Troubleshooting	4	High
Server Configuration / Troubleshooting	4	High
Application configuration / Troubleshooting	6	Medium
Miscellaneous	6	Medium
Software Installation / Troubleshooting	6	Medium
Email configuration / Troubleshooting	24	Low
Asset Installation	48	Medium

Daily monitoring format

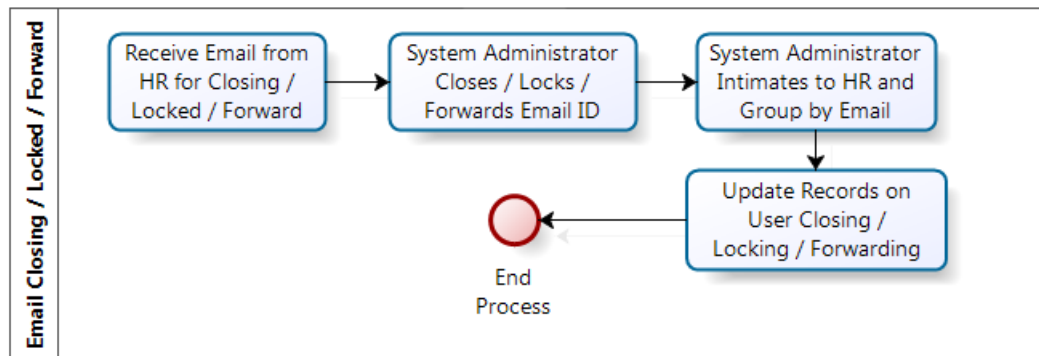
Sr. No.	Daily Activity	Activity Description	Standard Time
1	Backup Server	Data Backup	30
		Service Check	10
		Space Utilization	10
		Log Check	15
		Connectivity Check	5
2	Firewall	Service Check	10
		Space Utilization	10
		Log Check	15
		Connectivity Check	5
3	Antivirus (VMWARE)	Service Check	10
		Space 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



- 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



- 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 Internet Procedure

7.4.1 Applicability

These procedures are applicable to:

- All systems and services provided or owned by CIPL for Internet connectivity.
- All Users of the CIPL's Internet services.

Where, Systems means all hardware and software systems / components used for making the Internet accessible to the employees and customers.

Services means

- Internet access provided to the employees.

User's means

- All employees, contractors, consultants, temporary users and third party employees who are authorized by the Business Owner of the CIPL to access Internet from CIPL's workstations using CIPL's network
- All other users who access CIPL's Internet site and any links provided therein or any other site launched by the CIPL.

7.4.2 Usage Controls:

All approved Internet users, who are authorized to use Internet from the CIPL's network and CIPL's network, will use the Internet through the gateway provided by CIPL and internet service provided to CIPL.

7.4.3 Procedure for Creation of User-id on CIPL Gateway in CIPL:

- Request for creation of IDs on CIPL gateway shall be given by authorized person from CIPL. The authorized person from CIPL shall seek approval for Internet access for any user working at the location under his control in user creation form format.
- Form for ID Creation in CIPL & for CIPL users is user creation form.
- On receipt of such request, IT Manager will approve/reject such request and send the same to the technology Department for further action. In case of approved request only, the technology department will enable the Internet access to such user and communicate the User-name and Password to the HR-Department head in case of CIPL gateway IDS and to the CIPL's authorized person in case of CIPL's gateway IDs.
- Technology department will make an entry in the List of Groups and User IDs maintained at the site and obtain acknowledgement from such user.

7.4.4 Access Control and content filtering:

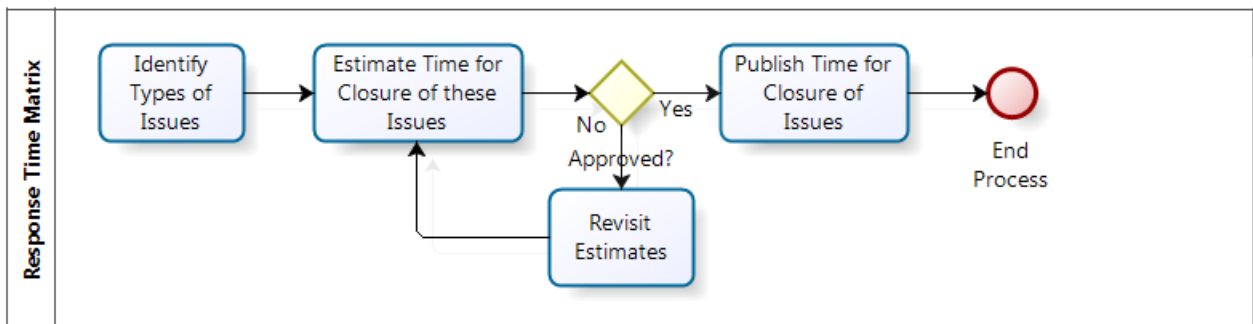
- To avoid misuse or theft of data, respective server Administrator will control over desktops which has Internet connection, as per Desktop Policy.
- Administrator should make sure that desktop connected to Internet is properly hardened, patched up with all necessary updates and should have Antivirus running on it with regular updates, as per Patch Management Policy and Anti-Virus Policy.
- Administrator should monitor Internet activities of users by periodically checking system logs and will report actual and potential security incident or non-compliance to the Helpdesk.
- The access control on the user id will be ensured as per the request.

