IT Policies & Procedures

Introduction

The effective management of Information Technology is key to the performance of the Manjushree Technopack Limited (MTL). The aim of this policy is to define a framework within which MTL can operate without compromising Organisational performance. The primary intended audience of the policy is stakeholders and employees of MTL. It is therefore the responsibility of everyone to adhere to this policies and procedures.

The need for Standards

In the absence of common standards and operational practices, there are chance of risks that each MTL Business units or business functions within the organisation will develop their own, creating barriers and hindering the deployment of best practice across MTL.

Common standards will facilitate the transfer of essential data and will allow the development of central Knowledge bases on common software, hardware, infrastructure and security issues.

IT Policy Operation

The MTL IT Policy covers the following.

Section: 1] IT Organisation at MTL

Section: 2] General code of Conduct

Section: 3] Desktop, Laptop, Network & Telephone Infrastructure

Section: 4] Infrastructure overview

Section: 5] Business / Enterprise Resource Planning (ERP) Systems

Section: 6] CAD / CAM / CAE

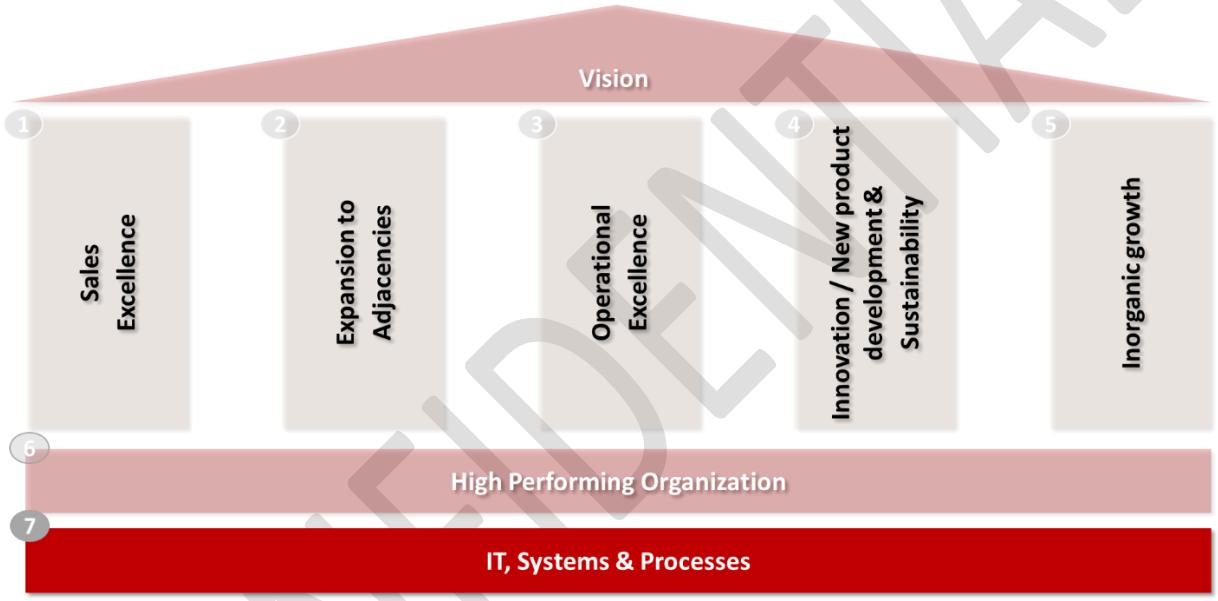
Section: 7] Data security, Backup and Disaster Recovery planning

Section: 8] Email & Internet usage

Section: 9] Control & Management of Major IT Projects

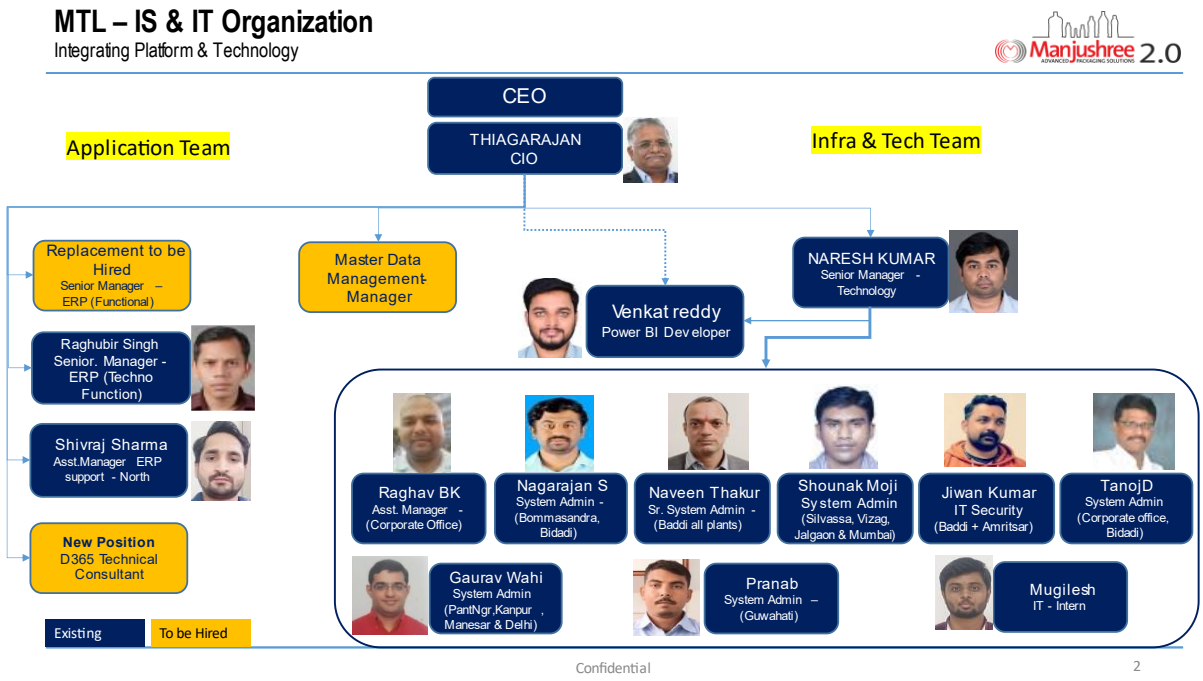
Section: 1] IT Organization at MTL

IT is no more support or service function in any organisation today. IT being part of the business growth and decisions, as a business enabler, the road map to achieve that requires full involvement and contribution from the leadership team. It is also for the leadership team to understand that creating IT technology in the organisation has several direct impacts to the business outcomes. The same is the case with MTL. Below is the representation of various pillars in MTL and IT Systems & Process is one of the key pillar for the business growth and support.



We at MTL, follow the 4 pillar approach / strategy on every IT initiatives to facilitate and support the business through Information Technology and System.

IT Organisation Structure



Section: 2] General code of Conduct

- **Your role:** You must understand your role and responsibilities regarding MTL IT systems. If this is unclear, you must consult your line manager in the first instance.
- **IT security incidents:** You must immediately report all actual or suspected IT security incidents to itsupport@manjushreeindia.com or it@manjushreeindia.com
- **Business use:** You must only use MTL IT systems for business activities which are related to your work with Manjushree Technopack Ltd.
- **Personal use:** You are permitted reasonable and limited personal use of the MTL IT asset provided to you such that, it does not adversely affect MTL business ethics.
- **Your privacy:** Your personal privacy is respected, but you must understand that we may monitor your use of our IT systems. In so far as the law allows, MTL reserves the right to monitor IT systems activity for the purposes of maintaining your safety and information security.
- **Zero Tolerance on Data Breach:** Incidents where confidential information is accessed by unauthorised individuals could be a privacy breach. Promptly report this through appropriate channels. Respect organisational confidential data at all times.
- **Accessing our IT systems:** When accessing MTL IT systems, you must only carry out the activities that you are authorised to do and must only access information or IT systems which you are authorised to use.
- **Offensive material:** You must not use MTL IT systems to access any information that contains nudity, pornographic, obscene, indecent, hateful, racist or other offensive material.
- **Working with sensitive information:** You must only access, print, share, post, publish, upload or email information that you are authorised to do.

- **Use of Personal Devices & Gadgets:** In MTL office premises, you are not allowed to bring any authorised personal Gadgets and digital devices for using it official purposes.

