

	IT Security Policy	Doc. No.	PH/L3/IT/001		
		Issue No.	01		
		Rev. No.	001	Date	02.04.2022
		Page No.	1 of 17		

Contents

1 Introduction	2
Information Security Topics	2
IT Security Principle	2
Ownership & Administration	2
Applicability	2
General Instructions	3
Data Loss Prevention	4
Portable Storage Device Policy	4
Backup Policy	5
Physical Safety Policy	6
Computer Files Usage Policy	7
Departmental Policies	8
Security Policy for Purchasing Hardware	9
Data Protection & Encryption Policy	9
Password Policy	10
Authorized Software Policy	11
Access Control Policy	12
Server Security Policy	13
Patch Management Policy	13
Endpoint Security Policy	13
Mobile Computing Policy	14
Network Security Policy	14
Routers, Hubs and Switches	15
Cabling Policy	15
Wireless Network Security Policy	15
Clock Synchronization Policy	15
Software Development Policy	16
Inventory Management Policy	17
Print Management Policy	17

1. Introduction

Information Security Policy

A security policy is a strategy for how Polyhose will implement Information Security principles and technologies. It is essentially a business plan that applies only to the Information Security aspects of a business.

A security policy is different from security processes and procedures, in that a policy will provide both high level and specific guidelines on how Polyhose is to protect its data but will not specify exactly how that is to be accomplished. This provides freedom to choose which security devices and methods are best for the company and budget. A security policy is technology and vendor independent – its intent is to set policy only, which can be implemented in any manner that accomplishes the specified goals.

A security policy covers all electronic systems and data. As a rule, a security policy would not cover hard copies of company data but recommends using a clean desk policy.

2. Information Security Topics

Information Security Topics	Guidelines
IT Security Principle	A security policy must specifically accomplish three objectives: Confidentiality: Protecting information from unauthorized disclosure information to those who are not entitled to have the same. Integrity: Protecting information from unauthorized modification of information. Availability: Ensuring information is available when it is required. Data can be held in many different areas, some of these are: Network Servers, NAS, Cloud Storage, Laptop, Desktop, Portable hard disk/storage. This is commonly referred to as the CIA approach which is shared by all major security regulations and standards. Additionally, this approach is consistent with generally accepted industry best practices for security management.
Ownership & Administration	This IT Security Policy is owned and administered by Polyhose IT Department
Applicability	This policy applies to all systems, including network equipment and communication systems, supporting Polyhose internal and remote operations and products and services. Polyhose uses reasonable efforts to protect the security and privacy of all information received by, though or on behalf of Polyhose. In cases where a system or provider cannot meet these requirements, exceptions will be noted and documented by Information Security, and alternate controls will be implemented.

Information Security Topics	Guidelines
General Instructions	1) In case of uncertainty about a task, make sure there is a copy of the data to restore from. 2) Follow instructions or procedures that comes from IT Support time to time. 3) Users are not supposed to do his or her personal work on computers. 4) Please intimate IT Support in case of system malfunction. 5) User should always work on his/her allotted machines. In case of any urgency/emergency user may use other's machine with consultation of IT Support. 6) Antivirus software should be updated timely in consultation with IT Support. 7) Don't give others the opportunity to look over your shoulder if you are working on sensitive data/contents. 8) Do not use unnecessary shareware. 9) Do not install or copy software on system without permission of IT Support. 10) Avoid unnecessary connectivity of Internet. 11) Do not panic in case system hangs. Report it your IT Support. 12) Please ensure that preinstalled Antivirus is running on the system. 13) Food and drinks should not be placed near systems. Cup of Tea/ Coffee or water glass should not be on CPU or Monitor or Keyboard. 14) Always power off the system when cleaning it. 15) Never use wet cloth for wiping the screen. 16) Never shut the system down while programs are running. The open files will, more likely, become truncated and non-functional. 17) Never stack books/ files or other materials on the CPU. 18) Place the cover on the computers when you close the computers at the end of the day.
Data Loss Prevention	Leading Causes of Data Loss are Natural Disaster, Viruses, Human Error, Software Malfunction, Hard disk, and system failure.
Natural Disaster	Natural Disasters: The best way to prevent data loss from a natural disaster is an offsite back up.
Viruses	Viruses: There are several ways to protect against a viral threat: 1) Install a Firewall on system 2) Install an antivirus program on the system and use it regularly for scanning and be sure to check for updates for anti-virus program on a regular basis. 3) Back up and be sure to test backups from infection as well. 4) Beware of any email containing an attachment. 5) Upon notification of a virus infection systems shall be isolated from the network, scanned, and cleaned appropriately. Any removable media or other systems to which the virus shall have spread shall be treated accordingly. 6) If a system has been identified as potentially infected and removal/quarantine of the virus/malware cannot be definitively proven, the system shall be completely wiped and re-imaged.

