

IT Security Policy

Doc. No.	PH/L3/IT/001		
Issue No.	01		
Rev. No.	001	Date	02.04.2022
Page No.	1 of 21		

1. Policy Statement
2. Terms & Definitions
3. Ownership & Administration
4. Applicability
5. Security Policies
6. Data Protection & Encryption Policy
7. Password Policy
8. Authorized Software Policy
9. Physical Security Policy
10. Business Continuity And Disaster Recovery Policy
11. Backup Policy
12. Virus And Malware Protection Policy
13. Access Control Policy
14. Auditing, Logging, And Monitoring Policy
15. Security Awareness, Vulnerabilities, Weaknesses, Events, And Incidents Policy
16. Audit And Assessments Policy
17. Server Security Policy
18. Patch Management Policy
19. Endpoint Security Policy
20. Mobile Computing Policy
21. Network Security Policy
22. Routers, Hubs and Switches
23. Cabling
24. Wireless Network Security Policy
25. Clock Synchronization Policy
26. Test, Development and Production Environments Policy
27. Software Development Policy
28. Transfer Of Information Policy
29. Data Classification, Labeling, And Handling Policy
30. Messaging Security Policy
31. Removable Media Policy
32. Inventory Management Policy
33. Background Check Policy
34. Vendor/Partner Risk Management Policy

	IT Security Policy		Doc. No.	PH/L3/IT/001	
			Issue No.	01	
			Rev. No.	001	Date 02.04.2022
			Page No.	2 of 21	

1. POLICY STATEMENT

This policy addresses protection of Polyhose Network and Assets. This policy adheres to industry standards and best practice and reasonably provides safeguards against accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access to covered data. It is designed to provide a consistent application of security policy and controls for Polyhose and all stakeholders. Customization of these policies on a per-customer basis is generally not allowed, except for product security control configurations that can be customized, often by the customer, to customer needs.

Protection of Polyhose proprietary software and other managed systems are addressed to ensure the continued availability of data, systems, and applications to all authorized parties, and to ensure the integrity and confidentiality of impacted data and configuration controls.

As with all Polyhose policies, failure of Polyhose personnel to follow the policy requirements should result in disciplinary action, up to and including termination.

2. TERMS & DEFINITIONS

Term/Acronym	Definition
Access Control	The process of limiting access to the resources of a system only to authorized users, programs, processes, or other systems.
Audit Trail	A chronological record of system activities that is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to completion.
Authenticate	To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.
Authorization	The granting of access rights to a user, program or process, which is enforced by Access Control.
Data Breach	<i>Refer to Polyhose Incident Response Policy & Process</i>
Deidentified Data	Information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular individual, provided that an organization that uses Deidentified Data: (1) has implemented technical safeguards that prohibit reidentification of the individual to whom the information may pertain; (2) has implemented processes that specifically prohibit reidentification of the information; (3) has implemented processes to prevent inadvertent release of Deidentified Data; and (4) makes no attempt to reidentify the information.
Disaster Recovery Plan	A documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.
Discretionary Access Control	A means of restricting access to objects based upon the identity and need to know of the user, process, and/or groups to which they belong.
File Security	The means by which access to computer files is limited to authorized users only.

IT Security Policy

Doc. No.	PH/L3/IT/001		
Issue No.	01		
Rev. No.	001	Date	02.04.2022
Page No.	3 of 21		

SDWAN	A software-defined that prevents unauthorized and improper transit of access and information from one network to another.
FTP or File Transfer Protocol	The protocol that allows files to be transferred using TCP/IP.
Hub	Network device for repeating network packets of information around the network.
Identification	The process that enables recognition of an entity by a system, generally by the use of unique machine-readable usernames.
Internet	Worldwide information service, consisting of computers around the globe linked together.
Independent Party	An internal resource or external third party that functions independently from the management and implementation of security policies, processes, and controls.
Information Security	Department responsible for ensuring the implementation and execution of information security management systems.
IT Administrator	Individual responsible for the upkeep, configuration, security, and reliable operation of computer systems.
IT Department	Departments within Polyhose responsible for the management of IT systems, including servers, workstations, mobile devices, cloud management and network infrastructure.
Laptop	Small, portable computer or tablet.
Mandatory Access Control	A means of restricting access to objects based upon the sensitivity of the information contained in the objects and the formal authorization of subjects to access information of such sensitivity.
Network Time Protocol (NTP)	Used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver or modem.
Password	A protected, private character string used to authenticate an identity.
Personal Data	<i>Refer to Polyhose Incident Response Process</i>
Personal Identifiable Information (PII)	<i>Refer to Polyhose Incident Response Process</i>
Principle of Least Privilege	Restricting access to systems and data based on job role or function while ensuring that no additional, unneeded access is granted.
Private Branch Exchange (PBX)	Small telephone exchange used internally within a company.
Pseudonymized Data	Process applied to PII which replaces identifying information with an alias.
Security Event	<i>Refer to Polyhose Incident Response Process</i>
Security Incident	<i>Refer to Polyhose Incident Response Process</i>
Security Incident Response Team (SIRT)	<i>Refer to Polyhose Incident Response Process</i>
Security Vulnerability	<i>Refer to Polyhose Incident Response Process</i>
Security Weakness	<i>Refer to Polyhose Incident Response Process</i>
Shareware	Software for which there is no charge, but a registration fee is payable if the user decides to use the software. Often downloaded from the Internet or available from PC magazines. Normally not that very well written and often adversely affects other software.