Section: 3] Desktop, Laptop, Network & Telephone Infrastructure

- **PC Desktop / Laptop Hardware:** The standard Pc Desktop or Laptop hardware is to be Intel or Intel compatible. Following are the recommended configuration as per the current software usage requirements. The review of the make, model and configuration will happen, once in a year.
    - **MEX Grade:** - Laptop HP series, i7 processor, 8GB RAM, 500GB SSD or equalent.
    - **All others:** Laptop HP series, i5 / i7 processor, 8GB RAM, 1TB HDD or equalent
    - **Standard desktops**: All-in-one Lenovo / HP with i5 / i7 processor, 8GB RAM, 512 GB SSD
    - **Design & RND Desktops**: High end All-in-one Dell / HP with 32GB RAM, 1TB SSD
- **PC Desktop / Laptop Software:** All the MTL provided Desktop and Laptops are to be compliance with the following software components. Any exception to the list below needs to be discussed with CIO of Manjushree Technopack Limited and obtain approval prior to implementation. The review of the approved software lists will happen, once in a year.
- **Laptops / Desktops provisioning:** As per MTL IT policy, following are the criteria for availing company Laptops or Desktops.
    - Employees who are frequent travellers for business purpose are eligible for Laptops
    - Employees who are required to perform their day-to-day duties using ERP, business system and occasional travellers will be provided Desktop computers.
    - All the MEX, MELT and Senior & Middle management employees are eligible for Laptops. However, any employees whose job requirement demands laptop and who are required to support the business after office hours or provide remote support will be allotted Laptops based on the justification and approval from their functional head(s).
    - The life of the Laptops and Desktops issued by the company to employees are minimum 5 years. After completion of 5 years, depending on the need and condition the laptops will be replaced.
    - Procurement of new Laptops or Desktops will be made, only when there is no usable hardware is in stock.

Provisioning of Laptops or Desktops are subject to approval from the respective HOD / Functional heads as per the Job role of the employees as mentioned above.

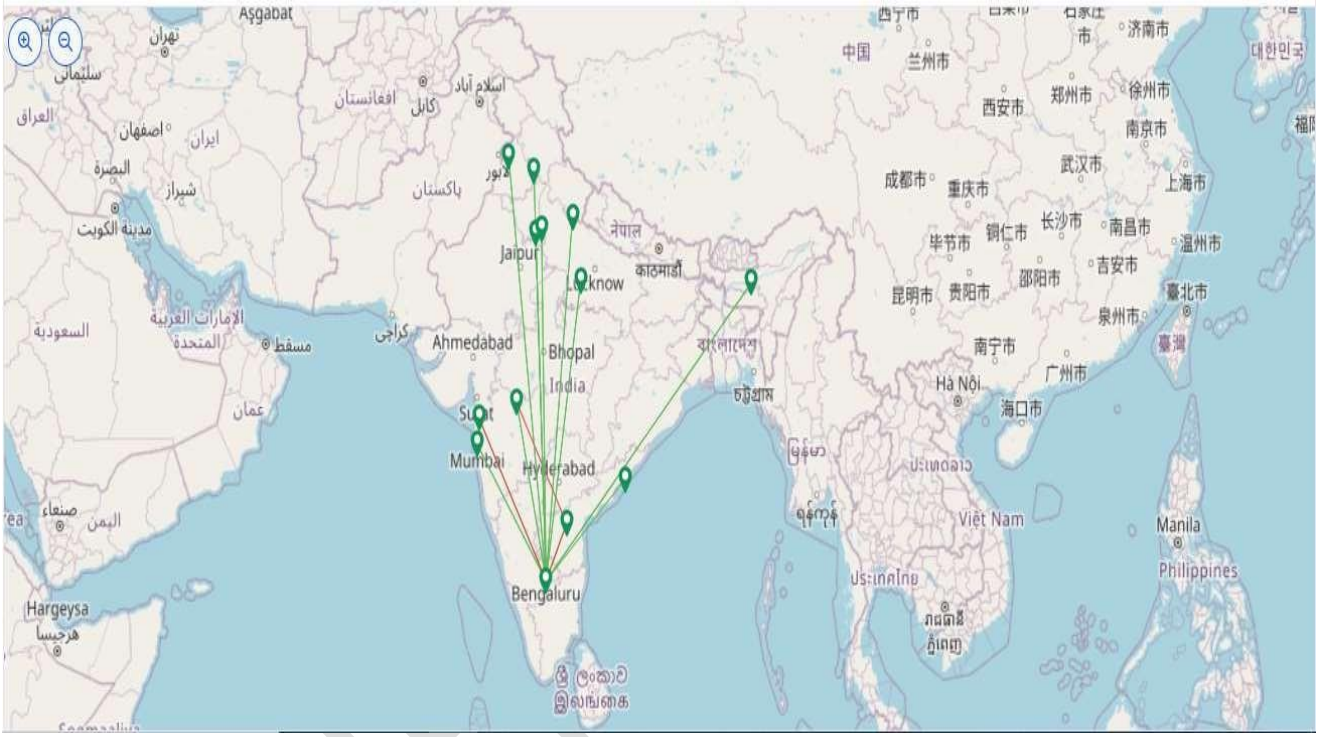
Employees are advised to fill the attached **Annexure – 1** and submit to IT after obtaining the IT assets.

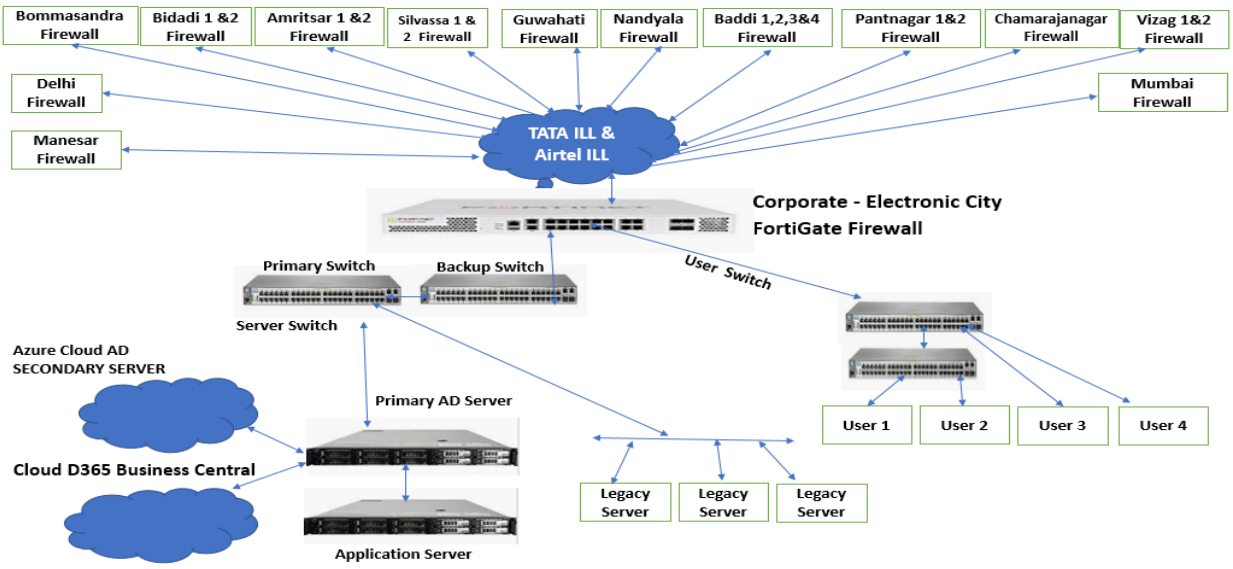
Printers / Scanners / Photo copiers: As per MTL IT policy,

- All the employees are recommended to use the common high-speed printers installed at the office premises. On an exceptional case like Cheque printing or Confidential documents printings, a dedicated desk printer will be allotted.
- There is a common high-speed all-in-one printer installed at office premises can be used for document scanning and photo copier purpose.

- All employees are recommended to use mono (black&white) printing until there is a strong need for color printing.
- All employees are advised to avoid printing as much as possible and make use of emailing and other communication solution implemented in our organisation to share the documents.