7.4.5 Logging of Internet usage:

Code of conduct for Usage of Internet from CIPL's & CIPL's network:

- Only the users authorized by the Business owner will be allowed access to Internet from the CIPL's /CIPL's network.
- Such usage will be only for the period authorized by the Business owner.
- The Internet access will not be used for any personal purpose.
- The user will not use the Internet access for chatting, surfing unauthorized sites or communicating with individual email ids. Communication with individual email ids will be routed through Mail server of the CIPL
- Such authorized user must ensure that the desktop used for Internet access is equipped with Antivirus software and the signature file is up-to-date as mentioned in Anti-Virus Policy document.
- The user will ensure that all downloads are scanned and are free of malicious code before opening or using such files.
- Only the information authorized by the Business Owner will be disclosed through the Internet.
- The user will change the password as per the Password Policy.
- All authorized users will be given access after taking authorized signature of IT Manager in the user lists.
- IT Manager will hand over a document stating the permission of the usage, allowed sites and timing of usage to the authorized user at the time of granting Internet access to the authorized user.

7.5 Response Time Matrix

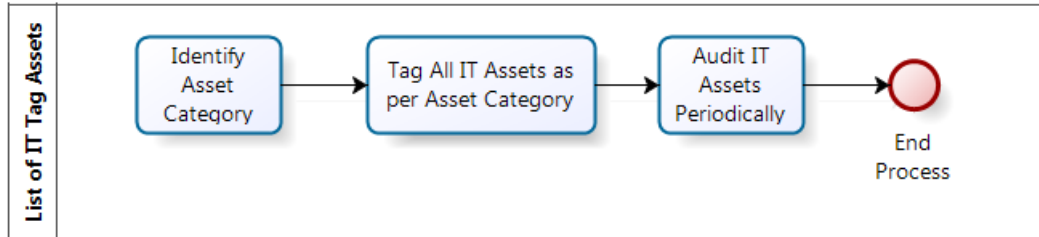


- As per the Helpdesk process, we commit a response time to every ticket. The following are the various types of the issues and the corresponding are the response time. The IT infra team will work hard to ensure that all issues is responded within the committed response time.
- Refer IT Manual for screenshots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

7.6 List of IT Tag Assets



- 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

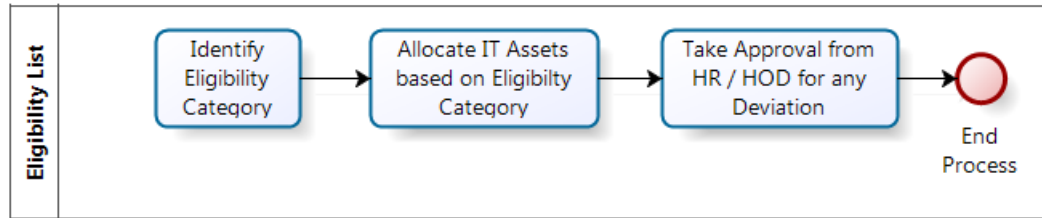
IT asset tag category

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 :	

7.7 Employee Eligibility list

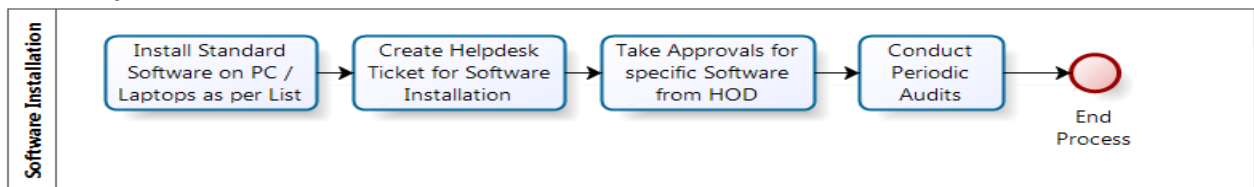


- All allotment of IT asset to employee's should be done in line with the below mentioned eligibility.
- In case of deviation, the same should be communicated by the HR or Functional Manager
- Refer IT Manual for screenshots

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

7.8 Software Installations



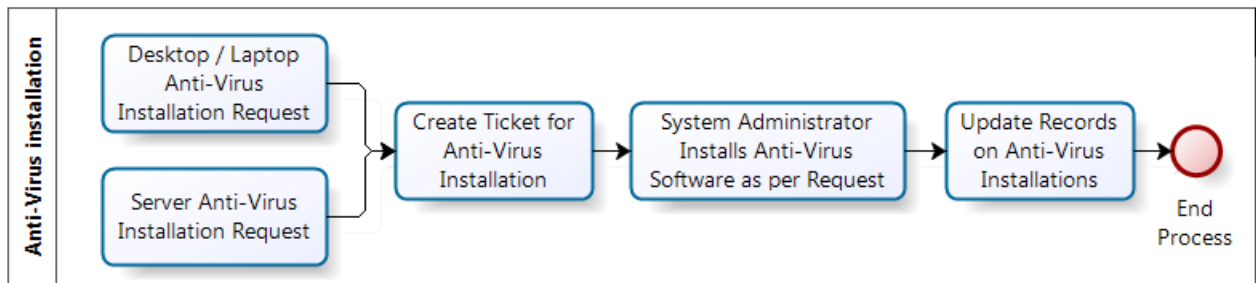
All software installation should be done as per the instructions given below.

