
Polyhose

Information Technology (“IT”) Policy

Applicability	Polyhose Group
	All Manufacturing Units under Polyhose Group

	IT Policy	Doc. No.	PH/L3/IT/004		
		Issue No.	01		
		Rev. No.	00	Date	05.04.2022
		Page No.	2 of 32		

DOCUMENT CONTROL

Author	Chief Information Officer
File Name	Polyhose IT Policy Document
Created	31 st Mar 2021
Last Edited	6 th April, 2022

Targeted Readership: All Stakeholders

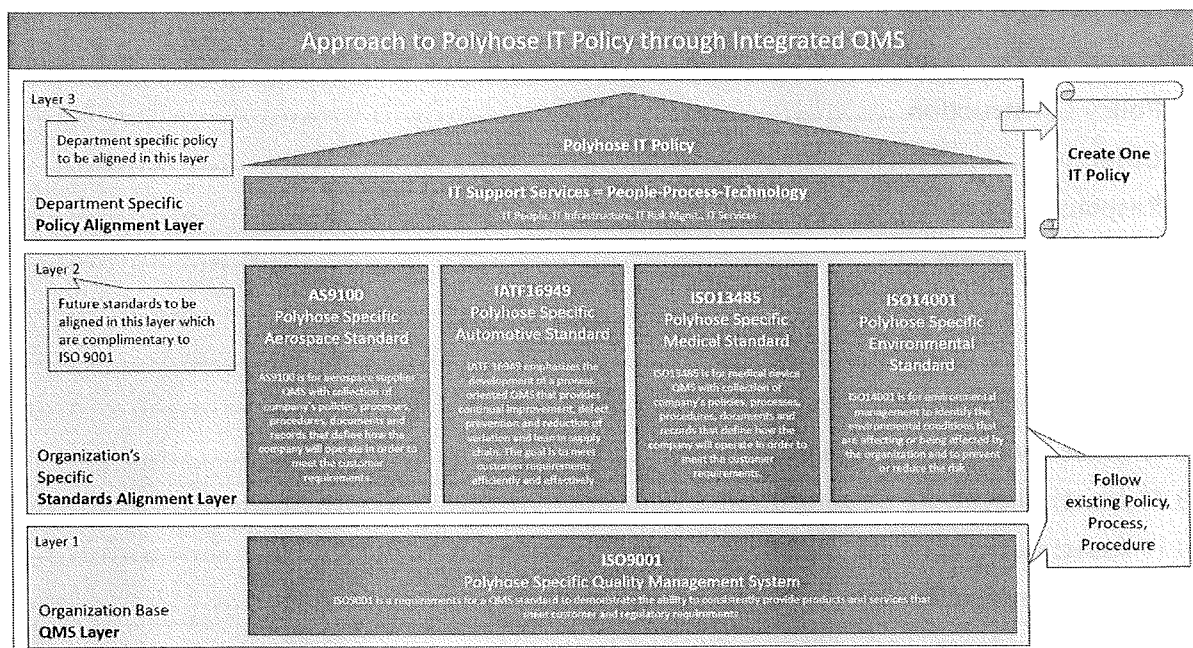
	IT Policy	Doc. No.		PH/L3/IT/004	
		Issue No.		01	
		Rev. No.	00	Date	05.04.2022
		Page No.	3 of 32		

Table of Contents

1. Introduction	4
1.1 Background.....	4
1.2 Policy Construction.....	4
1.3 Objectives	4
1.4 Responsibilities.....	5
1.5 Policy Awareness	5
1.6 Changes to the Policy	5
1.7 Enforcement	5
2.1 IT Asset Purchase	7
2.2 IT Asset Inventory Management	8
2.3 IT Asset: Allocation, De-allocation & Relocation	8
2.4 IT Asset: General Usage, Maintenance and Security	9
2.5 IT Asset Physical Security	10
2.6 IT Asset Incidents	10
2.7 IT Asset Loss	11
2.8 IT Asset Compensation.....	13
2.9 IT Assets Disposal	13
3.1 Hardware & Accessories.....	13
3.3 Networking.....	16
3.5 Internet	21
3.6 Cloud Computing.....	23
3.7 Digital Data.....	24
3.8 3 rd Party Tools.....	26
3.9 Information Security	26
4.Risk & Contingency Plan	28
4.1 Risk Mitigation.....	28
4.2 Contingency Plan	28
5. Data Retention & Destruction.....	27

Polyhose® Providing Flexible Solutions Globally	IT Policy	Doc. No.	PH/L3/IT/004		
		Issue No.	01		
		Rev. No.	00	Date	05.04.2022
		Page No.	4 of 32		

1. Introduction



1.1 Background

Polyhose provides and maintains technological products, services, and facilities like Personal Computers (PCs), peripheral equipment, servers (On-Premises & Cloud), telephones, Internet, and application software to its employees for official use and facilitate to enhance the management of its operations. Information management and information technology management are vital in the delivery of organization programs and, when planned and managed properly, would improve service delivery, increase productivity, and reduce costs to the organization.

1.2 Policy Construction

The construction and administration of information technology and security policies will enhance the performance of the organization in delivering, implementing, and maintaining Devices, software, hardware, and networks suitable to the organizational needs, as well as its collaborating organizations with which Polyhose shares information.

The policy defines the duties and responsibilities of the Polyhose Employees, who use IT Assets like Devices, Network, Software, and hardware systems in performance of their duties.

1.3 Objectives

The Polyhose policy document is developed to achieve the following objectives.

1. Provide a policy framework within which the organization can derive the maximum benefits from the use of information technology
2. Provide suitable hardware and software systems that guarantee information security, secure environment, and safe working practice in the operation of the equipment.
3. Ensure that users are aware of and fully comply with the Information Technology and Security policies, procedures, guidelines, standards, and relevant regulations to achieve best value in Information Technology provision.
4. Ensure that the organization plays an active and responsible part in the wider use of Information and Communications Technology.

	IT Policy		Doc. No.		PH/L3/IT/004	
			Issue No.		01	
			Rev. No.	00	Date	05.04.2022
			Page No.	5 of 32		

5. Ensure that all users understand their responsibilities in protecting the data and equipment that they handle.
6. Provide guidelines on IT Assets Purchase, Inventory Management, Allocation, De-allocation & Relocation, Maintenance / Upgrade, Loss/Damage, Disposal / Expiry, Usage, Risk/Contingency Plan, Staff Security, Infra Security, Network Security, Data Security, and IT Audit.
7. This policy applies to all Employees, Contractors, and Consultants, including all personnel affiliated with the organization whether at the company's On-Premises or Off-Premises.
8. The policies also apply to all equipment that is owned or leased by the organizations which are essential resources for accomplishing the organization's strategies and objectives. These resources are valuable IT assets to be used and managed responsibly to ensure their integrity, security, and availability for appropriate organizational activities.
9. Users must be aware of user rights and responsibilities, which outline liability for personal communication, privacy and security issues and consequences of violations.
10. The policy is to ensure the responsible use, availability, confidentiality, and integrity of Information Technology systems that support all the activities of the organization.
11. All authorized users of these resources are required to use them in an effective, efficient, and responsible manner.

1.4 Responsibilities

The IT General Manager shall be responsible for the following:

1. Initiating and drafting Information Technology Policy, IT Security Policy and IT Audit Policy and arrange to get the approval process from Technical Director.
2. Maintaining Information Technology policy in an up-to-date and in an accessible form.
3. Broadcast the Information Technology policy in an appropriate and accessible way.

Each Employee, Contractor, Consultants, and all personnel affiliated with the organization shall be responsible for the following:

- 1) Understanding and complying with Information Technology and IT Security policies.
- 2) Reporting to authorities any breach of the laid down policies

1.5 Policy Awareness

All Information technology and IT Security policies, guidelines, procedures, and standards, will be made freely available electronically on the company's intranet or share folder to all Employees and will form the up-to-date official version.

1.6 Changes to the Policy

The normal process for changing Information Technology Policy will be based on request to be made to the IT department who will arrange for review of the requested changes with the IT General Manager and thereafter the Technical Director and approval from him. After approval, the Information policy will change and be published on the CORE WebPortal/Intranet/Share Folder. In the event of a need for urgent change, this may be approved by the Technical Director and update to be done to the document accordingly to publish.