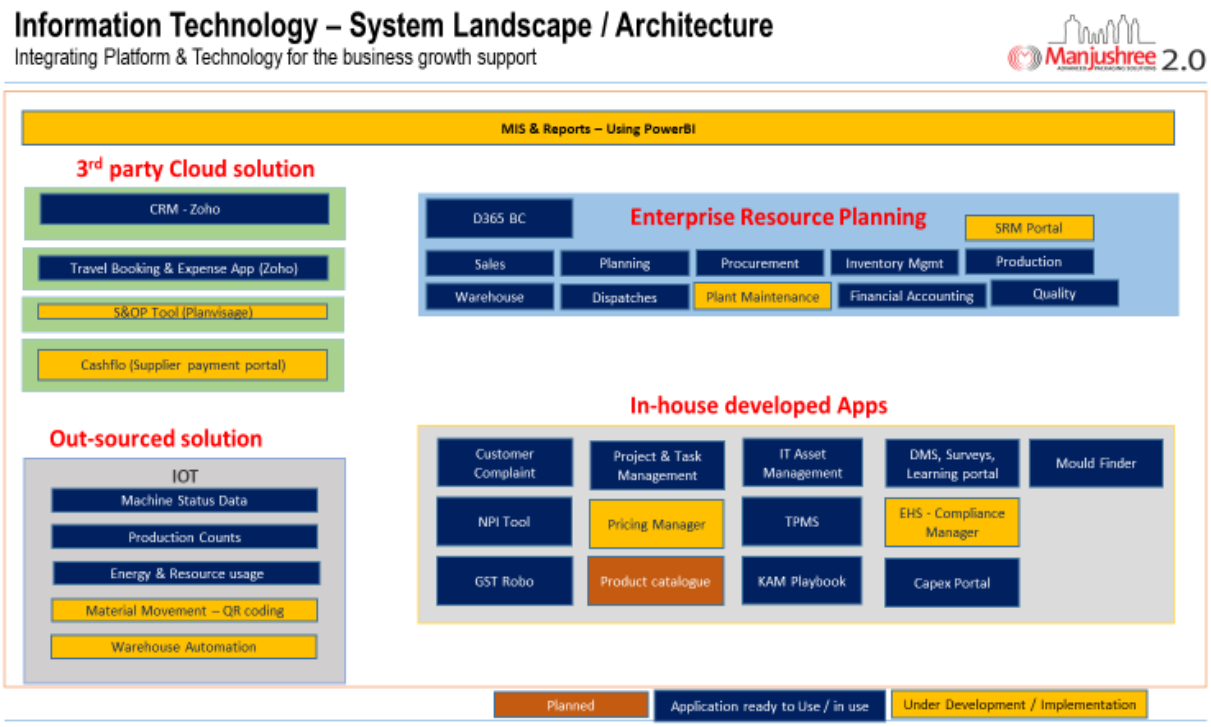
Section: 4] MTL Infrastructure overview

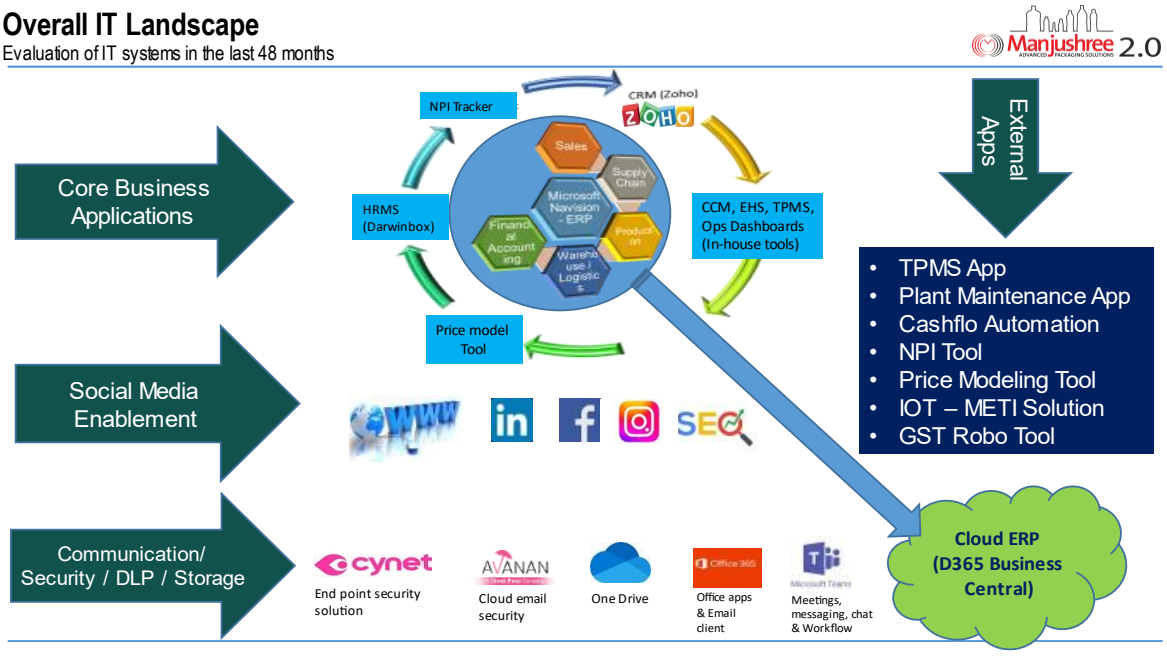




Section: 5] Business / Enterprise resource planning system

IT Landscape





At present in MTL, we use Microsoft Dynamics D365 Business Central as a core business application or Enterprise Resource Planning with below functionalities;

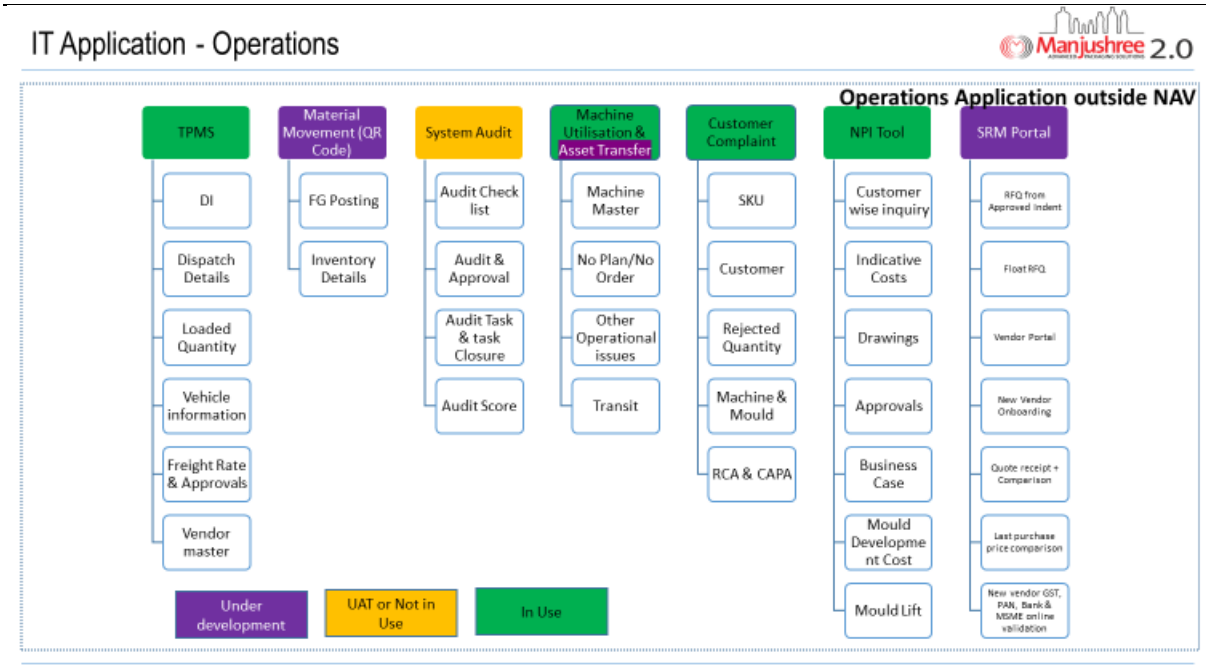
- Sales and Receivables
- Procurement and Payables
- Operations
- Inventory Management
- Financial Management
- Quality Management
- Plant Maintenance