Information Security Topics	Guidelines
Human Errors	Human Errors: 1) When transferring data, be sure it is going to the destination. If asked "Would you like to replace the existing file" make sure, before clicking "yes". 2) In case of uncertainty about a task, make sure there is a copy of the data to restore from. 3) Take extra care when using any software that may manipulate drives data storage, such as: partition mergers, format changes, or even disk checkers. 4) Before upgrading to a new Operating System, take back up of most important files or directories in case there is a problem during the installation. Keep in mind slaved data drive can also be formatted as well. 5) Never shut the system down while programs are running. The open files will, more likely, become truncated and non-functional.
Software Malfunction	Software Malfunction: Even the world's top programs cannot anticipate every error that may occur on any given program. There are still few things that can lessen the risks: 1) Be sure the software used will meant ONLY for its intended purpose. Misusing a program may cause it to malfunction. 2) Using pirated copies of a program may cause the software to malfunction, resulting in a corruption of data files. 3) Be sure that the proper amount of memory installed while running multiple programs simultaneously. If a program shuts down or hangs up, data might be lost or corrupt. 4) Back up is a tedious task, but it is very useful if the software gets corrupted.
Data Loss Prevention	Hardware & System Malfunction: The most common cause of data loss, hardware malfunction or hard drive failure, is inherent to computing. There is usually no warning that hard drive will fail, but some steps can be taken to minimize the need for data recovery from a hard drive failure: 1) Do not stack drives on top of each other, leave space for ventilation. An overheated drive is likely to fail. Be sure to keep the computer away from heat sources and make sure it is well ventilated. 2) Use an UPS (Uninterruptible Power Supply) to lessen malfunction caused by power surges. 3) NEVER open the casing on a hard drive. Even the smallest grain of dust settling on the platters in the interior of the drive can cause it to fail. 4) If system runs the scan disk on every reboot, it shows that system is carrying high risk for future data loss. Back it up while it is still running. 5) If system makes any irregular noises such as clicking or ticking coming from the drive. Shut the system down and call Hardware Engineer for more information.
Portable Storage Device Policy	1) Storage devices should be used in consultation with IT Support and should be scanned before use. 2) Unofficial storage devices should not be used on office systems.

Information Security Topics	Guidelines
Backup Policy	1) Backup should be maintained regularly on the space provided on central server of the department or on the storage media or in Cloud as per department policy. 2) Keep paper copy of server configuration file which will be useful on emergency. 3) Keep the removable media in a secure location away from the computer. 4) Always backup the data before leaving the workstation. 5) For sensitive and important data offsite backup should be used. 6) Backups for critical systems and systems that contain production Data shall be performed on at least a daily basis.