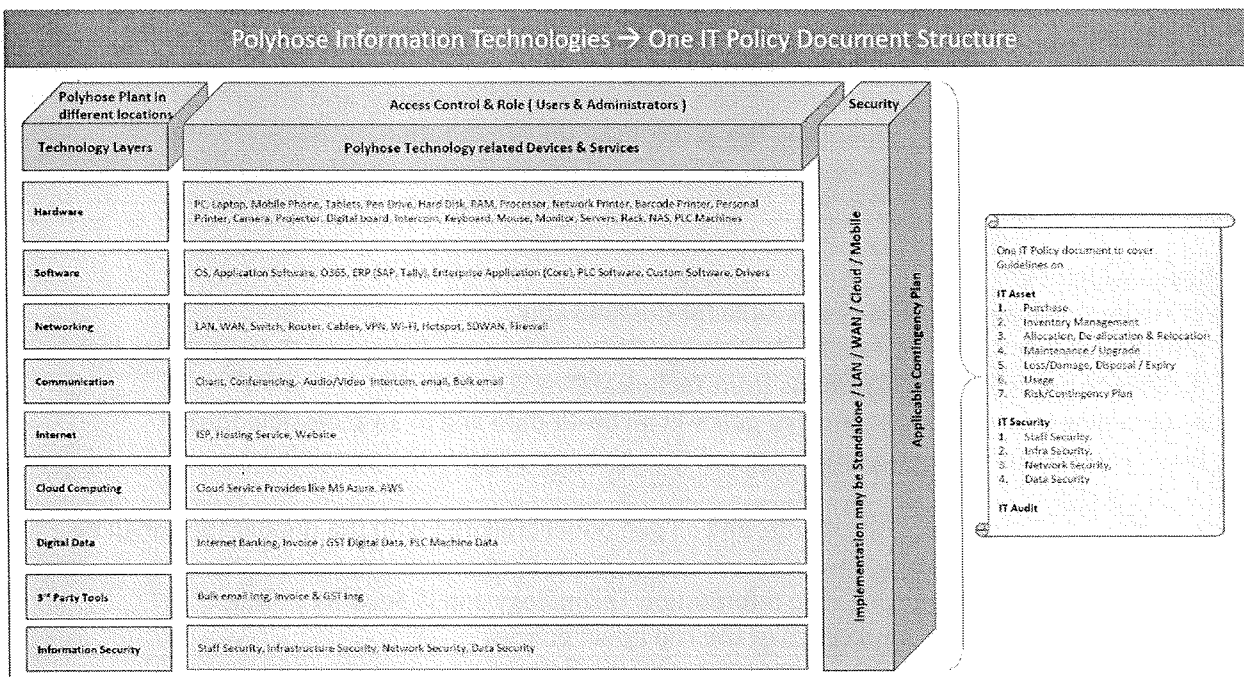
1.7 Enforcement

The IT Support Team and the respective department coordinators shall conduct quarterly audits to ensure that the policies are followed. Disciplinary action shall be taken against those who violate the regulations according to the decision that shall be arrived at by the Human Resources department in consultation with the IT Department and respective department coordinator.

Classification of offences and penalties:

- Minor** : Issues which can happen due to ignorance of IT Policy
- Example** : Unauthorized repair of IT Assets
- Penalty** : Issuance of Warning letter
- Major** : Offences which occur due to deliberate negligence of the IT policy guidelines
- Example** : Vandalizing or Losing IT property
- Penalty** : Payment of a fine
- Serious** : Very serious offences committed deliberately to sabotage organization operations.
- Example** : Hacking into the server, Deliberate deletion of data
- Penalty** : Termination of contract

Polyhose Information Technologies → One IT Policy Document Structure



	IT Policy		Doc. No.		PH/L3/IT/004	
			Issue No.		01	
			Rev. No.	00	Date	05.04.2022
			Page No.	7 of 32		

2. IT Assets Policy Objective

The IT asset usage policy informs employees and managers about equipment purchase/rental/managed service/cloud services, organizational and project-level inventory management, rules for allocating & transferring equipment to employees, departments or projects and best practices from purchase to retirement/expiry stages of an IT Asset.

2.1 IT Asset Purchase

- 1) The Purchase Dept. procedures & guidelines need to be followed to purchase new IT Assets, Services, Software for official purposes.
- 2) All approved IT Assets, Services, Software will be purchased through the Purchase Dept., unless informed/permited otherwise.
- 3) IT Dept. will assist the Purchase Dept. while evaluating best and most cost-effective hardware or software or IT Services to be purchased for a particular dept./project/purpose based on the requirement. The IT Dept. will also make sure all hardware/software standards defined in the IT Policy are enforced during such purchases.
- 4) The IT Dept. will maintain a small inventory of essential and frequently replaced IT assets (Mouse, Keyboard, Monitor, LAN Cables) to minimize delay in fulfilling critical orders.
- 5) The following IT Assets are Purchased / Rental / Managed Service/ Cloud Service by the organization and provided to employees, departments, or projects for their official use. The list is not limited to the following and can be included later.

S. No	Technology	Devices/Services
1)	Hardware & Accessories	PC, Laptop, Mobile Phone, Tablets, Network Printer, Barcode Printer, Personal Printer, Camera, Projector, Digital board, Intercom, Servers, Rack, NAS, PLC Machines, Biometric Devices Accessories: Pen Drive, Hard Disk, RAM, Processor, Keyboard, Mouse, Monitor
2)	Software	OS, Application Software, O365, ERP (SAP, Tally), Enterprise Application (Core), PLC Software, Custom Software, Drivers
3)	Networking	LAN, WAN, Switch, Router, Cables, VPN, Wi-Fi, Hotspot, SDWAN, Firewall
4)	Communication	Chant, Conferencing, - Audio/Video, Intercom, email, Bulk email
5)	Internet	ISP, Hosting Service, Website
6)	Cloud Computing	Cloud Service Provides like MS Azure, AWS
7)	Digital Data	Internet Banking, Invoice, GST Digital Data, PLC Machine Data
8)	3 rd Party Tools	Bulk email Integration, Invoice & GST Integration
9)	Information Security	Staff Security, Infrastructure Security, Network Security, Data Security

	IT Policy	Doc. No.		PH/L3/IT/004	
		Issue No.		01	
		Rev. No.	00	Date	05.04.2022
		Page No.	8 of 32		

2.2 IT Asset Inventory Management

- 1) The IT Dept. is responsible for maintaining an accurate inventory of all IT Assets Software and tangible IT assets purchased by the organization.

The following information is to be maintained for above mentioned assets in an Inventory Sheet:

Tangible IT assets

- 1) Item
- 2) Brand/ Company Name
- 3) Serial Number
- 4) Make/Model
- 5) Asset ID
- 6) Basic Configuration (RAM/HDD/Processor)
- 7) Warranty Details
- 8) Supplier
- 9) Physical Location
- 10) Date of Purchase
- 11) Purchase Cost
- 12) Cost Centre
- 13) Current Person In-Charge

IT Services

- 1) Service Name
- 2) Account Number
- 3) Plan
- 4) Validity Period
- 5) License
- 6) Configuration
- 7) Credentials
- 8) Support In-Charge

- 2) Proper information about all IT Assets provided to a specific department, project must be regularly maintained in their respective Inventory Sheets by an assigned coordinator from that dept., project on a regular basis. The information thus maintained must be shared with the Purchase Dept. and IT department as and when requested.
- 3) When an Inventory Sheet is updated or modified, the previous version of the document should be retained. The date of modification should be mentioned in the sheet.
- 4) All technological assets of the organization must be physically tagged with Codes / Bar Code / QR Code for easy identification. The codes can have essential attributes from servicing point of view.
- 5) The purchased items to be accounted against the cost centre code and current location may vary.
- 6) Periodic inventory audits will be carried out by the IT Dept. to validate the inventory and make sure all assets are up-to-date and in proper working condition as required for maximum efficiency and productivity.
- 7) The critical IT asset used by the users to be maintained in Active Directory under description attribute like IT Assets Code, SAP License, O365 Licence, Department Code, Warranty, Config, Serial Number, Make/Model, Brand, Cost Centre.

2.3 IT Asset: Allocation, De-allocation & Relocation

- 1) Allocation of IT Assets to Users:

- a) New Employees may be allocated a personal computer (desktop or laptop) for office work on the Day of Joining, as per work requirement.
- b) The HR Department to send the request 1 Week in advance so that the machine can be made ready with required software and access.