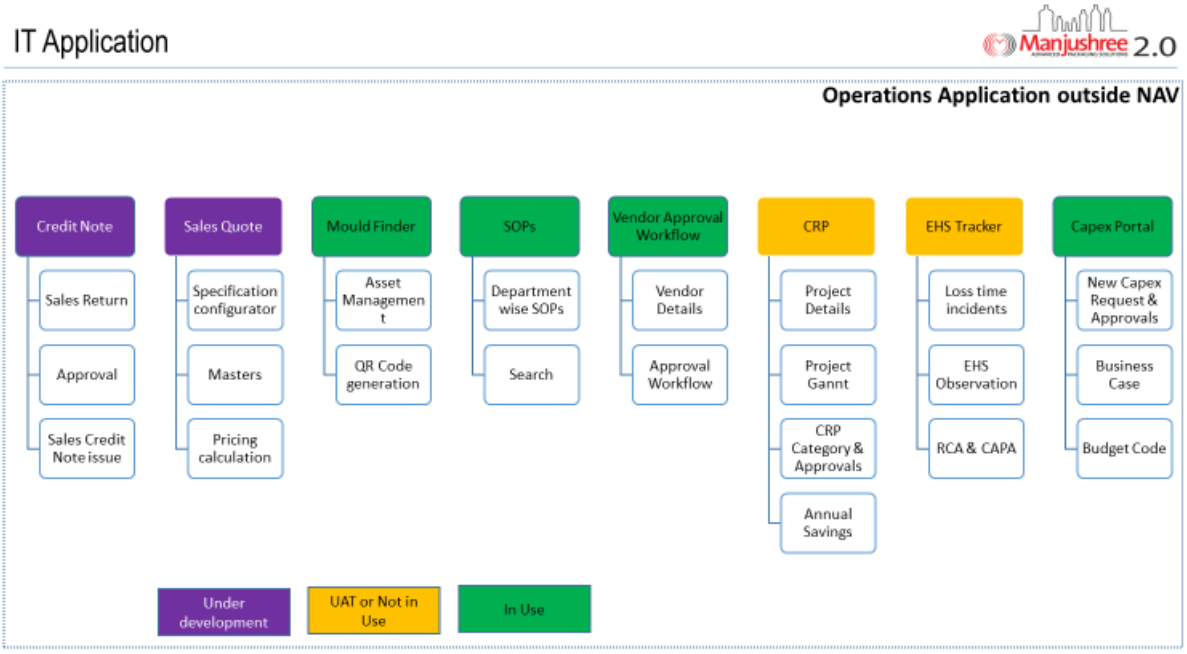
Along with suit of external applications that includes.

- Demand Planning – Planvisage
- CRM – Zoho CRM
- HRMS – Darwinbox
- Employee expense & Reimbursement - Zoho Expense
- Lawrbit for Compliance

- Internally developed applications that include NPI, TPMS, Customer complaint etc.,

Below picture represents the current landscape of other application and its collaborative tools.


IT Application - Operations
Manjushree 2.0
Operations Application outside NAV
TPMS
DI
Dispatch Details
Loaded Quantity
Vehicle information
Freight Rate & Approvals
Vendor master
Material Movement (QR Code)
FG Posting
Inventory Details
System Audit
Audit Check list
Audit & Approval
Audit Task & task Closure
Audit Score
Machine Utilisation & Asset Transfer
Machine Master
No Plan/No Order
Other Operational issues
Transit
Customer Complaint
SKU
Customer
Rejected Quantity
Machine & Mould
RCA & CAPA
NPI Tool
Customer wise inquiry
Indicative Costs
Drawings
Approvals
Business Case
Mould Developme nt Cost
Mould Lift
SRM Portal
RFQ from Approved Indent
Float RFQ
Vendor Portal
New Vendor Onboarding
Quote receipt + Comparison
Last purchase price comparison
New vendor GST, PAN, Bank & MSME online validation
Under development
UAT or Not in Use
In Use


IT Application
Manjushree 2.0
Operations Application outside NAV
Credit Note
Sales Return
Approval
Sales Credit Note issue
Sales Quote
Specification configurator
Masters
Pricing calculation
Mould Finder
Asset Managemen t
QR Code generation
SOPs
Department wise SOPs
Search
Vendor Approval Workflow
Vendor Details
Approval Workflow
CRP
Project Details
Project Gannt
CRP Category & Approvals
Annual Savings
EHS Tracker
Loss time incidents
EHS Observation
RCA & CAPA
Capex Portal
New Capex Request & Approvals
Business Case
Budget Code
Under development
UAT or Not in Use
In Use

The following explains the overview of Change Management process being followed in MTL for any of the ERP system or process changes.

The following roles with corresponding responsibilities for any of the Navision ERP process related changes are defined.

Role	Description
Initiator	The individual who submits a new change request (CR)
Process owners	• The individual who is assigned responsibility for making changes in response to an approved CR and updates the status of the request over time. • Will be responsible for process Sign -off. • The individual who may be assigned to analyze the impact of a proposed change.
Super user / Power user	Work closely with IT Team to resolve their process related issues
Local IT Project Manager	• The individual who is responsible for overall planning and tracking of the development project activities. • The individual who determines whether a change was made correctly.
COA Manager	• The person who is authorized to approve the modified changes can be promoted to the next level. • The individual who decides to approve or reject proposed changes for a specific system. • The individual who is responsible for allocating the requests, ensuring they reach the right people and are actioned in a timely manner as well as maintaining a log of changes. • The individual having final decision-making authority and selects the appropriate COA Process owner for each CR.

Following is the Change Request Form which is mandatory filling for every change requests. The content in the below format is illustration purpose only.

Change Control – Risk Assessment Form

CHANGE REQUEST: MTL-CR-0012020	REQUEST DATE: 10/04/2020
Change Title:	Rate Discounting Process
Process Area:	Procurement
Change Initiator:	
Contact phone:	
Change Date:	
Change Time:	
Change Duration:	
System(s) Affected:	

DESCRIPTION OF CHANGE

What? –. Changes Required for managing Rate Discounts when Quantity is in multiples.

Why? – Some of the MTL components ordering should have Quantity based rate discount option when purchased in multiples and have discounts on Quantity Slabs.

References –

IMPACT OF CHANGE

Who will be affected by the change? –

How will they be affected during the change? – The changes in Rate Discounts should be updated for respective Vendor and Item and test in purchase order flow with report output, Accounts Transactions and Entries after GRN.

How will they be affected after the change? - There will be no impact on the other business divisions after these changes.

SECURITY IMPACT OF CHANGE

What is the risk of making the change and how is the risk being mitigated? –

This should not have any issues after implementing or using it.

What is the risk of not making the change and how could that risk be mitigated?

IMPLEMENTATION AND BACKOUT PLAN	
Implementation Plan: • Update transaction data and check the process flow. • Check output • Check Accounting Entries	**Backout Plan:** • Remove changes

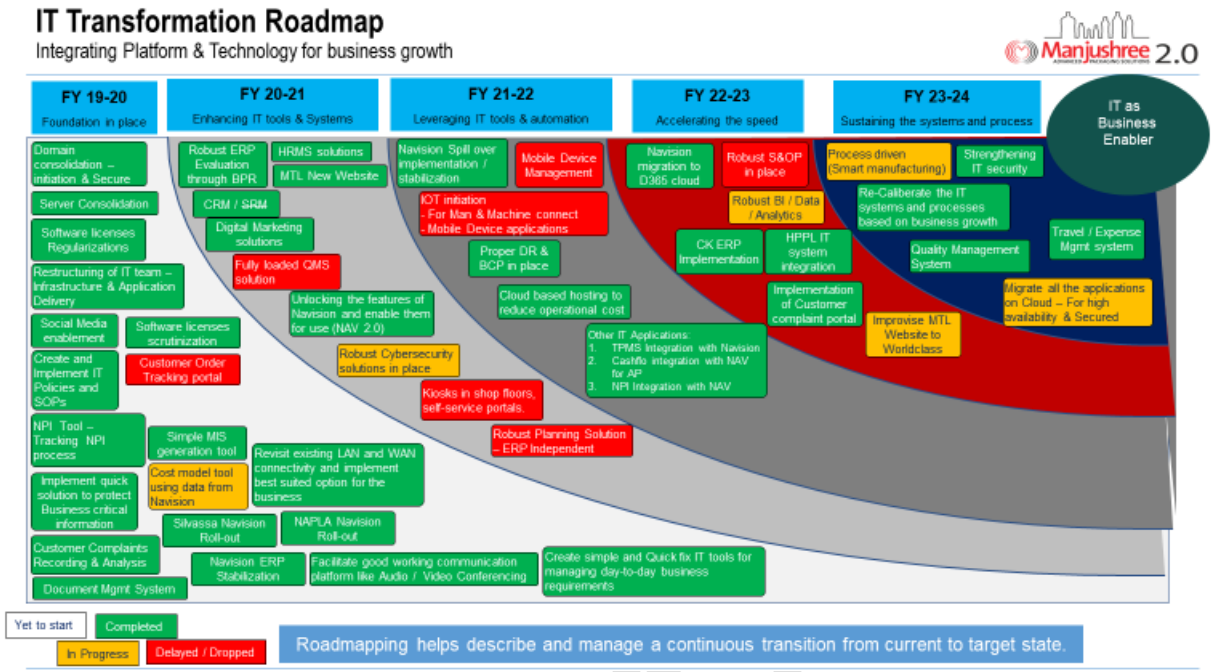
TESTING OF CHANGE
Supporting evidence: Test Cases and testing results after Beta Proto type validation and acceptance. **Validate Purchase Order Printout** **Validate Accounting Transaction after GRN and for Payment Voucher.**