- 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 joiners 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	Professional	Standard		
2	MS Office	2010	Professional	Standard		
3	MS Office	2012	Professional	Standard		
4	MS Office	2013	Professional	Standard	365 Pro	
5	MS Office	2016	Professional	Standard	365 Pro	
6	MS Visio	2003	Professional	Standard		
7	MS Visio	2010	Professional	Standard		
8	MS Visio	2016	Professional	Standard		
9	MS Project	2003	Professional	Standard		
10	MS Project	2010	Professional	Standard		
11	MS Project	2016	Professional	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 Certificates for the below					
40	https://cloverinfotech.co.in/Pay/Logon.aspx				Feb-17	Geo Trust
41	https://connect.cloverinfotech.in/adrenaline/				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					

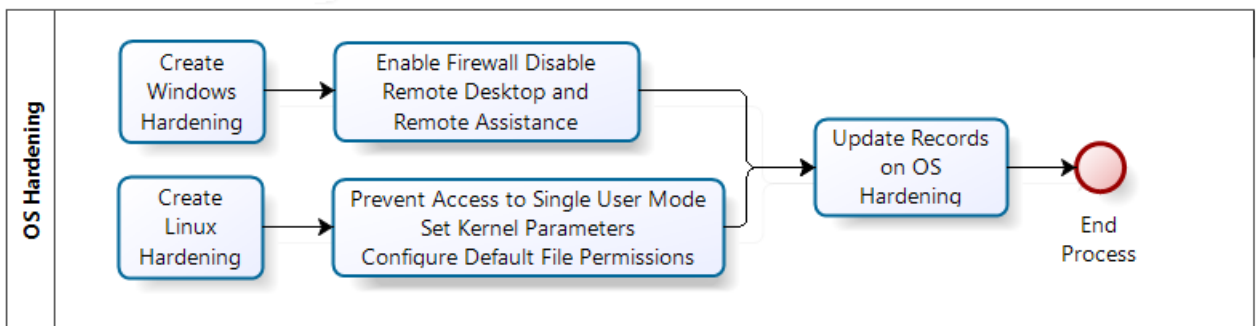
7.9 Anti-Virus Software installation



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

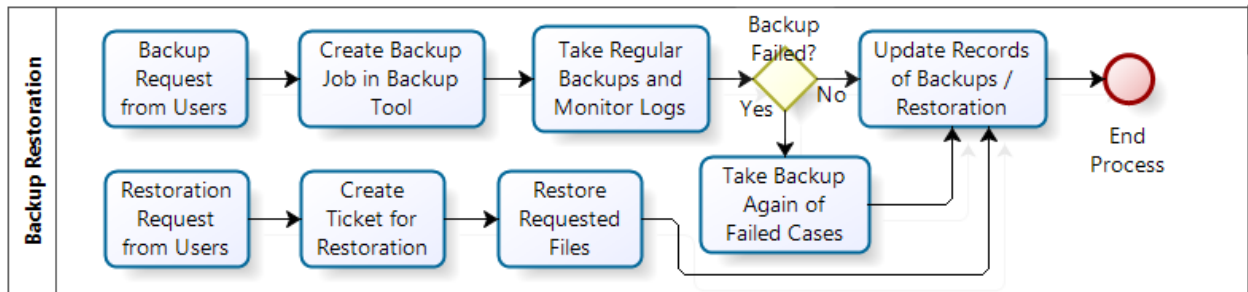
- Anti-Virus Software should be installed on all Desktops / Laptops
- Anti-Virus Software should be installed on all Servers
- All requests for Software installation will be executed as a part of Helpdesk ticket number
- Update all records related to installation of Anti-Virus
- Download daily signatures 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

7.10 Operating System Hardening



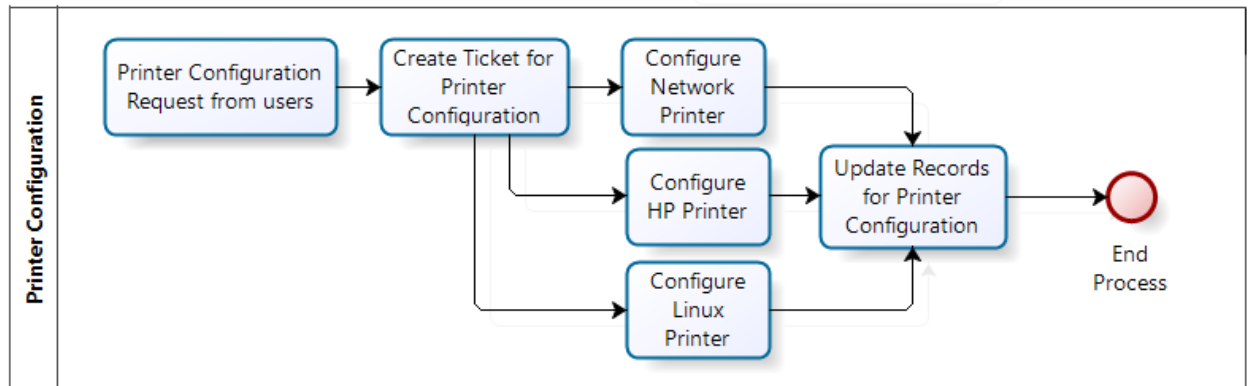
- Create Hardening Document for Windows Operating System with following parameters:
 - Enable Firewall Disable
 - Remote Desktop and Remote Assistance
- Create Hardening Document for Linux Operating System with following parameters:
 - Prevent Access to Single User mode
 - Set Kernel Parameters
 - Configure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