Information Security Topics	Guidelines
Physical Safety Policy	1) Protect the system from unauthorized use, loss or damage, e.g., the door should be locked when not in the office. 2) Keep portable equipment secure. 3) Position monitor and printers so that others cannot see sensitive data. 4) Keep storage media in a secure place. 5) Seek advice on disposal of equipment. 6) Report any loss of data or accessories to the IT Support. 7) Keep the system and sensitive data secure from outsiders. 8) Get authorization before taking equipment off-site. 9) Take care when moving equipment (Read instruction on moving equipment). 10) System should be properly shut down before leaving the office. 11) Log-off the system if you are leaving your seat. 12) Never remove the cables when your PC is powered ON since this can cause an electrical short circuit. 13) Do not stop scandisk if system prompts to run it at the time of system start up. 14) Always use mouse on mouse pad. 15) Be gentle while handling keyboard and mouse. 16) Do not open case of the hardware. 17) Make sure that there is some slack in the cables attached to your system. 18) All Personnel and authorized third parties shall follow clean desk/clean screen best practices, especially when stepping away from workspaces 19) Use of video cameras or other access control mechanisms to monitor individual physical access to sensitive areas. 20) Store video for at least ninety (90) days, unless otherwise required by law. 21) Restriction of unauthorized access to network access points. 22) Restrict physical access to wireless access points, gateways, and handheld devices. 23) Use of defined security perimeters, appropriate security barriers, entry controls and authentication controls, as appropriate. 24) Ensuring that all personnel with physical data centre access wear visible identification that identifies them as employees, contractors, visitors, etc. 25) Ensure that any physical access required by personnel are supervised. 26) All visitors shall log in and receive the appropriate access card, as necessary, and identifying badge. 27) Doors to physically secured facilities shall always be kept locked. 28) All servers are required to use universal power supplies (UPS). 29) All hubs, bridges, repeaters, routers and switches and other critical network equipment shall be UPS protected. 30) Sufficient power availability shall be in place to keep the network and servers running until the Disaster Recovery Plan can be implemented. 31) Redundant air conditioning units shall be in place to ensure maintenance of appropriate temperature and humidity in the data centre.

Information Security Topics	Guidelines
	32) UPS software shall be installed on all servers to implement an orderly shutdown in the event of a total power failure. 33) All UPSs shall be periodically tested 34) Emergency generators shall be in place and tested periodically to ensure that the operate properly for production data. 35) Fuel delivery services shall be in place to ensure the continued operation of emergency generators. 36) Consideration shall be taken to ensure environmental concerns are addressed such as fire, flood, and natural disaster (e.g., earthquake, flood, etc.)
Computer Files Usage Policy	All file level security depends upon the file system. Only the most secure file system should be chosen for the server. Then user permission for individual files, folders, drives should be set. - Any default shares should be removed. - Only required file and object shares should be enabled on the server. - Never download or run attached files from unknown email ID. - Always keep files in the computer in organized manner for easy accessibility. If required create new folders and sub-folders. - Avoid creating junk files and folders. - System files and libraries should not be accessed as it can cause malfunctioning of system. - When transferring data, be sure it is going to the destination. If asked "Would you like to replace the existing file" make sure, before clicking "yes".

Information Security Topics	Guidelines
Departmental Policies	1) Department should have a system administrator or in charge of IT Support. 2) Departmental staff should be aware of IT Security policies. 3) Department should have its own written security policies, standards, and processes, if needed. 4) There should be clearly defined system security procedures for the Administrator. 5) Personnel in the department should have sufficient authority to accomplish IT security related duties and policies. 6) Competent personnel should be assigned to back up IT security related duties in the event the regular System Administrator is unavailable. 7) Department should have a process to address incidents or compromises. 8) Computer equipment should be situated safely and free from potential danger (i.e., leaky roofs etc.). 9) Uninterruptible Power Supplies (UPS) should protect servers and workstations. 10) Heating, cooling, and ventilation should keep your systems at the appropriate temperature and humidity. 11) Department should have plans to use software that enforces strong passwords. 12) There should be written procedures for forgotten passwords 13) Physical security audit should be conducted. 14) Department should have physical security standards and procedures. 15) There should be procedures for locking server room, stock room. 16) Department should have an alarm system. 17) Accesses should be secure when offices/departments are off/closed. 18) Workstations and laptops should be locked down to deter theft. 19) Department should have a network map/diagram of the LAN (Local Area Network). 20) There should be a partnership with vendors who can help in an emergency if your equipment is damaged due to disaster.
	21) Backup files should be sent off-site to a physically secure location. 22) Department should store media off site. 23) Environment of a selected off-site storage area (temperature, humidity, etc.) should be within the manufacturer's recommended range for the backup media. 24) Department should have a configuration/asset control plan for all hardware and software products. 25) Trained authorized individuals should only be allowed to install computer equipment and software.