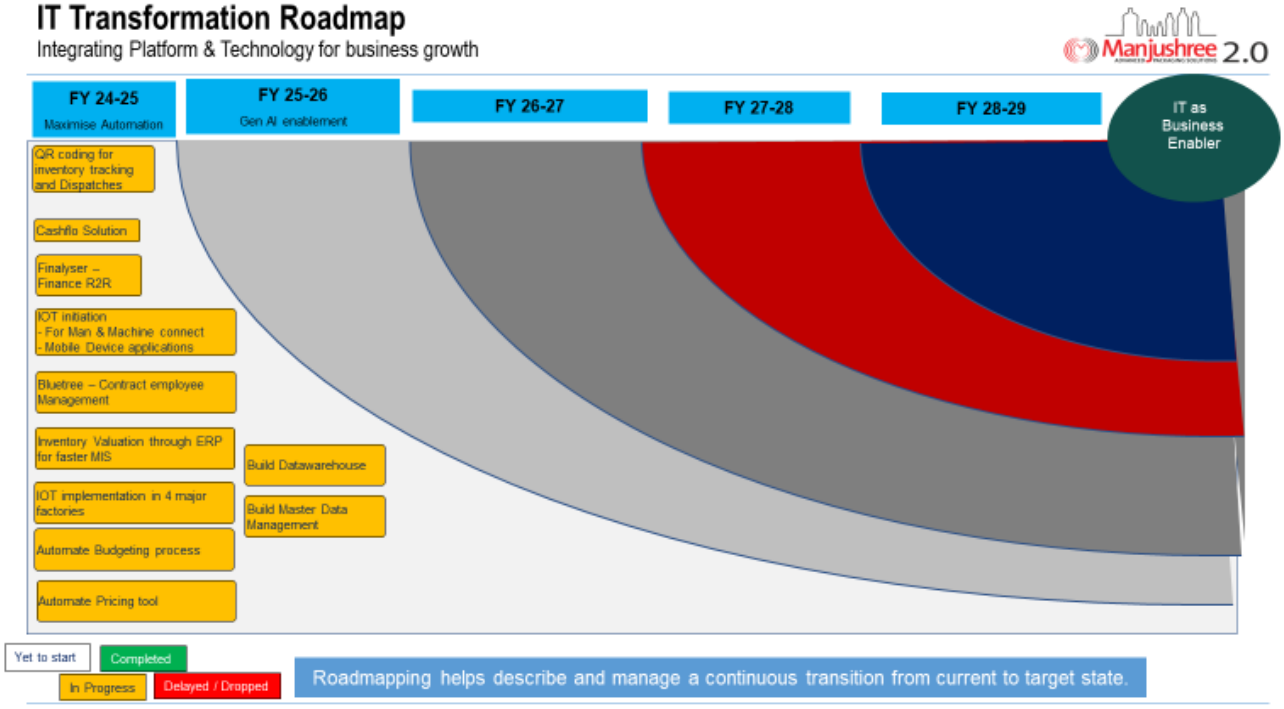
For Change Control coordinator Use Only

APPROVALS			
Date	***Name***	***Approved for***	***Signature***

CONDITIONS ON APPROVAL

IT Roadmap – 4 years plan





Section: 6] CAD / CAM / CAE

Following are the CAD / CAM tools are currently being used in MTL for New product design and development purpose.

1. AutoCAD 2019
2. PTC CREO
3. Corel Draw
4. Adobe Photoshop
5. Keyshot

Section: 7] Data security, Backup & Disaster Recovery plan

Introduction:

MTL is critically dependent on information and information systems. The good reputation that MTL enjoys is also directly linked with the way our Intellectual properties are protected and managing information systems. The purpose of the IT security policy is to establish management direction, procedures, and requirements to ensure the appropriate protection of MTL information systems data.

To be effective, information security must be a team effort involving the participation and support of every MTL employees who access MTL computers, networks, and information. It is the policy of MTL to prohibit unauthorised access, disclosure, duplication, modification, appropriation, destruction, loss, misuse, and theft of all MTL information.

Requests for changes to, or variation from, this policy are to be forwarded to the MTL CIO including any supporting documentation for the change.

Data destruction and Disposal policy:

All customers and vendors related data will be disposed after 7 years of time, when organisation decides that they are no longer required for business. Employee related data will be disposed other than basic necessary information required for the business.

Responsibilities:

Overall responsibility to deploy and enforce IT security policies in all MTL locations lies with Corporate IT function. Every employee at MTL must comply with the information security policies found in this and other related information security documents.

Data protection:

- Sensitive data printed on paper output must be shredded prior to disposal. Some of the typical examples for sensitive data are;
    - Salary information
    - Personnel records
    - Customer and Vendor details
    - Sales enquiry and Sales data
    - Confidential corporate matters
    - Pricing calculations etc.,
- Incase of employment termination, employee resignation and service completion, users are not allowed to remove or copy the data from their computer. All credentials assigned to that employee will be revoked during the exit clearance process.

- Employees are advised not lend their laptops or computers and login credentials to others at anytime.
- Computer equipment supplied to users by MTL should not be altered or added without prior authorization from MTL CIO.
- Printers must not be left unattended if sensitive information is being printed or to be printed (drawings, Financial information, Payroll, HR information and other confidential information of the business)

Information or Data Security

Communication by email is not confidential or an entirely secure means of transmitting information. It can be intercepted by "hackers" or can be sent to the wrong person or organization. It can easily be copied and widely distributed. These factors should be carefully borne in mind when Users send emails. All external emails, which are sent from the Company's system, must contain the disclaimer set out in Working Practices for Email and Internet Use
(NB: the disclaimer is automatically applied to outgoing external emails).
Users must not delete, alter, or otherwise interfere with the content of the disclaimer. It is possible, in exceptional circumstances, to encrypt information of a highly confidential or commercially sensitive nature. Such information should only be sent after consultation with the concern company authorities.

Data Breach Policy

Security incidents involve wrongful handling or disclosure of information and can give rise Data Breaches where confidential data is involved. While data breaches are a matter of concern, some will have more severe impact on the data subject. Potential damages to data subject takes three main forms:
1] Financial - If any bank or credit card details or other information which may allow someone to impersonate them, find their way into the wrong hands.
2] Security – If personal address or other information which are relevant to a person's security.
3] Reputational – if information which could be misused by our business competitors, media or other individuals can bring damage to our business performance.

When any employee becomes aware that confidential information has inadvertently been sent to the wrong person, he/ she must inform;

A] Their immediate manager and the IT Data security team.
B] In their absence, a senior Leadership member present at that point of time must be informed.

Failure to notify immediately on discovering such risk may result in disciplinary proceedings by the organization.

Employee must seek advice before taking any remedial action as soon as they realised such incidents.

Viruses, Spyware and Malware

While the organisation is having adequate protection and security measures in place to prevent intrusion of viruses into the Company's network, it is also important for the employees to be aware of viruses can intrude into company's network or transmitted to a third party's system by sending and receiving email and by using the Internet. The deliberate introduction of a virus is a criminal offence. Accidental introduction of viruses may, in certain circumstances, give rise to a claim against the Company. All Users must take all reasonable steps to ensure that no viruses are transmitted and to ensure that they do not allow a virus to affect the Company's computer systems. Failure to do so may result in disciplinary action being taken against an employee concerned.

At MTL, we use the following software's, tool and hardware for information protection purpose:

1. Perimeter Firewall - Our company utilizes FortiGate firewall, network security device that monitors and controls incoming and outgoing network traffic. It is used to block unauthorized access to our network, prevent malicious traffic from entering or leaving a network, and protect against denial-of-service attacks.
2. MFA - Our company has enabled multi-factor authentication (MFA) for all employees. This means that when you log in to your work accounts, you will be required to enter a code from your authenticator app in addition to your password. This adds an extra layer of security to your accounts and helps to protect them from unauthorized access.
3. Endpoints - Our company uses the Auto XDR Cynet and ATP Avanan security solutions to protect our endpoints. These solutions provide comprehensive protection against malware, ransomware, and other cyber threats.
4. IAM - We use Entra ID for identity and access management (IAM). Entra ID is a cloud-based IAM platform that helps us to manage user access to our systems and data. It also provides us with insights into how users are accessing our systems and data, which helps us to identify and mitigate potential security risks.
5. Zero Trust Framework - Our company has adopted a zero-trust framework for our security posture. Zero trust is a security model that assumes that no user or device can be trusted by default. All users and devices must be verified before they are granted access to any system or data.

Computer Viruses, Worms & Trojans

To assure continued uninterrupted service for both computers and networks, all computer users must keep approved virus detection software enabled on their computers. Updates to this software will occur automatically as and when the new updates are available.

Users must contact local IT representative whenever they believe that their system has been infected or some suspicious activity is noticed. This will help us to prevent and minimise the damages.