7.11 Backup Restoration



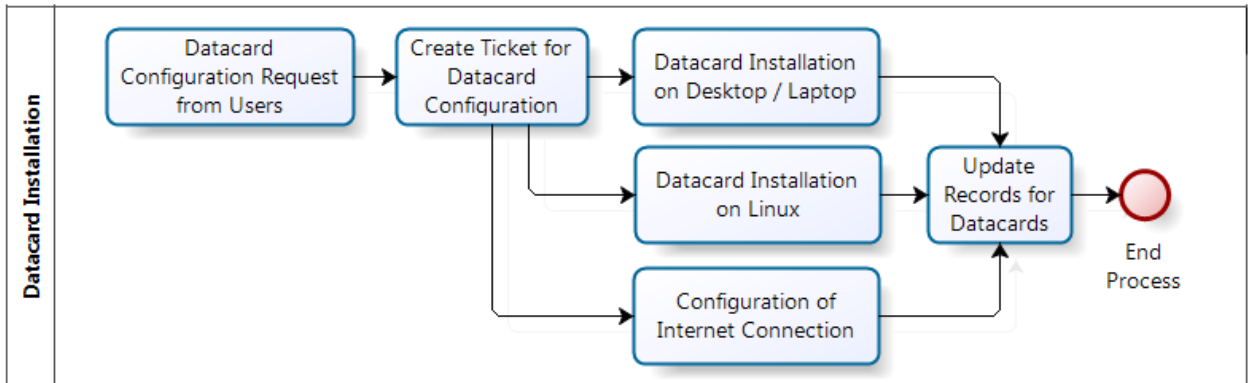
- Receive Request from Users for backup of files / folders
- IT Team creates batch job in Backup Tool
- IT Team takes regular backups based on the time defined
- IT Team checks logs of backups
- IT Team takes backup of failed cases again and updates backup records
- Receive Request from Users for restoration of file / folder
- IT Team creates ticket for restoration
- 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

7.12 Printer Configuration



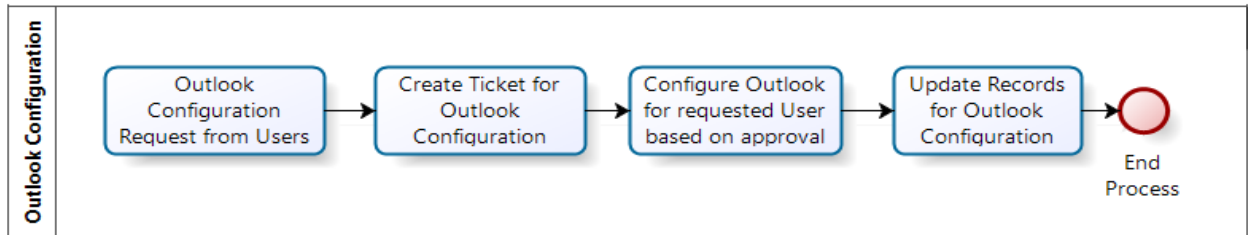
- Receive Request from Users for Printer Configuration for Network / HP / Linux Printer
- IT Team creates ticket for Printer Configuration based on the approval
- IT Team configures the requested printer and update records
- Refer IT Manual for screenshots

7.13 Datacard Installation



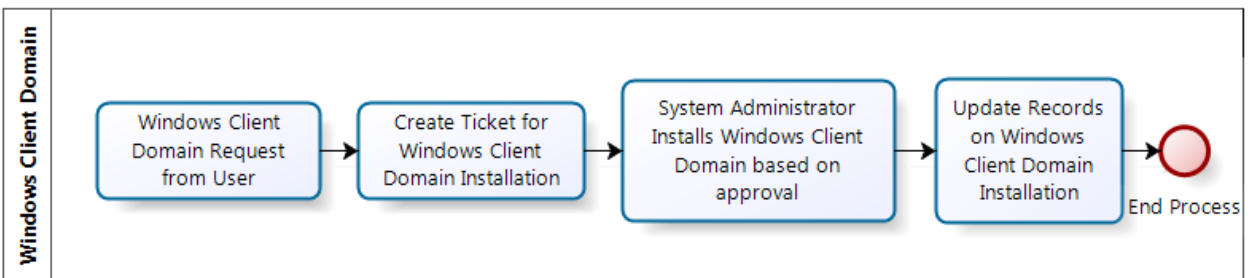
- Receive Request from Users for Datacard installation for Desktop / Laptop / Linux / Internet Connection
- IT Team creates ticket for Datacard installation based on the approval
- IT Team configures the requested Datacard and update records
- Refer IT Manual for screenshots

7.14 Microsoft Outlook Configuration



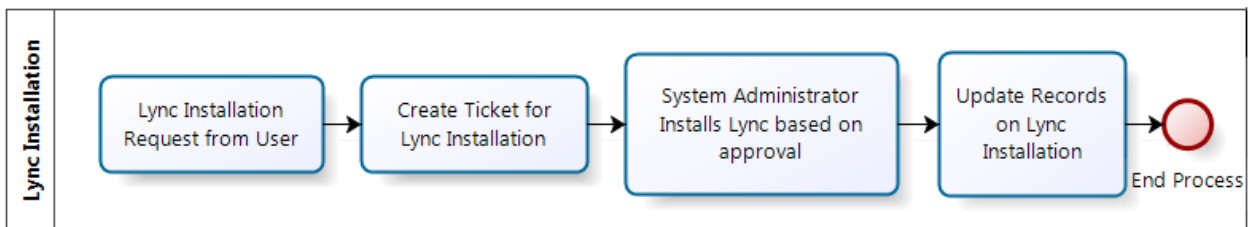
- Receive Request from Users for Outlook Configuration for Desktop / Laptop
- IT Team creates ticket for Outlook Configuration based on the approval
- IT Team configures Outlook for requested User and update records
- Refer IT Manual for screenshots