Information Security Topics	Guidelines
Security Policy for Purchasing Hardware	1) All purchases of new systems and hardware or new components for existing systems must be based upon a User Requirements Specification document and take account of longer term organizational operational needs. 2) The purchase of new computers and peripherals requires careful consideration of operations needs because it is usually expensive to make subsequent changes. 3) Information Security issues to be considered, when implementing the policy, include the following: 4) Approval of purchase of New System Hardware 5) The system must have adequate capacity or else it may not be able to process the data. 6) Where hardware maintenance is poor or unreliable, it greatly increases the risk to the organization, because, in the event of failure, processing could simply STOP. 7) User requirement specification including deployment and use of available resources and proposed use of new equipment.
Data Protection & Encryption Policy	1) To provide data confidentiality in the event of accidental or malicious data loss, all Personal Data, shall be encrypted at rest wherever required. 2) Encryption of data at rest shall use at least AES 256-bit encryption. 3) Digital signatures shall use minimum key length of 2048 bits and minimum digest length of 256. 4) Any wireless network encryption requirements that cannot be addressed by the identified device types above must be reviewed and approved by Information Security. 5) Personal Identifiable Information Data shall not be stored on equipment that is not owned or managed by Polyhose. 6) Data shall be transferred only for the purposes determined/identified in Polyhose. 7) Data loss prevention processes and tools shall be implemented to identify and/or prevent data loss.

Password Policy

Unless otherwise specified within this IT Security Policy, the following security requirements shall be adhered to when creating passwords:

- 1) Minimum of eight (8) characters in length, containing characters from the following three categories:
- 2) English uppercase characters (A through Z)
- 3) English lowercase characters (a through z)
- 4) Base 10 digits (0 through 9)
- 5) The use of non-alphabetic characters (e.g., \$, #, %) is optional but is highly recommended.
- 6) Password's history shall be kept for the previous six (6) passwords and passwords shall be unique across the password history.
- 7) Maximum password age is ninety (42) days.
- 8) Shall not be the same as or include the user id.
- 9) Passwords shall not be visible by default when entered.
- 10) Passwords shall not be easily guessable.
- 11) Set first-time passwords to a unique value for each user and change immediately after the first use.
- 12) User accounts shall be locked after seven (7) incorrect attempts.
- 13) Lockout duration shall be set to a minimum of thirty (30) minutes or until an administrator resets the user's ID upon proper user identify verification.
- 14) If a session has been idle for more than ten (10) minutes, the user shall be required to re-enter the password to re-activate access.
- 15) The following shall be adhered to when managing user passwords:
- 16) Verify user identity before performing password resets.
- 17) Where possible, these requirements shall be automatically enforced using management tools such as Active Directory Group Policy or specific system configuration(s).
- 18) Access to shared network/service/system power user/root/admin passwords shall be controlled and limited to no more than three administrators. Usage of these accounts shall be monitored.
- 19) Role based access to all systems shall be implemented, including individually assigned username and passwords.
- 20) Usernames and passwords shall not be shared, written down or stored in easily accessible areas.
- 21) Assigning multiple usernames to users shall be limited. However, when multiple usernames are assigned to personnel, different passwords shall be used with each username
- 22) Group, shared, or generic accounts and passwords shall not be used unless approved by IT Support.
- 23) Special administrative accounts, such as root, shall implement additional controls, such as alerting, to detect and/or prevent unauthorized usage.
- 24) Administrator, superuser, and service account passwords shall be stored in a secure location, for example a fire safe in a secured area. If these are stored on an electronic device, the device and/or data shall be encrypted, and access restricted accordingly.
- 25) Default passwords on systems must be changed after installation.