Un-Authorized Use

Email and the Internet must not be used for the creation, transmission, downloading, browsing, viewing, reproduction or accessing of any image, material or other data of any kind which:

- Is illegal, obscene, pornographic, indecent, vulgar or threatening.
- Contains unacceptable content, including but not limited to sexually explicit messages, images, cartoons or jokes, unwelcome propositions or any other content which is designed to cause or likely to cause harassment or provocation of any other person or organization based on sex, sexual orientation, age, race, national origin, disability, religious or political belief;
- Is defamatory.
- Deliberately introduces viruses into the computer systems of the Company or any other party or is designed to corrupt or destroy the data of other users;
- Conflicts with the Company's commercial interests.
- Infringes or may infringe the intellectual property (including but not limited to any rights in or to copyright, trade or service marks, trade names, designs, logos, graphics, software or information) or other rights of another; or Disrupts the work of other users.

Users must not deliberately or knowingly create, transmit or download chain letters, junk mail or unsolicited commercial or advertising materials. In some cases, it may be necessary to open and view an email to determine that it falls within one of these categories. All such emails should be immediately deleted.

Use of Social Media

- Access to some of the social networking websites are blocked by the company and employees will not attempt to access such sites at work except the MTL approved social media sites.
- Employees must take care to ensure that any reference to Manjushree Technopack or any other form of company representation within social media sites maintains company integrity.

Physical Security

- You are responsible for ensuring the security and safe keeping of our IT systems and other devices containing our information; particularly at non-MTL locations such as in your vehicle, at home, Airport, Hotels, when on the train, at a cafe etc.
- If you need to leave any mobile devices (such as mobiles, laptops and tablets), or any other device containing our information, in the office overnight or when you have finished working for the day, then you must lock it in secured manner wherever possible or at least place it out of sight. If you are at a non-MTL location, then you must take similar measures.
- In public places, such as Trains, Aircraft or coffee shops, you must be aware of others who may be able to view your password entry, screen or papers. You must take appropriate precautions, particularly with using sensitive information, in such circumstances.
- If you need to move away from our IT systems, or other devices containing our information, unattended then you must activate a password protected screen lock.
- You must immediately report all lost or stolen IT systems, or other devices containing our information, to your local IT support team.

Software Security Policy

- Users should assume that all software on MTL computers are protected by copyright and must not be reproduced in any form. Software purchased by MTL must be used in accordance with license agreements and copyright laws.
- All commercial software purchased by MTL is authorised for MTL use only. Making copies of MTL purchased software for personal use is illegal and prohibited.
- Computer games and other unauthorised software tools must not be loaded onto MTL computers.
- MTL computers and networks must not run software that comes from sources other than MTL other departments, knowledgeable and trusted user groups or software approved by IT department.

Password Policy

Keep passwords secure: You must keep all your passwords safe. Do not write them down in any manner that would make it easy to decipher and don't tell anyone your login details or password. Any activity carried out on your password protected account will be deemed to be your activity unless there is evidence to the contrary.

Your Password:

A] Must be strong and atleast with 8 characters long
B] Must be Unique from your previously used passwords
C] Should not contain any word spelled completely
D] Should include Uppercase letters, Lower case letters, numbers, and special characters

Whenever a new credentials are assigned to the users with pre-defined passwords, users are required to change them at first login.
The local administrative passwords and the server administrative passwords must be reset every 180 days for greater security and the

The minimum password age policy is 45 days.

Monitoring

General IT system monitoring: Systems have been implemented to automate monitoring to ensure real-time protection e.g. automatic removal of viruses.

Specific monitoring: Your communications may be monitored when it appears that our IT systems are being misused, in such instances an investigation might occur. There may be other reasons why your communications are monitored, eg: in your absence for business continuity purposes.

Specific monitoring will only occur after a formal request is approved by senior management.

VPN Users

Users who are required to access the MTL systems will be provided with VPN access. However, it is required to be approved by their functional heads with job requirement justification and subsequently the same will be reviewed and approved by the CIO before allocating the credentials. Employee who need a VPN access required to fill the necessary application form and submit to IT.

Refer Annexure – 3, VPN access request form.

Equipment Disposal policy

IT equipment can store a great deal of sensitive information. Also, the internal hard-drives of server computers, disk storage arrays, desktops, laptops modern digital scanner / copier / print stations often have internal storages which can store copies of documents printed or scanned using them. Network equipment's like routers, switches and firewalls contains configuration information potentially valuable to third parties. Whenever these assets are disposed, sold or replaced, the process should protect against information loss / leakage by adhering to the following requirements;

An auditable log of all IT equipment disposed should be retained.

All the MTL data including internal network and server configuration information should be cleansed / removed from all the equipment's including Servers, desktops, laptops, printers, scanners and copiers before being disposed of either through the use of software tools for secure eraser or low-level formatting.

All identifying badges or labels indicating that the equipment was a MTL asset should be removed prior to final disposal of the assets.

If any third party involved in data eraser / media destruction, appropriate certification should be provided by the third party detailing their role, the equipment disposed of and providing assurance that all MTL data has been removed / destroyed.

DR & Backup procedures

Definition of Disaster:

Disaster is any unforeseen event that can significantly put your organisation at risk by interfering with your operations – whether natural, like flooding, or man-made.

Disaster Recovery is the process of resuming normal operations following a disaster by regaining access to data, hardware, software, network equipment, power and connectivity.

The goal is to support the overall business continuity management process by ensuring that the required IT technical services and facilities can be recovered within required and agreed business timescales. IT service continuity management is therefore concerned with managing an organisation's ability to continue to provide a pre-determined and agreed level of IT services to support essentials business requirements following an interruption to the business.

This Disaster Recovery Plan (DRP) captures, in a single repository of all the Information that describes MTL's ability to withstand a disaster as well as the processes that must be followed to achieve Disaster Recovery.

Backup policy

To protect MTL information resources from loss or damage, all the computer users are required to backup their working files and data to their "OneDrive" account which has the limitation of 1 TB space as we do not have policy for centralised backup of the individual user data. IT team can help you to train the users for enabling "OneDrive" backup. Then, it is each individual user's responsibility to maintain regular backup of their critical data. However, the critical user's data and organisation critical data stored in a shared folder at the central storage will have periodic backup maintained by IT department. Please contact IT system administrator for more details on central storage.

IT department is responsible for maintaining backup of ERP system, Active Directory, Firewall and network device configuration and log files.

If the system is primarily used as a personal productivity tool, then back-up is at the discretion of the individual users.

Server Backups:

1. D365 Business Central
    a. Here is a summary of the key points regarding Microsoft's business continuity and disaster recovery practices for Dynamics 365 Business Central:
    b. Microsoft provides geo-redundancy and automatic backup of SQL and Azure

storage for production instances. This includes replicating data and infrastructure to a secondary Azure region.

c. In the event of an outage or region-wide disaster, Microsoft can fail over to secondary region instances with limited potential data loss (up to 15 minutes) and recovery times ranging from 4-10 hours.
d. During a failover, functionality is reduced. Financial reporting and Power BI reporting will be unavailable. Non-production instances may also see degraded performance.
e. Once the primary region is restored, Microsoft fails back with brief service interruptions but no data loss.
f. Microsoft handles redundancy and failover of services it provisions, including SQL, storage, and compute infrastructure. Customers are responsible for disaster recovery of any additional resources not provisioned by Microsoft.
g. Disaster recovery plans and infrastructure are reviewed, updated, and tested annually for Dynamics 365 services.

2. Apps Backup – On daily basis at 1900 hrs, an auto initiated backup job is run and the backup file is stored in 2 devices simultaneously.
    a. One at the local storage box and OneDrive.

Section: 8] Email & Internet usage policy

MTL email Policy:

As per MTL email provisioning policy, employees are advised to fill the **Annexure – 1** (for an existing employee who do not have MTL official email id) and submit to IT for email id creation. For all the new employees, HR will initiate the process at the time of employee joining MTL organisation.

- This Policy applies to all employees of the MTL and all MTL contractors, agents, suppliers, customers and any other persons who at any time use or have access to email or the Internet during the course of their employment or business dealings with the MTL Users.
- Provisioning of email ids to the employees subject to obtaining approval from respective HOD / Functional heads.
- As per MTL standard, email ids are to be created with "firstname.lastname@domain" to avoid confusions in identifying and ensuring the right contacts.
- All the employees are advised to follow the MTL defined email signatures to maintain standards and brand image of Manjushree Technopack.
- The MTL owns the IT components required to support the email system and Internet connectivity and provides the right to use these systems for legitimate business purposes only.
- Use of company provided computer system, email and Internet access are for business purposes, and are not private or confidential. No employee should have any expectation that any email or Internet communication he or she makes, regardless of its content, is private or confidential.
- The commercial and legal effects of sending and receiving emails or other electronic communication are the same as any other form of written communication. The style, tone and content of emails has a direct effect on the way the Company is perceived by others. Emails can contractually bind the Company and any advice, opinion, guarantee, representation, or other statement contained in an email can be relied upon by the Company's clients or other parties.
- All the emails sent from MTL employees will have disclaimer attached, and hence employees are advised to not to tamper or delete the disclaimer messages by any means.