	IT Policy	Doc. No.		PH/L3/IT/004	
		Issue No.		01	
		Rev. No.	00	Date	05.04.2022
		Page No.	9 of 32		

- c) If required, employees can request their Reporting Manager(s) for additional equipment or supplies like external keyboard, mouse etc.
- d) Allocation of additional assets to an employee is at the sole discretion of the Reporting Manager(s).
- e) No employee is allowed to carry official electronic devices out of office without permission from Reporting Manager.
- 1) Allocation of IT Assets to Department use:
 - a) IT asset may be allocated for department use based on approval from TD for the purchase request or from the inventory.
 - b) The request to raised by the IT Team based on the need.
- 3) De-allocation of IT Assets to Users:
 - a) It is the Reporting Manager's responsibility to collect all allocated organizational equipment & other assets from an employee who is leaving the organization.
 - b) Updating the Inventory Sheet is mandatory after receiving back all allocated equipment.
 - c) The received assets must be returned to the IT Department.
- 4) De-allocation of IT Assets from department:
 - a) IT Team will identify the reason for the de-allocation of IT asset and proceed with approval from TD.
 - b) The de-allocated IT asset assigned for the department may be re-allocated or scraped based on the need, repair, respectively.

2.4 IT Asset: General Usage, Maintenance and Security

- 1) It is the responsibility of all employees to ensure careful, safe, and judicious use of the equipment & other assets allocated to and/or being used by them.
- 2) Proper guidelines or safety information must be taken from designated IT Support Team before operating any equipment for the first time.
- 3) Any observed malfunction, error, fault, or problem while operating any equipment owned by the organization or assigned to you must be immediately informed to the designated staff in IT Dept.
- 4) Any repeated occurrences of improper or careless use, wastage of supplies or any such offense compromising the safety or health of the equipment and people using them will be subject to disciplinary action.
- 5) If your assigned computing device is malfunctioning or underperforming and needs to be replaced or repaired, then written approval from your Reporting Manager is required for the same. The malfunctioning device needs to be submitted to the IT Dept. for checking, maintenance, or repair. The IT Dept. staff person will validate and give a time estimate for repair/maintenance.
- 6) The Reporting Manager can be informed about excessive delay or dissatisfaction about the repair or maintenance performed by the IT Dept. The issue will then be resolved by the Reporting Manager in consultation with the IT Dept. Head. TD to be consulted in terms of serious disputes or unresolved issues.
- 7) It is the responsibility of the user to ensure that device is kept in good condition. This means that the assigned staff member must keep the device cool, dust-free, protected from any liquid.
- 8) Laptop maintenance shall be done every six months and is the responsibility of the IT team. Maintenance includes cleaning the cache, temporary files, virus, and malware scans, deleting unused programs and conducting performance benchmarks.
- 9) If an electronic device requires repair, the staff member must alert the IT Team promptly, who will then forward it for repair through warranty / repair process.

	IT Policy		Doc. No.		PH/L3/IT/004	
			Issue No.		01	
			Rev. No.	00	Date	05.04.2022
			Page No.	10 of 32		

2.5 IT Asset Physical Security

- 1) Physical security measures are steps that Polyhose will take to manage physical access to an information resource. Polyhose considers physical security as the first line of defence against theft, sabotage, and natural disasters. Examples of measures that Polyhose will undertake include restrictions on entry to equipment areas, locking, disabling, or disconnecting equipment.
- 2) To ensure protection of all information assets the information technology department shall maintain an inventory of information systems. This inventory should indicate all existing hardware software, databases, and data communication links.
- 3) Everyone that is granted access rights to an Information Resources must receive emergency procedures training for the resource where and when necessary.
- 4) Requests for access must come from the applicable information systems officer.

2.6 IT Asset Incidents

This section applies to all Employees of the Polyhose, contractual third parties and agents of Polyhose who use Polyhose IT facilities and equipment, or have access to, or custody of Polyhose devices. All users must understand and adopt use of this policy and are responsible for ensuring the safety and security of the Polyhose systems and the information that they use or manipulate.

An Information Security Incident includes, but is not restricted to, the following:

- 1) The loss or theft of data or information.
- 2) The transfer of data or information to those who are not entitled to receive that information.
- 3) Attempts (either failed or successful) to gain unauthorized access to data or information storage or a computer system.
- 4) Changes to information or data or system hardware, firmware, or software characteristics without Polyhose knowledge, instruction, or consent.
- 5) Unwanted disruption or denial of service to a system.
- 6) The unauthorized use of a system for the processing or storage of data by any person.

Incident Response Team

Any Incident noticed by the Stakeholder shall be escalated to the IT Helpdesk. Help desk shall act as the triage team or first point of contact for incident reporting by end users.

A designated team for Incident handling may be invoked using domain (Network, Windows, Unix etc) experts from Network and system administration Team, under the leadership of IT Manager.

Depending on the type of security incident, the members of a Security Incident Team can include from any of the following;

Change Control Team

- IT Engineer
- System/IT Administrator
- CIO

	IT Policy		Doc. No.		PH/L3/IT/004	
			Issue No.		01	
			Rev. No.	00	Date	05.04.2022
			Page No.	11 of 32		

Incident handling procedures:

The Incident handling procedure shall cover:

- Incident Categorization and Prioritization
- Analysis and identification of the cause of the incident.
- Initial containment of the Incident Eradication and Recovery.
- Collection of audit trails and similar evidence.
- Communication with those affected by or involved with recovery from the incident.
- Follow up and Documentation.

Incident Follow-up:

- A summary record of each incident shall be maintained by Network Administration Team.
- A summary report of all security incidents shall be submitted to Management on regular Interval.

Change Request

Change Requests maybe initiated by any “key” application user or the application owner within the IT Department. “Key” application user is defined as process lead, module lead, Departmental Head and CIO.

All Change Request must come either in Change Request in Helpdesk or on Mail having proper justification for defined but not limited to following parameters

- Change Request in specific Applications, Modules, Business Process, Business Sub-process
- Change Request Description
- Change Request Need
- Business Impact / Benefits
- Financial Impact
- Change Category
- Priority

Change Requests shall be processed based on prior approval from the change Control Team.

- All change Requests shall be analyzed from the perspective of business impact in terms of time and efforts as well as security considerations.
- Emergency change requests can be authorized by the Management.
- Impact Analysis
- Potential impact of any change on other applications or systems, or on other modules in the same application shall be assessed from risk perspective before accepting a change request.

2.7 IT Asset Loss

Polyhose invests a lot of financial resources in the purchase, distribution, and maintenance of Information system equipment. All employees allocated Polyhose IT assets must take utmost good care of the property failure to which a corrective measure may be taken. The IT support in the

	IT Policy		Doc. No.		PH/L3/IT/004	
			Issue No.		01	
			Rev. No.	00	Date	05.04.2022
			Page No.	12 of 32		

respective plant is responsible for the overall quality and security of equipment in areas they manage.

In the event of asset loss due to situations beyond the employees' control such as theft, fire damage or any other accidental occurrence the employee should:

- 1) Report the incidence to a police station
- 2) Fill a form indicating the information about the incidence
- 3) Submit a written report to the procurement department, the IT support coordinator in charge and the information technology department together with a copy of the incident report form.

2.8 IT Asset Compensation

In the event of loss of Polyhose IT asset due to employee negligence the following compensation shall be effective within an agreed period:

- 1) X1% (approx. 75%) purchase price for all equipment less than 1 year old.
- 2) X2% (approx. 50%) purchase price for all equipment more than 1 year old but less than 2 years old.
- 3) X3% (approx. 25%) purchase price for all equipment more than 2 years old.

2.9 IT Assets Disposal

- 1) The IT Department to identify the disposal items and in consultation with purchase department shall determine the appropriate time, equipment to be disposed.
- 2) All IT asset which are not in use, have expired or damaged beyond repair shall be returned to IT department for safe storage and inventory keeping.
- 3) All Polyhose staff upon completion of their contract are required to submit the IT Assets under their care to the IT Department as part of the exit clearance process.
- 4) The disposal of hardware by destruction may only be carried out with the approval of the IT manager and purchase manager.
- 5) Approval of destruction of IT asset to be created by the IT Manager and the hardware will be disposed of according to the current WEEE (Waste Electrical and Electronic Equipment) regulations.
- 6) These regulations ensure environmental conservation through the efficient, safe, and conservative disposal of electronic waste.