Information Security Topics	Guidelines
Authorized Software Policy	1) Only authorized, supported, and properly licensed software shall only be installed on Polyhose owned or managed systems. 2) Only IT Support personnel shall install authorized and licensed software. 3) The use of unauthorized software is prohibited. Immediate removal of unauthorized software is required if discovered. 4) Workstation configurations or build standards defined by the IT Department in alignment with Information Security policies are required to be followed. Change of definitions is only allowed by the IT Department. 5) A security review and approval of all software shall be completed prior to production release. The review shall be based on system criticality and data type. Free, shareware, and open-source software as well as software as a service (SaaS) shall be reviewed as well. 6) Software that is end-of-life and no longer supported is considered unauthorized software.

Access Control Policy

- 1) Confidentiality of all data shall be maintained through discretionary and mandatory access controls administered by IT Support.
- 2) Establish process for linking all access to system components each individual user.
- 3) The IT Department shall be notified of all personnel leaving Polyhose employ prior to or at the end of their employment. As soon as possible after notification, not to exceed twenty-four (24) hours, rights to all systems shall be removed unless a specific exception request is received from HR.
- 4) Administrators shall only log into systems with user ids attributable to them or follow processes that would not break attribution. For example, administrators shall use the super user or admin login.
- 5) Access to shall always be authenticated through AD. This includes access by applications/services, administrators, and all other users or sources.
- 6) All access shall be removed for users who administer or operate systems and services that process Personal Data and PII where their user controls are compromised (e.g., due to corruption or compromise of passwords, or inadvertent disclosure).
- 7) The reissuance of de-activated or expired user IDs for systems or services that process Personal Data and PII shall not be permitted.
- 8) All logins to the shall be secured through an encrypted connection (e.g., HTTPS) and appropriately authenticated.
- 9) Ensure proper user management for all users as follows:
- 10) Users (including temps, consultants, and contractors) shall formally request access to systems with only the rights necessary to perform their job functions.
- 11) A manager or above and the system owner shall formally approve user roles and access requests. System administrators shall act as the final gatekeeper to ensure access is granted appropriate to the identified role.
- 12) Inactive user accounts reviewed and disabled and/or remove at least every ninety (90) days. Exceptions shall be documented, reviewed, and approved by Information Security.
- 13) Enable accounts used by vendors for remote maintenance only during the time period needed. Ensure all vendor activity is monitored.
- 14) Performance of periodic review of users' access and access rights shall be conducted to ensure that they are appropriate for the users' role.
- 15) Remote access to Polyhose networks shall only to be granted to personnel and/or authorized third parties and shall use two-factor authentication (TFA) or multifactor (MFA) authentication.
- 16) Two-factor authentication (TFA) or multi-factor authentication (MFA) shall be used for any services remotely accessible by personnel and/or authorized third parties (e.g. Office365, VPN, etc.), unless personnel and/or authorized third parties are connected to the protected corporate network.
- 17) Remove external access to databases immediately upon notification that users have terminated their relationship with Polyhose.
- 18) Access to the Internet and other external services shall be restricted to authorized parties only based on the assigned role.

IT Security Policy

Doc. No.	PH/L3/IT/001		
Issue No.	01		
Rev. No.	001	Date	02.04.2022
Page No.	13 of 17		