- Users must not send emails or other electronic communication which make representations, contractual commitments or any other form of statement concerning the Company unless they have authority from the Company to do so.
- Users must be aware that the Company shall adopt an appropriate email retention policy in accordance with local legal requirements. Email and other electronic communication could be requested in the event of a legal proceeding through "e-discovery" efforts. Care is taken to preserve the integrity of archived email within the retention policy as well as destroyed once the appropriate retention period has expired.

Using MTL Internet facility

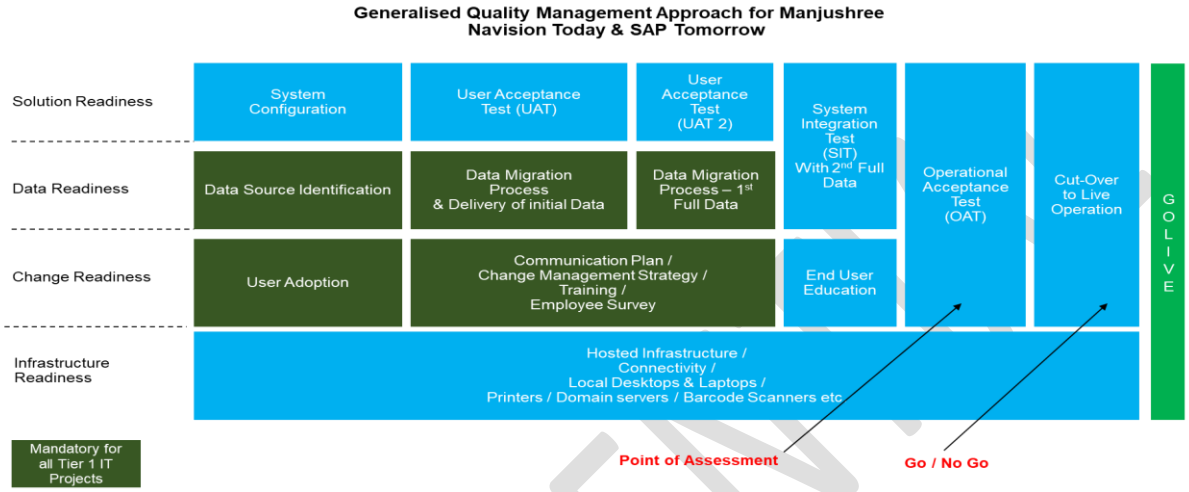
By default, all our employees are provided with MTL Internet access. However, usage of Internet has to follow strict guidelines as mentioned below.

- **Authorised software**: You must only download, install or run software on our IT systems after first obtaining the appropriate authorisation by contacting your local IT support team.
- **Personal use of social networking sites:** You should be mindful that anything you publish on social networking sites may be difficult to remove. If you access such sites from our IT systems, you should do so in compliance with this SOP.
- **Business use of social networking sites:** If you are authorised to access social networking sites for our business purposes then you must do so in a professional manner and in compliance with this SOP. You should be mindful that anything you publish, may be deemed to be for and on behalf of MTL and may prove difficult to remove.
- **Remote access:** When you use a public/shared device to access our information remotely, you must reject any prompt to save your username or password in the browser for future use. You must also ensure that you log out of the remote access service completely when you are finished and close any open browser. Where possible you should log out of the device completely and either shut it down or restart the device.
- **MTL practices:** Depending on our business requirements and day-to-day working requirements, we reserve the right to make and use of Internet access to employees.

Section: 9] Control & Management of Major IT projects (IT Governance)

All the IT projects (Major) are to be governed by the following approach

Governance structure for any Business Application System implementation
Ensure Successful adoption



Annexure – 1

PROVISIONING OF LAPTOP / DESKTOP

REQUEST FOR DESKTOP / LAPTOP

TO
THE IT DEPARTMENT
MANJUSHREE TECHNOPACK LIMITED.

ISSUE OF DESKTOP/LAPTOP-OFFICIAL USE

The company is pleased to issue you a Laptop/Desktop for official use. This asset has been provided to you to carry out your official duties with convenience and the company expects you to hold full responsibility of this Asset and take care of as if it is your own. Please read the below mentioned details carefully and sign.

You have been provided with a DESKTOP/LAPTOP computer &you have verified the details of the computer, as follows:

USER DETAILS			**EMP ID:**
Username			
User Category	☐ Employee		☐ Contract

COMPANY NAME		Job Title/Designation	
Unit / Branch / Location		Date of Joining	
Department			
Reporting To		Mobile No.	

REQUIREMENT	☐ All in one Desktop	Processor	GB RAM	GB HDD	
	☐ Laptop	Processor	GB RAM	GB HDD	LAPTOP BAG
	☐ AD Login ID :				

ADDITIONAL REQUIREMENTS	☐ Mouse ☐ Keyboard

SOFTWARE REQUIREMENTS	☐ Standard	Windows 10, WINDOWS 11, OFFICE 365 (E1/E3), CYNET Antivirus & TRELIX DLP,7Zip, Adobe Reader, Google Chrome, Java.
	☐ Other Software	AutoCAD, Acrobat Writer, CorelDRAW, Key shots, Creo.

Annexure – 1	**Requestor**	**CHRO**	**User Department Head**	**IT DEPT**
Name		ANIL PATRO		NARESH KUMAR G
Date				
Signature				

FOR USE OF IT ASSET MANAGEMENT TEAM			
Serial Number		**AD user ID**	
CAPIX ID		**ISSUED BY**	

Asset Details (attach the copy of the invoice of the asset purchased)				
MODEL				
Manjushree 2.0	Document No	MTL 2.0 01	Document Type	Form
	Document Name	Request for Desktop / Laptop	Version No	2.0

REQUEST FOR DESKTOP / LAPTOP

DESKTOP / LAPTOP USAGE POLICY

The above details pertaining to the issue of a desktop/laptop, is correct.

- Other than the above items, nothing else has been installed by the company and I hereby agree that, if at a later date anything downloaded/found on my desktop/laptop other than the above, is my whole and sole responsibility, as I have done it on my own risk.
- I agree that the company has provided me with an asset for office use and the same needs to be returned in good condition after working tenure or upon relieving.
- I agree that this laptop / desktop contain confidential information regarding the company and sharing of such information with any outsider amounts to breach of confidentiality and lack of trust. If I am found guilty of such breach of confidentiality, I am liable to be terminated from the services of this organization with immediate effect and any/all perquisites stand cancelled in such regard.
- PC Desktop / Laptop Software: All the MTL provided Desktop and Laptops are to be compliance with the following software components. Any exception to the list below needs to be discussed with CIO of Manjushree Technopack Limited and obtain approval prior to implementation. The review of the approved software lists will happen, once in a year.
- Laptops / Desktops provisioning: As per MTL IT policy, following are the criteria for availing company Laptops or Desktops. o Employees who are frequent travelers for business purpose are eligible for Laptops o Employees who are required to perform their day-to-day duties using ERP, business system and occasional travelers will be provided Desktop computers.
- All the MEX, MELT and Senior & Middle management employees are eligible for Laptops. However, any employees whose job requirement demands laptop and who are required to support the business after office hours or provide remote support will be allotted Laptops based on the justification and approval from their functional head(s).
- The life of the Laptops and Desktops issued by the company to employees are minimum 5 years. After completion of 5 years, depending on the need and condition the laptops will be replaced. o Procurement of new Laptops or Desktops will be made, only when there is no usable hardware is in stock. Provisioning of Laptops or Desktops are subject to approval from the respective HOD / Functional heads as per the Job role of the employees as mentioned above.

- Physical Security • You are responsible for ensuring the security and safe keeping of our IT systems and other devices containing our information; particularly at non-MTL locations such as in your vehicle, at home, Airport, Hotels, when on the train, at a cafe etc. • If you need to leave any mobile devices (such as mobiles, laptops and tablets), or any other device containing our information, in the office overnight or when you have finished working for the day, then you must lock it in secured manner wherever possible or at least place it out of sight. If you are at a non-MTL location, then you must take similar measures. • In public places, such as Trains, Aircraft or coffee shops, you must be aware of others who may be able to view your password entry, screen or papers. You must take appropriate precautions, particularly with using sensitive information, in such circumstances. • If you need to move away from our IT systems, or other devices containing our information, unattended then you must activate a password protected screen lock. • You must immediately report all lost or stolen IT systems, or other devices containing our information, to your local IT support team.