3.0 IT Asset Usage Policy Objective

The main aim of this policy is to provide guidelines in using the IT assets by the employees, so that it helps in trouble shooting.

3.1 Hardware & Accessories

The Hardware & Accessories Usage Policy is defined to provide guidelines for appropriate installation, usage and maintenance of hardware products installed in organization.

IT Assets	Guidelines
Hardware: PC, Laptop, Mobile Phone, Tablets, Network Printer, Barcode Printer, Personal Printer, Projector, Digital board, Intercom, Biometric Devices	1. It is the responsibility of the IT Dept. to establish and maintain standard configurations of hardware owned by the organization. The standard, can however, be modified at any point in time as required by the IT Dept. Head in consultation with TD. 2. Multiple configurations are maintained as per the different requirements of various departments and projects in the organization, in consultation with the Dept./Project Head. 3. Only in exceptional cases, when none of the standard configurations satisfy the work requirements, can an employee request a non-standard configuration. Valid reasons need to be provided for the request and written approval of the Reporting Manager(s) is required for the same.
Accessories: Pen Drive, Hard Disk, RAM, Processor,	4. The accessories can be purchase based on the need basis when the item is not in a usable condition and no spare available to support the operations. 5. The major hardware purchase to be processed through Purchase & TD.

	IT Policy	Doc. No.		PH/L3/IT/004	
		Issue No.		01	
		Rev. No.	00	Date	05.04.2022
		Page No.		14 of 32	

Keyboard, Mouse, Monitor	
Camera	1. All cameras being used in the respective plant are enabled to connect to the organization's Local Area Network as well as the Internet. 2. Network security is enabled in all PCs through Firewall, Web Security and Email Security software. 3. The cameras to be connected to storage and to be retained for 30 days. 4. Only specific employees and IT Support will have access to camera and on approval from TD.
Servers, Rack, NAS	1. Servers, racks, NAS to be managed by IT support 2. Access to these devices will be to IT Support and only through them other support people like EB, AC or other maintenance to be accessed.
PLC Machines	1. PLC Machines will be managed by the respective department 2. The PLC Machines will be in a different network and not part of the regular LAN 3. There will not any internet support to this LAN. 4. Only on request during the time of technical support the internet will be provided to the designated machine for the specified time.

3.2 Software

The Software Usage Policy is defined to provide guidelines for appropriate installation, usage and maintenance of software products installed in organization.

IT Assets	Guidelines
General Guidelines	1. Third-party software (free as well as purchased) required for day-to-day work will be preinstalled onto all company systems before handing them over to employees. A designated person in the IT Dept. can be contacted to add to/delete from the list of pre-installed software on organizational computers. 2. No other third-party software – free or licensed can be installed onto a computer system owned or provided to an employee by the organization, without prior approval of the IT Dept. 3. To request installation of software onto a personal computing device, an employee needs to send a written request via the IT Ticket System or IT Support Email. Any software developed & copyrighted by the organization belongs to the organization. Any unauthorized use, storage, duplication, or distribution of such software is illegal and subject to strict disciplinary action.
Software acquisition	1. When software for use by the Polyhose is being procured/developed there must be an assessment of whether the software incorporates adequate security controls for its intended purpose. 2. It must be investigated and considered whether proposed new software or upgrades are known to have outstanding security vulnerabilities or issues. 3. During procurement of software, the purchase policy will apply, and it may be important to have assurance that manufacturers will provide updates to correct any serious security vulnerabilities discovered in future.

IT Assets	Guidelines
Software development and Ownership	1. All software acquired for or on behalf of the organization or developed by company employees or contract personnel on behalf of the organization shall always remain organization property. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements. 2. Software developed at Polyhose must be assessed by the IS team for its potential to introduce information security risks and any such risks must be adequately addressed. 3. Upgrades or other changes to locally developed software must be assessed by the IS team for any risks to information security.
Software installation, regulation, and usage	1. For each item of software owned and managed by the organization a master copy of any media, enabling codes and installation instruction must be stored safely in accordance with the organizational procedures. 2. Use of illegal software and using software for illegal activities could be construed to be gross misconduct. 3. Use of software which tests or attempts to break Polyhose system or network security is prohibited unless the Network Administrators have been notified and given authorization for the purpose of penetration testing. 4. Use of software which causes operational problems to the network platforms, or which makes demands on resources which are excessive or cannot be justified is prohibited. 5. Software that is known to be causing a serious security problem, which cannot be adequately mitigated, should be removed from service. 6. When decommissioning a computer system, for disposal or re-use, appropriate measures must be taken in relation to any software and data stored on it.
Compliance	1. No employee is allowed to install pirated software on official computing systems. 2. Software purchased by the organization or installed on organizational computer systems must be used within the terms of its license agreement. 3. Any duplication, illegal reproduction, or unauthorized creation, use and distribution of licensed software within or outside the organization is strictly prohibited. Any such act will be subject to strict disciplinary action. 4. The Purchase Dept. procedures & guidelines need to be followed to purchase new software (commercial or shareware) for official purposes. All approved software will be purchased through the Purchase Dept., unless informed/permitted otherwise. 5. Any employee who notices misuse or improper use of software within the organization must inform his/her Reporting Manager(s).
Software Registration	1. Software licensed or purchased by the organization must be registered in the name of the organization with the Job Role or Department in which it will be used and not in the name of an individual. 2. After proper registration, the software may be installed as per the Software Usage Policy of the organization. A copy of all license agreements must be maintained by the IT Dept.

IT Assets	Guidelines
	3. After installation, all original installation media (CDs, DVDs, etc.) must be safely stored in a designated location by the IT Dept.
Software Audit	1. The IT Dept. will conduct periodic audit of software installed in all company-owned systems to make sure all compliances are being met. 2. Prior notice may or may not be provided by the IT Dept. before conducting the Software Audit. 3. During this audit, the IT Dept. will also make sure the anti-virus is updated, the system is scanned and cleaned, and the computer is free of garbage data, viruses, worms, or other harmful programmatic codes. 4. The full cooperation of all employees is required during such audits.
Data Backup Procedure	1. Data Backup is setup automatic by configuring OneDrive and placing all the folder inside the One Drive. In this way there is no need to worry about data loss and can be accessed from anywhere and from any machine. 2. File Backup System: • Organization will be having NAS storage for the department specific files and this will be backed up in OneDrive. • Respective people and IT Support admin will have access to that data. 3. All employees will login to the domain server through polyhose Employee ID and password.
Antivirus Software	1. Approved licensed antivirus software to be installed on all PCs owned by the organization. 2. Employees are expected to make sure their Antivirus is updated regularly. The IT Dept. should be informed if the Antivirus expires. 3. Any external storage device like pen drive or hard disk is only for the specific person and based on TD approval and rest will have external data transfer disabled policy. 4. Any external storage device like pen drive or hard disk connected to the PC needs to be completely scanned by the Antivirus software before opening it and copying files to/from the device.

3.3 Networking

The Networking Policy is defined to provide guidelines for appropriate installation, filtering, blocking, usage and maintenance of products installed in organization or in cloud or managed through managed service provider to protect the systems from unauthorized access and prevent damages.

IT Assets	Guidelines
General Guidelines	1) All PCs being used in the organization are enabled to connect to the organization's Local Area Network as well as the Internet. 2) Network security is enabled in all Client Machines through Firewall/SDWAN, Web Security, Domain Authentication, SSO to O365 and Endpoint security. 3) The PLC machines and related clients will be in a separate LAN within the premises and internet will be provide only during the time of technical support on request.
Network Security: LAN, WAN, Switch, Router, VPN, Wi-Fi,	1) Relocation, changes and other reconfigurations of network access points and devices will only be carried out by network Administrators according to procedures laid down by them.