7.15 Add Windows Client in Domain



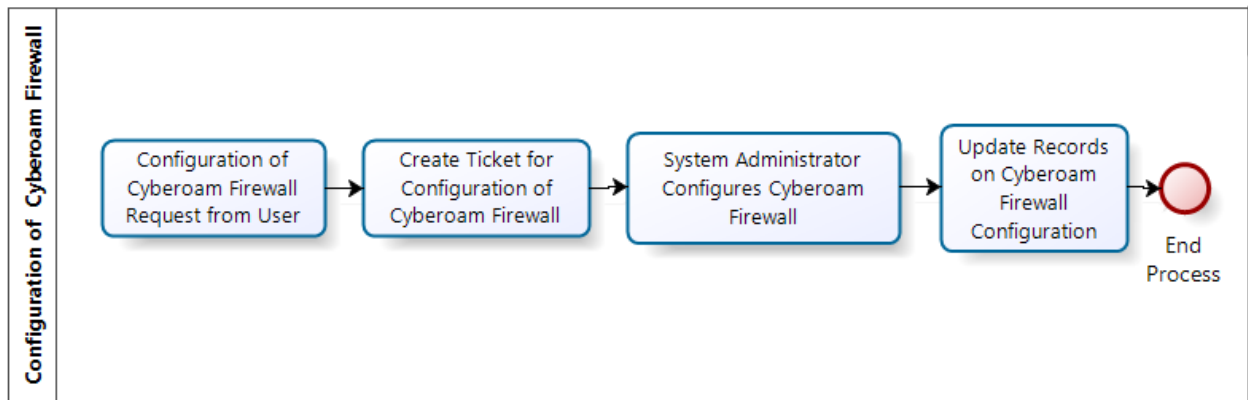
- Receive Request from Users for Windows Client Domain Installation
- IT Team creates ticket for Windows Client Domain installation based on the approval
- IT Team installs Windows Client Domain for requested User and update records
- Refer IT Manual for screenshots

7.16 Lync Installation



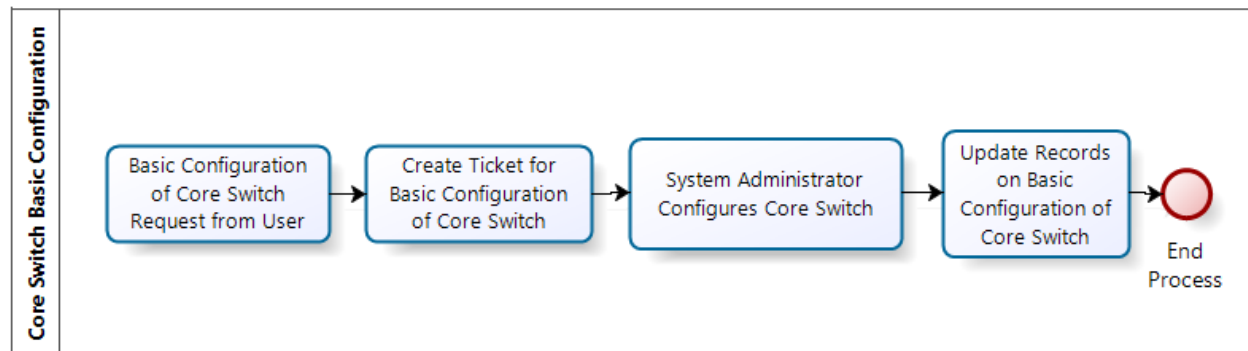
- Receive Request from Users for Lync Installation
- IT Team creates ticket for Lync installation based on the approval
- IT Team installs Lync for requested User and update records
- Refer IT Manual for screenshots

7.17 Configuration of Cyberoam Firewall



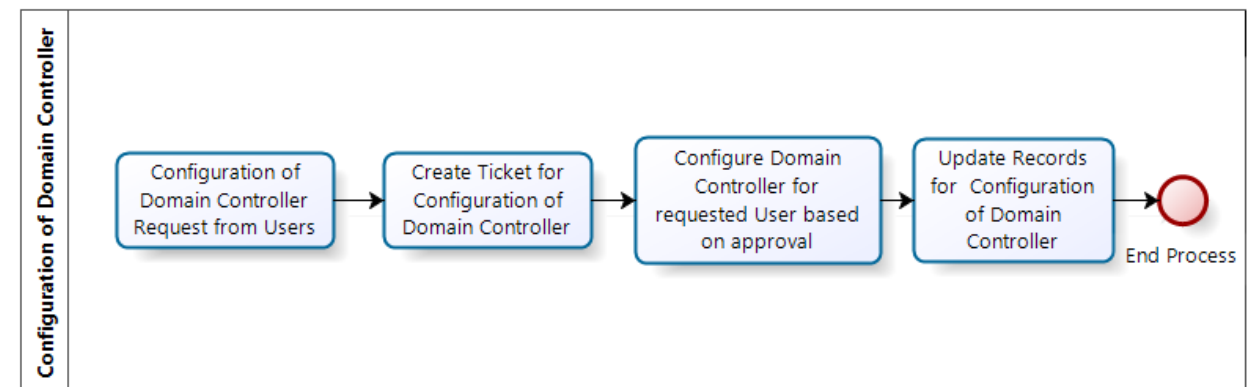
- Receive Request from Users for Configuration of Cyberoam Firewall
- IT Team creates ticket for Configuration of Cyberoam Firewall based on the approval
- IT Team Configures of Cyberoam Firewall for requested User and update records
- Refer IT Manual for screenshots