- Software Security Policy • Users should assume that all software on MTL computers are protected by copyright and must not be reproduced in any form. Software purchased by MTL must be used in accordance with license agreements and copyright laws. • All commercial software purchased by MTL is authorized for MTL use only. Making copies of MTL purchased software for personal use is illegal and prohibited. • Computer games and other unauthorized software tools must not be loaded onto MTL computers. • MTL computers and networks must not run software that comes from sources other than MTL other departments, knowledgeable and trusted user groups or software approved by IT department.

- Password Policy Keep passwords secure: You must keep all your passwords safe. Do not write them down in any manner that would make it easy to decipher and do not tell anyone your login details or password. Any activity carried out on your password protected account will be deemed to be your activity unless there is evidence to the contrary.
  Your Password:
- A Must be strong and at least with 8 characters long
- B Must be Unique from your previously used passwords
- C Should not contain any word spelled completely
- D Should include Uppercase letters, Lower case letters, numbers, and special characters Whenever a new credentials are assigned to the users with pre-defined passwords, users are required to change them at first login.
- The local administrative passwords and the server administrative passwords must be reset every 180 days for greater security and the minimum password age policy is 45 days

I,_____, have read and understood the above terms and conditions on the acceptable usage of the desktop / laptop / tablet with the required accessories and agree to abide by the same. I further understand that if I violate this policy, my privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

Signature of the User

Manjushree 2.0	Document No	MTL -2.0 01	Document Type	Form
	Document Name	Request for Desktop / Laptop	Version No	2.0

Annexure – 2

REQUEST FOR E-MAIL ID CREATION

TO
THE IT DEPARTMENT
MANJUSHREE TECHNOPACK LIMITED

REQUEST FOR E-MAIL ID CREATION

USER DETAILS		EMP ID:
First Name		
Last Name		
Display Name		
Suggested e-Mail ID		

User Category	☐ Employee	☐ Contract / Intern

ADDITIONAL DETAILS			
Company Name		Job Title/Designation	
Unit / Branch / Location		Date of Joining	
Department			
Reporting To		Mobile No.	

NEW LICENSE	☐ Office-365 Plan E1	☐ Office-365 Plan E3

REASSIGN LICENSE	(mention New mail id): Groups need to Add	
	Hand over Backup of deactivated mailbox to:	
	Action on deactivated mail id	☐ Delete the mail id ☐ Redirect the mails
	If we have to redirect, to which mail id?	
REMARKS		

Annexure – II	Requestor	CHRO	User Department Head	IT DEPT
Name		ANIL PATRO		NARESH KUMAR G
Date				
Signature				

FOR USE OF MAIL ADMINISTRATION TEAM					
CREATED BY		LICENCE TYPE		AD USER ID	

	Document No	MTL-2.0 02	Document Type	Form
Manjushree 2.0	Document Name	E-mail ID Creation	Version No	2.0

REQUEST FOR E-MAIL ID CREATION

POLICY ON E-MAIL USAGE

MTL E-mail Policy: -

As per MTL email provisioning policy, employees are advised to fill the Annexure – 1 (for an existing employee who do not have MTL official email id) and submit to IT for email id creation. For all the new employees, HR will initiate the process at the time of employee joining MTL organization.

- This Policy applies to all employees of the MTL and all MTL contractors, agents, suppliers, customers and any other persons who at any time use or have access to email or the Internet during the course of their employment or business dealings with the MTL Users.
- Provisioning of email ids to the employees subject to obtaining approval from respective HOD / Functional heads.
- As per MTL standard, email ids are to be created with "firstname.lastname@domain" to avoid confusions in identifying and ensuring the right contacts.
- All the employees are advised to follow the MTL defined email signatures to maintain standards and brand image of Manjushree Technopack.
- The MTL owns the IT components required to support the email system and Internet connectivity and provides the right to use these systems for legitimate business purposes only.
- Use of company provided computer system, email and Internet access are for business purposes, and are not private or confidential. No employee should have any expectation that any email or Internet communication he or she makes, regardless of its content, is private or confidential.
- The commercial and legal effects of sending and receiving emails or other electronic communication are the same as any other form of written communication. The style, tone and content of emails has a direct effect on the way the Company is perceived by others. Emails can contractually bind the Company and any advice, opinion, guarantee, representation, or other statement contained in an email can be relied upon by the Company's clients or other parties.
- All the emails sent from MTL employees will have disclaimer attached, and hence employees are advised to not to tamper or delete the disclaimer messages by any means.
- Users must not send emails or other electronic communication which make representations, contractual commitments or any other form of statement concerning the Company unless they have authority from the Company to do so.
- Users must be aware that the Company shall adopt an appropriate email retention policy in accordance with local legal requirements. Email and other electronic communication could be requested in the event of a legal proceeding through "e-discovery" efforts. Care is taken to preserve the integrity of archived email within the retention policy as well as destroyed once the appropriate retention period has expired.

USER COMPLIANCE

I,_____, understand and agree to abide by the e-Mail Usage Policy. I further understand that if I violate this policy, my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

Signature of the User

Manjushree 2.0	Document No	MTL-2.0 02	Document Type	Form
	Document Name	E-mail ID Creation	Version No	2.0

Annexure – 3

REQUEST FOR D365 ERP NAVISION

TO
THE IT DEPARTMENT
MANJUSHREE TECHNOPACK LIMITED.

D365 NAVISION ACCESS

The company is pleased to issue you a D365 ERP NAVISION ACCESS. This ID has been provided to you to carry out your official duties with convenience and the company expects you to hold full responsibility of this ID and take care of as if it is your own. Please read the below mentioned details carefully and sign.

USER DETAILS		EMP ID:	
Username			
User Category	☐ Employee	☐ Contract	
COMPANY NAME		Job Title/Designation	
Unit / Branch / Location			
Department		Mail ID:	
Reporting To		Mobile No.	

NOTE: - PERMISSION ARE GIVEN BY USER REPORTING MANAGER OR USER HOD

USER MODULE	PERMISSIONS
Finance Management Module	☐ YES ☐ NO
Payable	☐ YES ☐ NO
Receivable	☐ YES ☐ NO
Purchase Entry	☐ YES ☐ NO
General Ledger	☐ YES ☐ NO
Master approvar	☐ YES ☐ NO
Fixed Assets	☐ YES ☐ NO
Sales & Marketing module	☐ YES ☐ NO
Sales order Creation	☐ YES ☐ NO
Sales order Approver	☐ YES ☐ NO
Sales price Creation	☐ YES ☐ NO
Purchase Module	☐ YES ☐ NO
Purchase order Creation	☐ YES ☐ NO
Purchase order approver	☐ YES ☐ NO
Manufacturing /warehouse	☐ YES ☐ NO
Bom Approver	☐ YES ☐ NO
Production Data Entry (SFG)	☐ YES ☐ NO
PRODuction Data Entry (FG)	☐ YES ☐ NO
Material (store) Module	☐ YES ☐ NO
GRN Creation and Posting	☐ YES ☐ NO
Material Movement	☐ YES ☐ NO
Transfer order creation and post	☐ YES ☐ NO
QA Module	☐ YES ☐ NO
Qc approval	☐ YES ☐ NO
Indent module	☐ YES ☐ NO
Indent Creation	☐ YES ☐ NO
Indent Approver	☐ YES ☐ NO
Report viewer	☐ YES ☐ NO

Annexure – III	HOD	IT DEPT	CREATED BY
Name		NARESH KUMAR G	
Date			
Signature			

I,_____ , have read and understood the above terms and conditions on the acceptable usage of D365 ERP NAVISION ACCESS the required access and agree to abide by the same. I further understand that if I violate this policy, my privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

Signature of the User

Document No	MTL-2.0 03	Document Type	Form
Document Name	D365 ERP NAVISION ACCESS	Version No	2.0

Annexure – 4

VPN Access Request form

From

<Name of the Employee>

<Designation>, <Department>

<Location>

To

The IT Department

Manjushree Technopack Limited

Please approve the MTL VPN permission to the following employee to access MTL network, while he / she is away from office. I will ensure the VPN permission will be used only for official purpose and the assure you that the login credentials will not be shared to anyone else.

Sr.#	Employee ID	Name of the Employee	Purpose of VPN access (eg: Navision access or Other IT tools access or shared folder access)

Employee Signature / Date:

Approving HOD / Functional Head sign / Date:

CIO signature / Date:

Comments: Approved / Not Approved.