IT Assets	Guidelines
Hotspot, SDWAN, Firewall	- The implementation of new equipment or upgraded network software or hardware must be carefully planned tested and managed by the IT Support team. - If the Network working service are managed service like MS Azure, SDWAN, Cloud Wi-Fi, ISP then network administrator along with managed service supplier the implementation, changes, maintenance/version upgrade will be carried out at a suitable time without/minimal impact to operations.
Network design and configuration policy	- The network must be designed and configured to deliver levels of performance, security, and reliability suitable for the Polyhose organizational needs, with high degree of control over access. - Access controls and routing should be used to prevent unauthorized access to network resources and unnecessary traffic flows between domains. - Appropriately configured firewalls should be used to help protect the Polyhose critical systems. - No changes to the network infrastructure, such as the introduction of a router or switch, may be undertaken without approval in advance by the Network administrator.
Access Control	- Access to the network, servers and systems in the organization will be achieved by individual logins and will require authentication. Authentication includes the use of passwords, biometrics, or other recognized forms of authentication. - All users of systems which contain high or medium risk data must have a strong password as defined in the IT Policy. - Default passwords on all systems must be changed after installation. - Where possible and financially feasible, more than one person must have full rights to any organization-owned server storing or transmitting high risk and medium risk data.
Virus Prevention	- Virus prevention for personal computers and email usage has been described previously. - Apart from that, all servers and workstations that connect to the network must be protected with licensed anti-virus software recommended by the vendor. The software must be kept up to date. - Whenever feasible, system/network administrators must inform users when a virus/ other vulnerability has been detected in the network or systems.
Intrusion Detection	- Intrusion detection must be implemented on all servers and workstations containing high and medium risk data. - Operating system and application software logging process must be enabled on all systems. - Server, firewall and critical system logs must be reviewed frequently.
Connecting devices to the network	- Privately owned network devices may only be connected to the Polyhose network in special circumstances approved by the Network administrator. - All devices whether privately owned, or owned by other organizations, must meet Polyhose network connection standards and their usage must conform to Polyhose Security policy - Network administrators have the right to inspect the configuration, test security and monitor network traffic for all devices connected to Polyhose Networks in accordance with normal operational network management procedures.

IT Assets	Guidelines
	- Every device connected to the network must be associated with a contactable person responsible for its administration and must be actively maintained. - Where applicable, network devices should have current and automatically updated anti-virus software installed. Employees in possession of devices should alert the system administrator 3 months in advance if any of the installed software is near expiry. - As a default all ports should be closed unless specifically opened.
Network termination or restrictions	- The organization shall terminate or restrict the network connection without notice whenever a LAN, a network device or a user poses any security risk to the company network equipment, software, and data. - If there is any doubt as to whether some intended usage of the network is permitted, or could significantly impact performance of the network, then advice should be sought from the Network Administrator before proceeding. - Network monitors and similar devices which allow the inspection of network traffic must not be used without the prior approval of the network administrator.

3.4 Communication

This policy provides information about acceptable usage, ownership, confidentiality, and security while using electronic messaging systems and chat platforms provided or approved by the organization. The policy applies to all electronic messages sent or received via the above-mentioned messaging systems and chat platforms by all official employees of the organization.

IT Assets	Guidelines
Phone Usage	- Landline phone systems are installed to communicate internally with other employees and make external official calls. - The landline phones should be strictly used to conduct official work only. As far as possible, no personal calls should be made using landline phones owned by the organization. - Long distance calls should be made after careful consideration since they incur significant costs to the organization. - The IT. Dept. is responsible for maintaining telephone connections in offices. For any problems related to telephones, they should be contacted. - Employees should remember to follow telephone etiquette and be courteous while representing themselves and the organization using the organization's phone services.
General Guidelines: email, chat, Audio/Video	- The organization reserves the right to approve or disapprove which electronic messaging systems and chat platforms would be used for official purposes. It is strictly advised to use the pre-approved messaging systems and platforms for office use only. - An employee who, upon joining the organization, is provided with an official email address should use it for official purposes only. - Any email security breach must be notified to the IT Dept. immediately. - Upon termination, resignation or retirement from the organization, the organization will deny all access to electronic messaging platforms owned/provided by the organization.

IT Assets	Guidelines
	5) All messages composed and/or sent using the pre-approved messaging systems and platforms need to comply with the company policies of acceptable communication. 6) Electronic mails and messages should be sent after careful consideration since they are inadequate in conveying the mood and context of the situation or sender and might be interpreted wrongly. 7) All email signatures must have appropriate designations of employees and must be in the format approved by the Management Committee.
Ownership	1) The official electronic messaging system used by the organization is the property of the organization and not the employee. All emails, chats and electronic messages stored, composed, sent and received by any employee or non-employee in the official electronic messaging systems are the property of the organization. 2) The organization reserves the right to intercept, monitor, read and disclose any messages stored, composed, sent or received using the official electronic messaging systems. 3) The organization reserves the right to alter, modify, re-route or block messages as deemed appropriate. 4) IT Administrator can change the email system password and monitor email usage of any employee for security purposes.
Confidentiality	1) Proprietary, confidential, and sensitive information about the organization or its employees should not be exchanged via electronic messaging systems unless pre-approved by the Reporting Manager(s) and/or the Management Committee. 2) Caution and proper judgment should be used to decide whether to deliver a message in person, on phone or via email/electronic messaging systems. 3) Before composing or sending any message, it should be noted that electronic messages can be used as evidence in a court of law. 4) Unauthorized copying and distributing of copyrighted content of the organization is prohibited.
Email Security	1) Anti-Virus: a) Anti-virus software pre-approved by the Dept. Head - IT should be installed in the laptop/desktop provided to a new employee after joining the organization. b) All employees in the organization are expected to make sure they have anti-virus software installed in their laptops/desktops (personal or official) used for office work. c) Organization will bear responsibility for providing, installing, updating and maintaining records for one anti-virus per employee at a time for the official laptop provided by the organization. The employee is responsible for installing good quality anti-virus software in their personal laptop/desktop used for office work. d) Employees are prohibited from disabling the anti-virus software on organization provided laptops/desktops. e) Employees should make sure their anti-virus is regularly updated and not out of date. 2) Safe Email Usage: Following precautions must be taken to maintain email security:

IT Policy

Doc. No.	PH/L3/IT/004		
Issue No.	01		
Rev. No.	00	Date	05.04.2022
Page No.	20 of 32		

IT Assets	Guidelines
	- Do not to open emails and/or attachments from unknown or suspicious sources unless anticipated by you. - In case of doubts about emails/ attachments from known senders, confirm from them about the legitimacy of the email/attachment. - Use Email spam filters to filter out spam emails.
Inappropriate Use	- Official Email platforms or electronic messaging systems including but not limited to chat platforms and instant messaging systems should not be used to send messages containing pornographic, defamatory, derogatory, sexual, racist, harassing or offensive material. - Official Email platforms or electronic messaging systems should not be used for personal work, personal gain or the promotion or publication of one's religious, social or political views. - Spam/ bulk/junk messages should not be forwarded or sent to anyone from the official email ID unless for an officially approved purpose.
Email Usage	- All messages composed, sent, or received on the electronic mail system are and remain the property of Polyhose. They are not the private property of any employee. - The use of the electronic mail system is reserved solely for the conduct of business at Polyhose. It may not be used for personal business. Occasional personal use, which does not interfere with the employee's job performance, is acceptable, but such use remains subject to all provisions of this policy. Employees are advised to create a separate e-mail address for personal communications. - The electronic mail system may not be used to solicit for commercial ventures or political or religious causes, outside organizations, or other non-job-related solicitations. - The electronic mail system is not to be used to create, send, or forward messages which are indecent, pornographic, offensive, harassing, threatening, contain racial or sexual insults, or which are otherwise inappropriate in the context of the organization's ethos and core values. - Chain Letters would be regarded as inappropriate electronic mail. - The electronic mail system shall not be used to violate copyrights or other proprietary rights by distributing unauthorized copies of materials owned by others, nor shall it be used to distribute confidential or proprietary Polyhose materials without proper authorization. - The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality. - The attachment of data files to a mail shall only be permitted after confirming the classification of the information being sent and then having scanned and verified the file for the possibility of a virus or other malicious code. - Incoming e-mail shall be treated with the utmost care due to its inherent Information Security risks. The opening of e-mail with file attachments is not permitted unless such attachments have already been scanned for possible viruses or other malicious code.

3.5 Internet

The Internet Usage Policy provides guidelines for acceptable use of the organization's Internet network to devote Internet usage to enhance work productivity and efficiency and ensure safety and security of the Internet network, organizational data, and the employees.