7.18 Core switch basic configuration



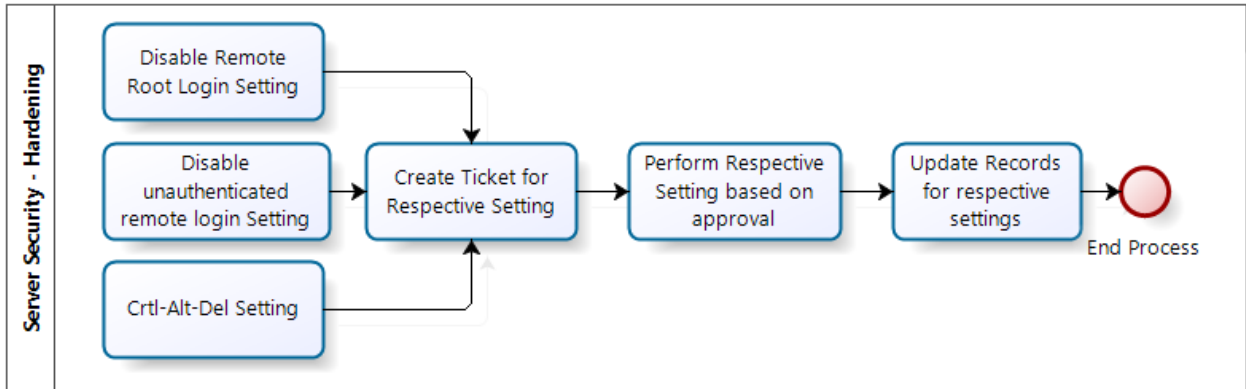
- Receive Request from Users for Core Switch Basic Configuration
- IT Team creates ticket for Basic Configuration of Core Switch based on the approval
- IT Team Configures of Core Switch for requested User and update records
- Refer IT Manual for screenshots

7.19 Configuration of Domain Controller



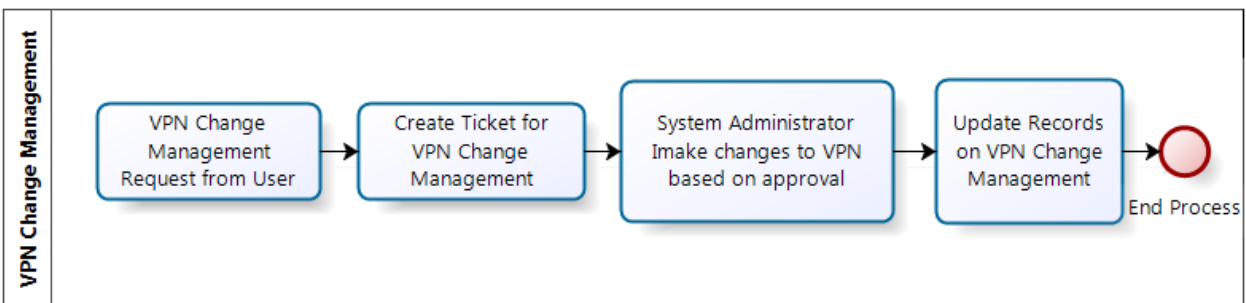
- Receive Request from Users for Configuration of Domain Controller
- IT Team creates ticket for Configuration of Domain Controller based on the approval
- IT Team Configures of Domain Controller for requested User and update records
- Refer IT Manual for screenshots

7.20 Server Security – Hardening



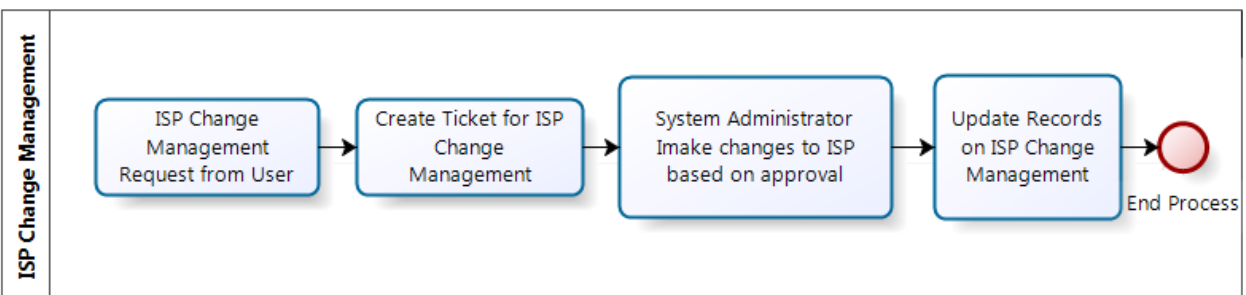
- Receive Request from Users for specific purpose.
- IT Team sets the details as per request