Information Security Topics	Guidelines
Server Security Policy	1) Servers shall be physically secured. 2) Access via unencrypted protocols (i.e Telnet / FTP) is not allowed without prior IT Support approval. 3) Limit the number of concurrent administrative connections to three (3), where possible. (Supplier -1, IT Support -1, User/Remote -1) 4) Only one (1) primary function per server shall be implemented, where possible.
	5) Server administrators shall be limited to one primary administrator and two backup administrators, where feasible. Exceptions shall be approved by IT Department. 6) End-of-life and/or end-of-support servers shall not be used and, if discovered, removed from the network as soon as possible. 7) Define and implement server build standards that include, at a minimum, the following: a) Hardening based on industry best practice through GPO b) Host based intrusion detection c) Anti-virus/anti-malware d) Centralized logging configuration e) Security Incident Event Management (SIEM)
Patch Management Policy	1) Server operating systems shall be patched within 30 days of a critical and/or security patch release. 2) Workstations and Laptops shall be patched within 30 days of a critical and/or security patch release. 3) Network devices shall be patched within 30 days of the release of a critical and/or security patch. 4) Zero-day patches shall be applied on all systems within 14 days, and all other systems within 30 days. 5) Patches shall be tested prior to rollout in the production environment. Less critical systems shall be patched first.
Endpoint Security Policy	1) Users shall shutdown, logout or lock workstations when leaving them for any length of time. 2) Workstations and laptops shall be restarted periodically. 3) Define and implement endpoint build standards that include, at a minimum, the following: 4) Defined configurations based on industry best practice. a) Authorized software b) Anti-virus/anti-malware c) Web Filtering/Cloud Access Security Broker (CASB) if required. d) Security Incident Event Management (SIEM) agents if required. e) Workstation access to the Internet shall be controlled based on assigned or departmental role.

Information Security Topics	Guidelines
Mobile Computing Policy	1) Ensure appropriate controls are in place to mitigate risks to protected information from mobile computing and remote working environments. 2) Data loss prevention processes and tools shall be implemented to identify and/or prevent data loss. 3) Polyhose data shall be removed from employee-owned mobile devices within the timelines defined in termination policies. 4) Devices owned by personnel or authorized parties are not allowed to connect to corporate or production networks. 5) Employee-owned mobile devices shall have the ability to connect to a network separate from the guest network, where feasible
Network Security Policy	1) Access to internal and external network services shall be controlled through: a) Network access control lists (NACLs), or equivalent. b) Firewall policies, or equivalent. c) Security groups, or equivalent. d) IP whitelists, or equivalent. e) A multi-tier architecture that prevents direct access to data stores from the internet. f) Usage of role-based access controls (RBAC) shall be implemented to ensure appropriate access to networks. g) Two-factor authentication for remote access shall be implemented. 2) Firewalls, routers, and access control lists, or equivalent access controls, shall be used to regulate network traffic for connections to/from the Internet or other external networks, as follows: a) Configuration standards shall be established and implemented. b) Access control policy shall limit inbound and outbound traffic to only necessary protocols, ports, and/or destinations. c) 17.2.5. Only IT Support approved connections shall be allowed into Polyhose networks. d) 17.2.6. The use of all services, protocols, and ports allowed to access Polyhose networks shall be reviewed on a periodic basis, at a minimum every six (6) months, for appropriate usage and control implementation. e) 17.2.7. All internet facing rule set modifications shall be reviewed and approved by the IT Department prior to implementation. f) 17.2.8. Direct access between the Internet and any system containing PII shall be prohibited. 3) Network equipment shall be configured to close inactive sessions. 4) Remote access servers shall be placed with firewall control. 5) Network intrusion detection systems (IDS) shall be implemented and monitored by IT Support/MSP.

IT Security Policy

Doc. No.	PH/L3/IT/001		
Issue No.	01		
Rev. No.	001	Date	02.04.2022
Page No.	15 of 17		