IT Assets	Guidelines
Internet Access	Internet connectivity, maintenance and fair usage auditing are the roles of the network administrator. It is the responsibility of internet users to ensure compliance with this policy and to exercise their own best judgment on the matter when using the internet. Setting up Internet Access: The network administrator is responsible for setting up Internet access are to ensure that the company's network is safeguarded from malicious external intrusion by deploying, as a minimum, a configured anti-virus program. Downloading Files and Information from the Internet: Great care must be taken when downloading information and files from the Internet to safeguard against both malicious code and inappropriate material. Internet users are encouraged to download only the material which has direct program relevance and only from trusted websites. Using Internet for Work Purposes: The network administrator is responsible for controlling user access to the Internet, as well as for ensuring that users are aware of the threats, and trained in the safeguards, to reduce the risk of Information Security incidents. The network administrator shall implement restrictions on network equipment to block access to sites deemed inappropriate Giving Information when Ordering Goods on Internet: Employees authorized to make online payment for goods ordered on the Internet, are responsible for its safety and appropriate use. Filtering Inappropriate Material from the Internet: The Organization shall use software filters and other techniques whenever possible to restrict access to inappropriate information on the Internet by Employees. - The network administrator has the right to utilize software that makes it possible to identify and block access to Internet sites containing explicit or other material deemed inappropriate in the workplace.
General Internet Guidelines	- Internet is a paid resource and therefore shall be used only for office work. - The organization reserves the right to monitor, examine, block, or delete any/all incoming or outgoing internet connections on the organization's network. - The organization has systems in place to monitor and record all Internet usage on the organization's network including each website visit, and each email sent or received. The Management Committee can choose to analyse Internet usage and publicize the data at any time to assure Internet usage is as per the IT Policy. - The organization has installed an Internet Firewall to assure safety and security of the organizational network. Any employee who attempts to disable, defeat, or circumvent the Firewall will be subject to strict disciplinary action. - All employees will be responsible for their internet usage.

IT Assets	Guidelines
	6) Username to login will be employee ID and IT Dept., will provide the password and access based on the request from HR Dept. 7) Sharing the Username and Password with another employee, visitor or guest user is prohibited. 8) A visitor or guest user who wants to use the office Internet will be given a Guest Username and Password. 9) The IT Dept. will define guidelines for issuing new passwords or allowing employees to modify their own passwords. 10) Any password security breach must be notified to the IT Dept. immediately. 11) Username and password allotted to an employee will be deleted upon resignation/ termination/ retirement from the organization.
Online Content Usage Guidelines	1) Employees are solely responsible for the content accessed and downloaded using Internet facility in the office. If they accidentally connect to a website containing material prohibited by the organization, they should disconnect from that site immediately. 2) During office hours, employees are expected to spend limited time to access news, social media and other websites online, unless explicitly required for office work. 3) Employees are not allowed to use Internet for non-official purposes using the Internet facility in office. 4) Employees should schedule bandwidth-intensive tasks like large file transfers, video downloads, mass e-mailing etc. for off-peak times or only from a designated machine.
Inappropriate Use	The following activities are prohibited on organization's Internet network. This list can be modified/updated anytime by the Management Committee as deemed fit. Any disciplinary action considered appropriate by the Management Committee (including legal action or termination) can be taken against an employee involved in the activities mentioned below: 1) Playing online games, downloading and/or watching games, videos or entertainment software or engaging in any online activity which compromises the network speed and consumes unnecessary Internet bandwidth 2) Downloading images, videos and documents unless required to official work 3) Accessing, displaying, uploading, downloading, storing, recording, or distributing any kind of pornographic or sexually explicit material unless explicitly required for office work 4) Accessing pirated software, tools or data using the official network or systems 5) Uploading or distributing software, documents or any other material owned by the organization online without the explicit permission of the Management Committee 6) Engaging in any criminal or illegal activity or violating law 7) Invading privacy of co-workers 8) Using the Internet for personal financial gain or for conducting personal business 9) Deliberately engaging in an online activity which hampers the safety & security of the data, equipment and people involved. 10) Carrying out any objectionable, thoughtless, or illegal activity on the Internet that shall damage the organization's reputation

IT Assets	Guidelines
ISP, Hosting Service, Website	Designated administrator to Maintain the IPs from each ISP in each location in a single sheet with customer support details. Maintain the login-in credentials of web site cPanel Backup of cPanel

3.6 Cloud Computing

This policy outlines guidelines to procure, evaluate, use, and approval processes for using cloud computing services to support the processing, sharing, storage, and management of company data. The cloud service delivery models that will be used are Infrastructure as a Service (IaaS), Software as a Service (SaaS), Platform as a Service (PaaS), Network as a Service (NaaS). The cloud deployment models that will be used are Private cloud – where services are provided by an internal provider, public cloud – where services are provided by third parties, i.e., external companies or entities, over the public Internet.

IT Assets	Guidelines
Cloud Service Provides like MS Azure,	When a customer uses a service provider, it is generally accepted that the customer is the data controller, and the service provider is the data processor. The cloud service models are as follows: SaaS: Software as a Service, that is, online software provisioning. PaaS: Platform as a Service, that is, online application development platform provisioning. IaaS: Infrastructure as a Service, that is, online computing and storage infrastructure provisioning. The deployment models are as follows: Public when a service is shared and pooled between many customers. Private when the Cloud is dedicated to one customer. Hybrid when a service is partly in a public Cloud and partly in a private Cloud. CSP Hardening includes but not limited to: 1. Disable or remove all unnecessary interfaces, ports, devices, and services. 2. Securely configure all virtual network interfaces and storage areas. 3. Establish limits on VM resource usage. 4. Ensure all operating systems and applications running inside the virtual machine are also hardened. 5. Designated employees need to have access to the Hypervisor administrative access logs. 6. Hypervisor complete Logging to be enabled. Data transmission and encryption requirements. 1. Authentication procedures. 2. Security and access controls, including intrusion/breach detection and prevention procedures. 3. Security, virus, malware, etc. scanning requirements. 4. Data ownership, retention, and recovery; and 5. Clear delineation of responsibility and liability in the event of a security breach Define the

	IT Policy		Doc. No.		PH/L3/IT/004	
			Issue No.		01	
			Rev. No.	00	Date	05.04.2022
			Page No.		24 of 32	

IT Assets	Guidelines
	- Permitted cloud-based applications for - Use with biometric device data - Confidential or Sensitive Information storage - Communications Tools [E.g., E-mail, Video Conferencing, Instant, Messaging] - Personal Use of Cloud-Based Applications and Cloud-Based Communication Tools Use an evaluation for - Department requirements - Vendor considerations - Data issues - Payments details - Support arrangements - Exit strategy
SAP	Refer the SAP contract with Ctrl S
NAS	Provide VPN connection to designated users Provide access to designated user, folders Administration to control the credentials
Wi-Fi Cloud Controller	The connection to be through SDWAN

3.7 Digital Data

The policy provides guidelines to protect data integrity based on data classification and secure the organization's information systems from unauthorized access, alteration, and destruction of data.

IT Assets	Guidelines
General Guidelines	- Various methods like access control, authentication, monitoring and review will be used to ensure data security in the organization. - Security reviews of servers, firewalls, routers, and monitoring systems must be conducted on a regular basis. These reviews should include monitoring of access logs and intrusion detection software logs. - Appropriate training must be provided to data owners, data users, and network & system administrators to ensure data security.
Data life cycle: General Guidelines	- The typical life cycle of data is generation, use, storage, and disposal. The following sections provide guidance as to the application of this policy through the different life cycle phases of data. - Users of data assets are personally responsible for complying with this policy. - All users will be held accountable for the accuracy, integrity, and confidentiality of the information to which they have access. Data must only be used in a manner consistent with this policy. In conformance with this policy only uniquely identified, authenticated, and authorized users are allowed to access data.
Classification of information/data	The information/data are classified as Sensitive, Confidential, Private & Public. Sensitive: This is highly sensitive information that could seriously damage the organization existence and reputation if such information were lost or