7.21 VPN Change Management 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

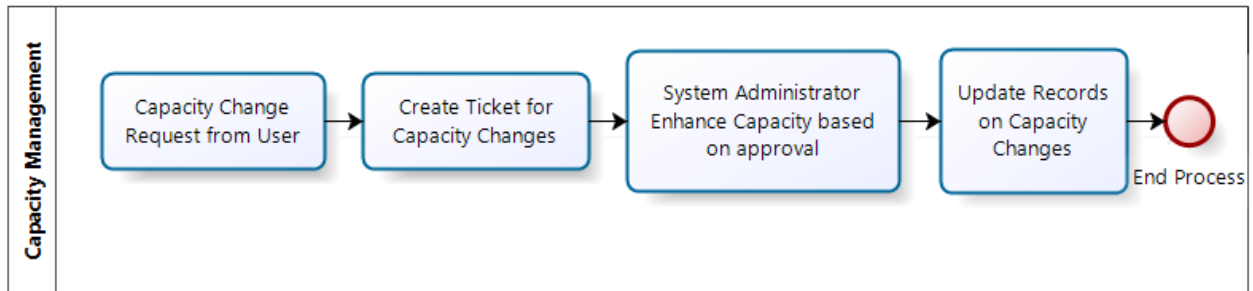
7.22 ISP Change Management Process



- Receive Request from Users for ISP Change Management Process
- IT Team creates ticket for ISP Change Management Process based on the approval

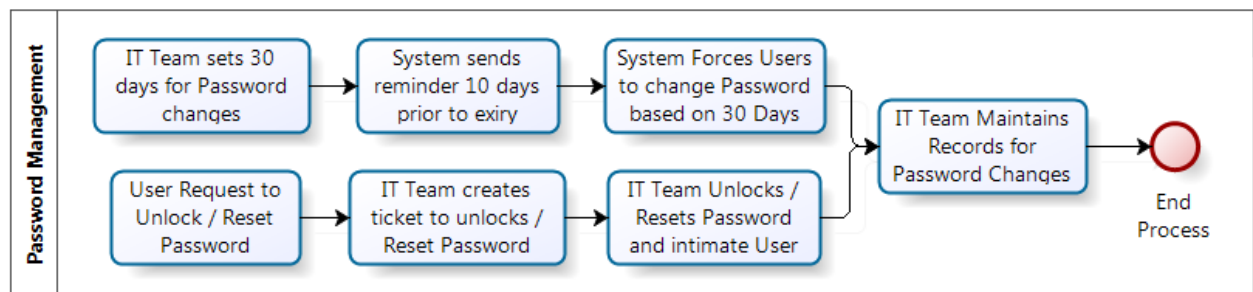
- IT Team make changes for ISP for requested User and update records
- Refer IT Manual for screenshots

7.23 Capacity Change Management 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

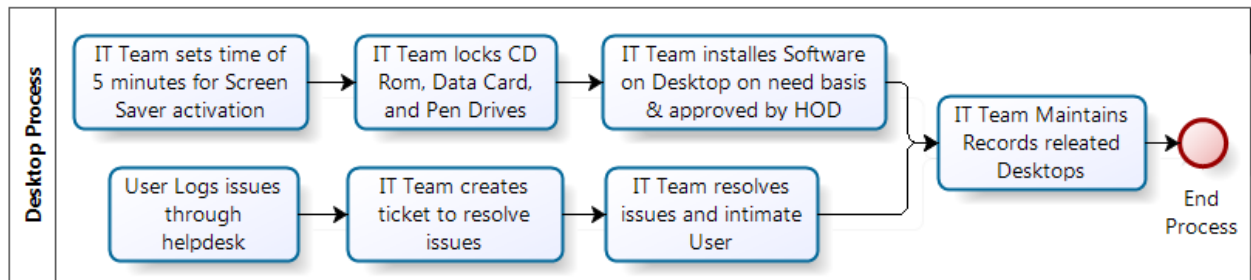
7.24 Password Management Process



- 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.

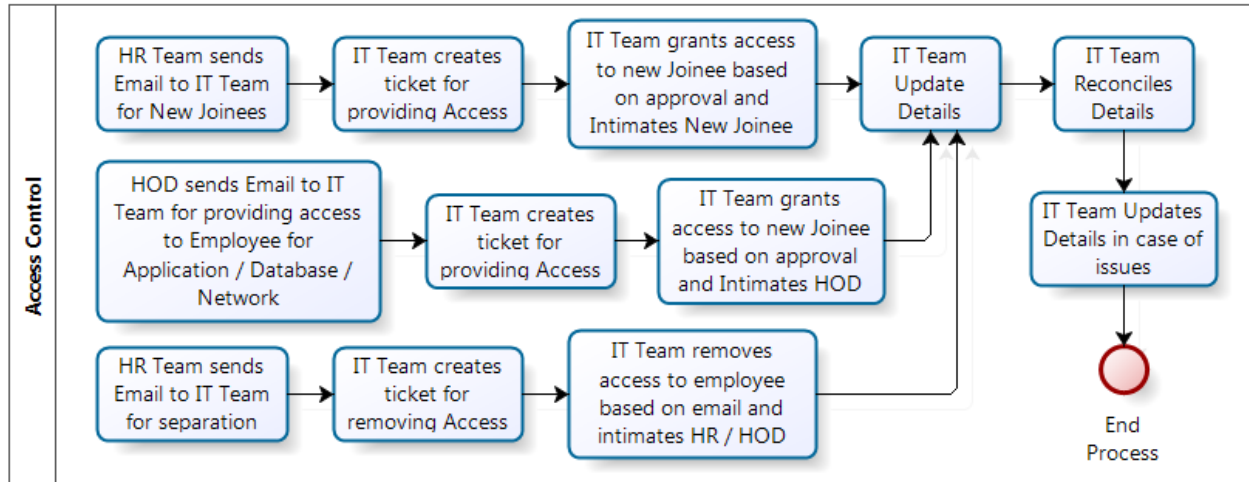
- Super Admin password, server passwords and domain passwords policy will remain the same as applicable as per group policy which is 30 days
- Password age is 30 days
- Password remembered is last 3
- User send request for Unlock / Reset password to IT Team
- IT Team creates ticket for Unlock / Reset password based on approval
- IT Team Unlocks/Resets password and intimate the User
- IT Team maintains the records of Password changes