Information Security Topics	Guidelines
Routers, Hubs and Switches	1) LAN equipment, hubs, repeaters, routers, and switches shall be kept in physically secured facilities. 2) Network equipment access shall be restricted to appropriate personnel only. Other staff and contractors requiring access are required to be supervised. 3) Access via unencrypted protocols (http, telnet, ftp, tftp) shall not occur. Unused channels shall be disabled. 4) Wireless access points and controllers shall not be allowed to connect to the production network. 5) Unnecessary protocols shall be removed from routers and switches. 6) Secure, encrypted VPN connections to other networks controlled by Polyhose or outside entities, when required, shall be approved by IT Department. 7) Configuration of routers and switches shall be documented and align with industry best practice. This shall include changing any vendor-supplied defaults (passwords, configurations, etc.) before installing in production. 8) End-of-life and/or unsupported network devices shall not be used and, if discovered, removed from the network as soon as possible.
Cabling Policy	1) Network cabling shall be documented in physical and/or logical network diagrams. 2) All unused network access points shall be disabled when not in use. 3) Storing or placing any item on top of network cabling shall be avoided. 4) Redundant cabling schemes shall be used whenever possible.
Wireless Network Security Policy	1) Wireless networks shall be encrypted 2) Access to wireless networks shall be restricted to only authorized devices. Any SSID can be used as long as the appropriate device and access and authentication are utilized. 3) Personnel and authorized third parties are not allowed to install unauthorized wireless equipment. 4) All Wi-Fi routers and gateways shall be physically secured. 5) Default SSIDs and usernames and passwords shall be modified or removed prior to implementation in a production environment.
Clock Synchronization Policy	1) Clocks of information processing systems performing critical or core functions within the Polyhose environment shall be synchronized to a single reference time source (i.e., external time sources synchronized to a standard reference, such as via NTP in AD Server).

Information Security Topics	Guidelines
Software Development Policy	1) Manage all code through a version control system to allow viewing of change history and content. 2) Ensure that a quality assurance (QA) methodology is followed using a multi-phase quality assurance release cycle that includes security testing. 3) Deliver security fixes and improvements aligning to a pre-determined schedule based on identified severity levels. 4) Perform vulnerability testing as a component of QA testing and address any severity 2 or higher findings prior to software release. 5) Ensure that software is released only via production managed change control processes, with no access or involvement by the development and test teams. 6) Awareness on secure coding to be insisted to supplier. 7) Develop all web applications (internal and external, including web administrative access to application(s)) based on secure coding best practice. Cover, at a minimum, prevention of common Open Web Application Security Project (OWASP) Top 10 coding vulnerabilities in software development processes, including the following: a) A1: Injection: attacker exploits insecure code to insert their own code into a program. b) A2: Broken Authentication: Incorrectly implemented authentication and session management calls can be a huge security risk. c) A3: Sensitive Data Exposure: APIs, which allow developers to connect their application to third-party services to be implement properly. d) A4: XML External Entities (XXE): upload or include hostile XML content due to insecure code. e) A5: Broken Access Control: authentication and access restriction are not properly implemented. f) A6: Security Misconfiguration: security configuration errors are huge risks g) A7: Cross-Site Scripting (XSS): attackers take advantage of APIs and DOM manipulation to retrieve data from or send commands to your application. h) A8: Insecure Deserialization: retrieving data and objects that have been saved, can be used to remotely execute code in your application. i) A9: Using Components with Known Vulnerabilities: APIs, and third-party components if they are not secure can be a risk. j) A10: Insufficient Logging & Monitoring: Failing to log errors or attacks and poor monitoring practices can introduce a human element to security risks.

IT Security Policy

Doc. No.	PH/L3/IT/001		
Issue No.	01		
Rev. No.	001	Date	02.04.2022
Page No.	17 of 17		

Information Security Topics	Guidelines
Inventory Management Policy	1) An inventory of all computer equipment and software in use throughout Polyhose shall be maintained. 2) Computer hardware and software audits shall be periodically carried out. Audits shall also be used to track: a) Unauthorized copies of software b) Unauthorized changes to hardware and software configurations c) Accuracy of current inventory
Print Management Policy	1) When Confidential Data, including Personal Data, is printed to centralized printers secure print or equivalent shall be used, where a PIN is required at the printer before the document is printed.

Rev No	Rev Date	Description	Remarks
00	03.04.2017	Initial release	-
001	02.04.2022	New Requirement added in New Policy	

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