IT Assets	Guidelines
	made public. Examples include includes financials, internal audits, and internal evaluation Confidential: Information that, if made public or even shared around the organization, could seriously impede the organization's operations, and is considered critical to its ongoing operations. Confidential Information would include accounting information, Employee evaluation and appraisal information. Private information: Information not approved for general circulation outside the organization where its loss would inconvenience the organization or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include internal memos and minutes of meeting, research data, monitoring and evaluation data. Public information: This is Information in the public domain which has been approved for view by the public. This information can be shared to anyone. Examples include program success stories - Different protection strategies must be developed by the IT department for the above three data categories. Information about the same must be published appropriately to all relevant departments and staff. - Sensitive & Confidential data must be encrypted when transmitted over insecure channels. - All data must be backed up on a regular basis as per the rules defined by the IT Dept. at that time.
Password Guidelines	The following password guidelines can be followed to ensure maximum password safety. - Select a Good Password: - Choose a password which does not contain easily identifiable words (e.g., your username, name, phone number, house location etc.). - Use 8 or more characters. - Use at least one numeric and one special character apart from letters. - Combine multiple unrelated words to make a password. - Keep your Password Safe: - Do not share your password with anyone. - Make sure no one is observing you while you enter your password. - As far as possible, do not write down your password. If you want to write it down, do no display it in a publicly visible area. - Change your password periodically (every 42 days is recommended). - Do not reuse old passwords. If that is difficult, do not repeat the last 5 passwords. - Other Security Measures: - Ensure your computer is reasonably secure in your absence. - Lock your monitor screen, log out or turn off your computer when not at desk.
Internet Banking, Invoice, GST Digital Data	While using ensure Lock symbol and https connection are there Certificate validity EPS validity Email from address is correct and it is not spam/phishing

IT Assets	Guidelines
PLC Machine Data	As of now ensure the PLC machines are in a different LAN network and access to internet is limited to designated PC on request for a specific period for specific reason. The data are stored inside the LAN and not exposed to internet except for technical support from supplier

3.8 3rd Party Tools

IT Assets	Guidelines
Bulk email Integration,	Ensure the emails are scanned before reaching the inbox
Invoice & GST Integration	Ensure the 3 rd party integration is through with proper validation

3.9 Information Security

IT Assets	Guidelines
Infrastructure Security,	Central Access Control to devices/systems/application Restriction of device usage Restriction of Printing & Storage
Staff Security	NDA Agreement Training Background verification Attendance system RFID/Biometric/Web Application
Network Security	Secure communication systems Strong Firewall Intrusion detection Intrusion prevention Content filtering Prevent cyber attack Access control
Data Security	Disable USB for pen drive and other data storage devices Download restrictions Antivirus software

Remote User Access Policy

1.0 Purpose

The purpose of this policy is to define the rules and requirements for connecting to Polyhose network from company laptops outside organisation.

These rules and requirements are designed to minimize the potential exposure from damages which may

	IT Policy	Doc. No.		PH/L3/IT/004	
		Issue No.		01	
		Rev. No.	00	Date	05.04.2022
		Page No.		27 of 32	

result from unauthorized use of company resources.

Damages include the loss of sensitive or organization confidential data, intellectual property, damage to public image, damage to critical internal systems, and fines or other financial liabilities incurred because of those losses.

2.0 Policy

It is the responsibility of our company's employees with remote access privileges to our corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection.

General access to the Internet for recreational use through our company network is strictly limited to our employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing our network from a personal computer, Authorized Users are responsible for preventing access to any company computer resources or data by non-Authorized Users.

Performance of illegal activities through our company network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see our Acceptable Use Policy. Authorized Users will not use our networks to access the Internet for outside business interests. For additional information regarding our remote access connection options, including how to obtain a remote access login/VPN, anti-virus software, troubleshooting, etc., see our IT technical lead.

3.0 Connection Procedures

1. Secure remote access will be strictly controlled with encryption through our Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see our company's Encryption and the Password rules in IT Policy.
2. Authorized Users shall protect their login and password, even from family members.
3. While using our corporate owned computer to remotely connect to our corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
4. Use of external resources to conduct our company business must be approved in advance by the appropriate business unit manager.
5. All hosts that are connected to our company's internal networks via remote access technologies must use the most up-to-date anti-virus software this includes personal computers. Third party connections must comply with requirements as stated in the Third-Party Agreement with our partner.
6. Personal equipment used to connect to our company's networks must meet the requirements of company owned equipment for remote access - and approved by your business unit leader.

4.0 Compliance

Our company's IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, checking login log. The results of this monitoring will be provided to the appropriate Director.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

	IT Policy		Doc. No.		PH/L3/IT/004	
			Issue No.		01	
			Rev. No.	00	Date	05.04.2022
			Page No.	28 of 32		

5.0 Exception to Policy

Any exception to the policy must be approved by Director.

6.0 Applicability

This policy applies to all company employees, contractors, vendors and agents with a company owned or personally-owned computer used to connect to polyhose network.

This policy applies to remote access connections used to do work on behalf of company, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to our company's networks.

4.Risk & Contingency Plan

Risk management is essential for organizations to ensure the long-term smooth running of the business operations. The risk is to be identified wherever required/possible/feasible for the technologies. An IT risk repository to be maintained with Probability, Severity, Priority, Risk Response, Actions to be Taken. There are two parts to risk management:

4.1 Risk Mitigation

Risk management actions are to be planned for the identified items irrespective of the occurrence and severity of the risk. These actions are to be taken even before a risk occurs and this may include techniques like avoid, mitigate, accept, transfer risks.

4.2 Contingency Plan

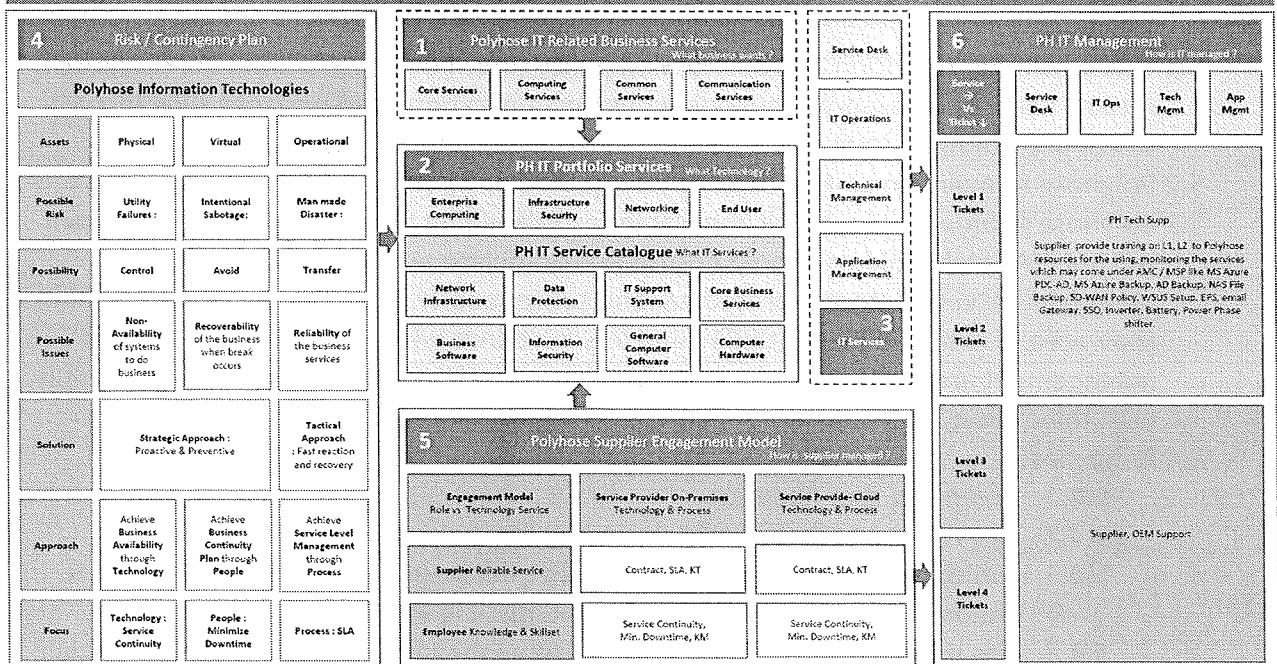
Contingency plan actions are to be planned for the identified items if the incident occurs. The pre-planning actions may be based on certain warning signs through alert or monitoring events.