7.25 Desktop Process



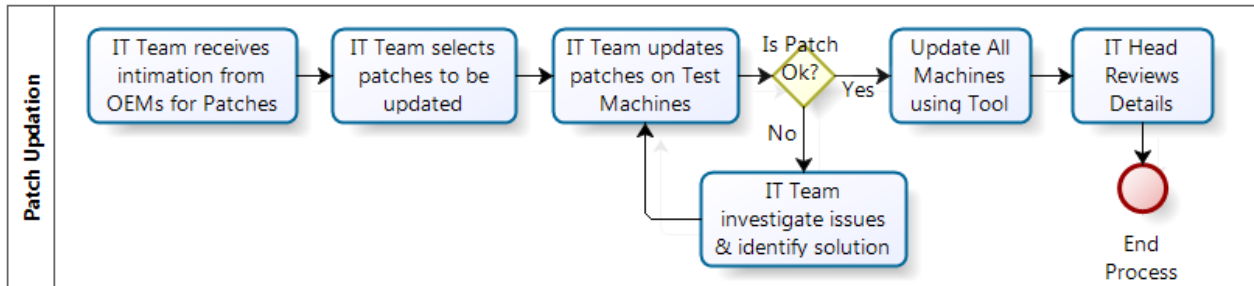
- Ensure that user should change their password, in case the same is shared with another user in case of emergency.
- IT Administrator to ensure that the desktop password is changed monthly.
- When the user leaves his desk, the automatic screen saver password configuration should lock the personal computer 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

7.26 Access Control



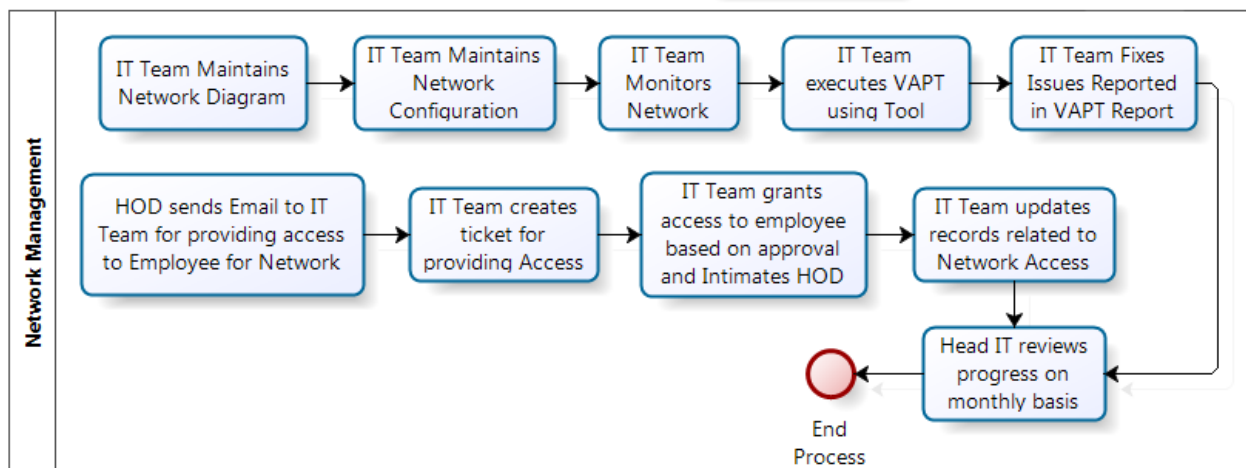
- IT Team creates Standard user profiles for user and policy management.
- User Registration and De-Registration at all levels will be defined and monitored as per the set SOP.
- All Privileges are granted to users as per the defined roles and responsibility and the same will be listed in the SOP.
-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

7.27 Patch Management



- 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 update tool
- IT Team maintains records of all patch update
- IT Head reviews status of Patch update on monthly basis

7.28 Network Management



- 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& PT should be done after office hours or off time.
- VA& PT tools should be kept in secure place and should be used only after management approval.
- 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 updation of Network Access

7.29 Network Time Synchronization

- All servers and network devices time will be synchronized with NTP server as defined in NTP policy and procedure. NTP procedure will be followed for all servers and network devices.

7.30 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.

7.31 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 & PT 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
---------------	-------------------	-----------------------	---------------------------------	---------------------------------	--------------------------

<i>Sr. No</i>	<i>Objectives</i>	<i>Responsibility</i>	<i>Frequency of Measurement</i>	<i>Reporting of Measurement</i>	<i>Target to Achieve</i>
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 & PT 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

<i>Outputs</i>
<ul style="list-style-type: none"> • 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 • 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

Outputs

- 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 & PT Report
- Change Request Form
- Change Request Register