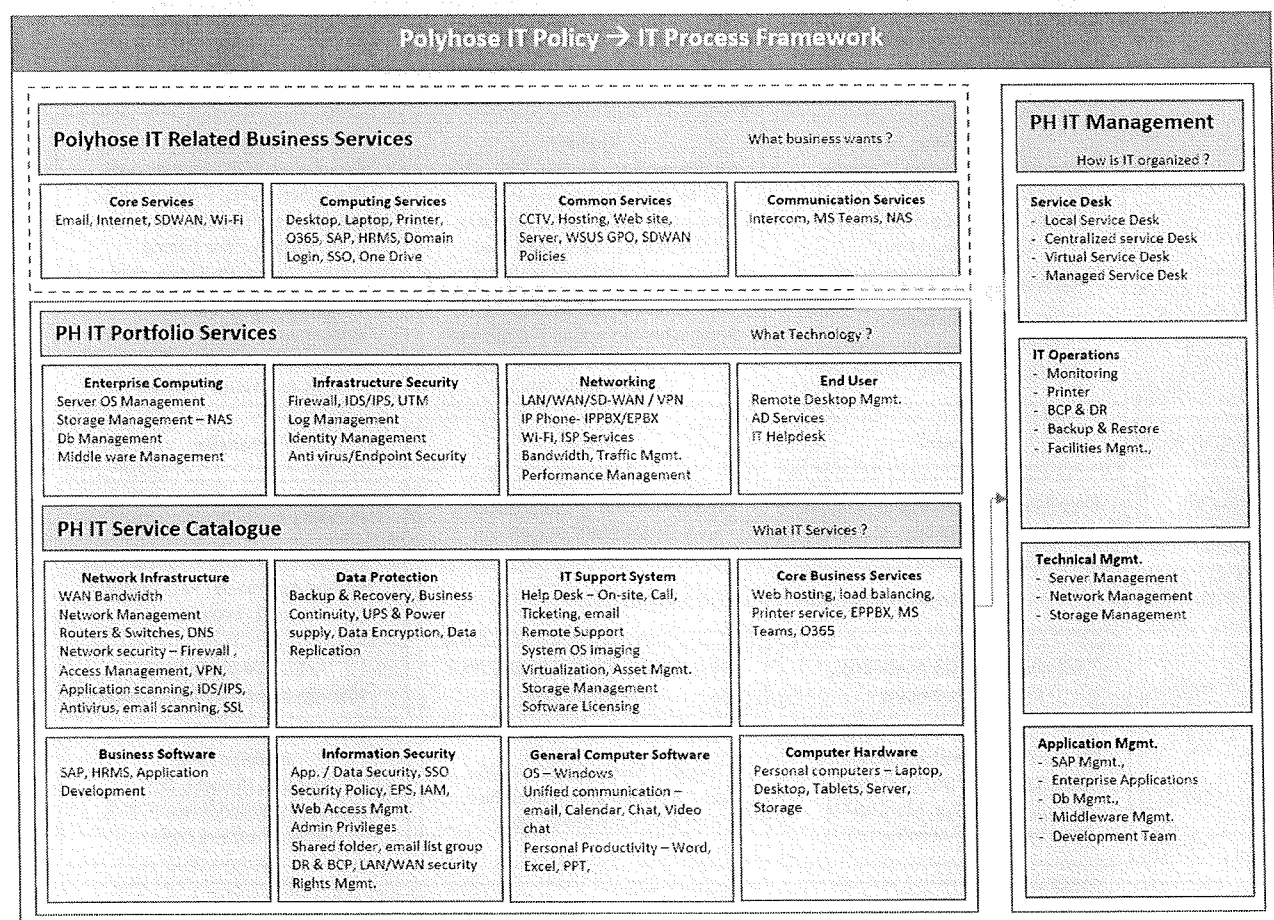
Polyhose IT Infrastructure : Risk / Contingency Plan

Polyhose Information Technology Framework

Assets	Physical Server, NAS, Storage, Camera, Desktop, Laptop, RFID, Firewall, EPPBX, Switch, Cables, SDWAN, CPE, Physical Locks	Virtual AV, Encryption, ILL, SSL, SSO, VPN, Filter, AD, Backup & Restore, Business/ System, Applications, Ticket Sys., SaaS, PaaS, IaaS	Operational Sec. Policy, SOP, License, AMC, Warranty, Policy & Procedures, App. Monitoring, Sys. Perf., Alert System, Fine Tuning
Possible Risk	Utility Failures : Occurs when utility fails. Electricity, ISP, LAN, Telephone	Intentional Sabotage: Occur when an action is done with an intent of business risk. Cyber attack, Virus	Man made Disaster : Occurs when there is a human negligence, mistake. Wrong setup / access
Possibility	Control	Avoid	Transfer
Possible Issues	Non-Availability of systems to do business	Recoverability of the business when break occurs	Reliability of the business services
Solution	Strategic Approach : Proactive & Preventive		Tactical Approach : Fast reaction and recovery
Approach	Achieve Business Availability through Technology	Achieve Business Continuity Plan through People	Achieve Service Level Management through Process
Focus	Technology : Service Continuity Apps, N/w, Sys., Db. Conf. Mgmt. Autodesk, Logging, Monitoring, Tracking, Alerting	People : Minimize Downtime Security Organization Structure – R&R, Awareness, IAM	Process : SLA Policies, Process, BCP, Standards, Procedures, IT Risk, Issues, Problem Mgmt.,

Polyhose IT Management : All-in-One IT Framework





5.0 Data Retention & Destruction:

5.1 This document retention and destruction policy (the “Policy”) sets out how Polyhose retains Records necessary for ongoing business operations and destroys such records, whilst promoting orderly and efficient records management.

5.2 Polyhose to maintain certain records for a period of 11 years.

5.3 Polyhose's compliance with all applicable recordkeeping requirements in the relevant territory. All stakeholders should ensure that complete and accurate records are identified, retained, stored, protected, and subsequently destroyed or archived within their area of assigned responsibility and in accordance with this Policy. All levels of management are responsible for ensuring that all staff under their supervision comply with this Policy.

5.4 Principles

- 5.4.1 to ensure that Records:
- 5.4.2 are retained appropriately including for the appropriate period.
- 5.4.3 which may need to be tendered as evidence in Proceedings are kept in a manner that ensures they will be admissible in those Proceedings.
- 5.4.4 are retained only if those Records serve the immediate purposes for which they were created; and
- 5.4.5 are permanently archived in accordance with law after their retention period

	IT Policy	Doc. No.		PH/L3/IT/004	
		Issue No.		01	
		Rev. No.	00	Date	05.04.2022
		Page No.	31 of 32		

has lapsed and they are no longer needed.

5.5 Retention Procedures

5.5.1 Records must be categorized by purpose and retained for specific periods.

5.5.2 Personal Data must be accurate and kept up to date. Inaccurate or out of date

5.5.3 Personal Data must be rectified or destroyed/erased.

5.5.4 Retention periods vary depending on the department in which the Records are kept.

5.6 Destruction of Documents

5.6.1 It is unlawful to destroy, conceal or falsify any Record for the purpose of obstructing or influencing any Proceeding. Doing so may subject Polyhose and any offending individuals to civil and criminal penalties including fines and imprisonment.

5.6.2 You are only permitted to destroy Records when all the following conditions are met:

- (a) no improper motive for the destruction of the Records.
- (b) no legal or regulatory reason to maintain the Records.
- (c) the destruction is in accordance with mandated retention periods

5.7 END OF SERVICE

5.7.1 Each Colleague must return to Polyhose or destroy, at Polyhose's option, all Records in their possession upon the end of their service with Polyhose. This includes, without limitation, Records located anywhere including without limitation in Polyhose's premises, personal homes of Colleagues and storage facilities.

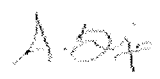
5.8 DOCUMENT CONTROL

5.8.1 The Polyhose is the owner of this Policy and is responsible for ensuring that it is reviewed in line with the relevant review requirements.

5.8.2 A current version of this Policy is available in HRMS.

 Providing Flexible Solutions Globally	IT Policy	Doc. No.	PH/L3/IT/004		
		Issue No.	01		
		Rev. No.	00	Date	05.04.2022
		Page No.	32 of 32		

Rev No	Rev Date	Description	Remarks
00	05.04.2022	Initial release	-

Prepared by : Suriya A 	Reviewed By: Satish Babu B 	Approved by : Aliasger SJ 
--	--	---