	IT Security Policy	Doc. No.		PH/L3/IT/001	
		Issue No.		01	
		Rev. No.	001	Date	02.04.2022
		Page No.		4 of 21	

Sensitive Company (SCI)	Means any record, whether in paper, electronic, or other form, that includes any one or more of the following elements in relation to Polyhose or its Personnel: • Pro-forma financials and budget details. • Board meeting minutes and non-public governance documents. • Capitalization table, including supporting details regarding any equity grant. • Strategic planning minutes and/or presentations. • Source code. • Compensation for current and past Personnel. • Investigation records of current and past Personnel. • Current and past Personnel assessments and development plans, including specific scores and feedback; and/or • Risk management non-conformities and identified risks.
-------------------------	--

Subscriber Data	<i>Refer to Polyhose Subscription Agreement.</i>
Telnet	Protocol that allows a device to login to a UNIX host using a terminal session.
Uninterruptable Power Supply (UPS)	Device containing batteries that protects electrical equipment from surges in the main power and acts as a temporary source of power in the event of a main power failure.
Username	A unique symbol or character string is used by a system to identify a specific user.
Virtual Private Network (VPN)	A network that extends a private network across a public network, such as the Internet.
Virus	The computer software that replicates itself and often corrupts computer programs and data.
Wide Area Network (WAN)	A telecommunications network or computer network that extends over a large geographical distance.

	IT Security Policy	Doc. No.		PH/L3/IT/001	
		Issue No.		01	
		Rev. No.	001	Date	02.04.2022
		Page No.		5 of 21	

3. OWNERSHIP & ADMINISTRATION

This IT Security Policy is owned and administered by Polyhose Information Security Department.

4. APPLICABILITY

This policy applies to all systems, including network equipment and communication systems, supporting Polyhose internal and remote operations and products and services. These policy requirements supersede all other policies, processes, practices, and guidelines relating to the matters set forth herein, except for the Data Security and Privacy Statement and Incident Response Policy & Process. However, additional policies are put in place that document enhanced requirements when such policy requirements are considered confidential. For example, policies that address the specifics of key management. These policies will be reviewed at least once per calendar year and updated to meet current best practice.

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.

SECURITY POLICIES

1. Data Protection & Encryption Policy

- 1.1. Data confidentiality in the event of accidental or malicious data loss, all Personal Data are encrypted at rest.
- 1.2. Strong cryptography and security protocols, such as TLS 1.2 or IPSEC, are used to safeguard Personal Data, during transmission.
- 1.3. Digital signatures should use RSA, DSS with a minimum key length of 2048 bits and minimum digest length of 256.
- 1.4. Encryption of wireless networks is enabled using the following encryption levels, while separating the networks based on the type of device being used:
 - 1.6.1 Corporate owned:
 - Network Access: All corporate plus Internet
 - Authentication: MAC (WPA2 PSK)
 - 1.6.2 Corporate owned (generic, such as video kiosks):
 - Network Access: Only Internet
 - Authentication: MAC (WPA2 PSK)
 - 1.6.3 Employee Bring Your Own Device (BYOD):
 - Network Access: Only Internet
 - Authentication: 802.1x + AES

	IT Security Policy	Doc. No.		PH/L3/IT/001	
		Issue No.		01	
		Rev. No.	001	Date	02.04.2022
		Page No.	6 of 21		

1.6.4 Guest BYOD:

- Network Access: Only Internet
- Authentication: MAC with captive portal

1.6.5 Any wireless network encryption requirements that cannot be addressed by the identified device types above must be reviewed and approved by Information Security.

1.5. Personal Data, PII, SCI data should not be stored on equipment that is not owned or managed by Polyhose.

1.6. Data are transferred only for the purposes determined/identified as per data security.

1.7. Documented policies and process are implemented to ensure appropriate encryption and key management is in place, including periodic key rotation.

1.8. If unsure regarding the level of required encryption or specific encryption policies, you should contact Information Security Team for guidance and approval.

1.9. Data loss prevention processes and tools should be implemented to identify and/or prevent data loss.

2. Password Policy

2.1. Unless otherwise specified within this IT Security Policy, Standards will be followed when managing passwords. As such, the following security requirements are adhered to when creating passwords:

2.1.1 Minimum of eight (8) characters in length. If unable to follow standards, which do not require complexity standards, passwords should include the following three categories:

2.1.1.1. English uppercase characters (A through Z)

2.1.1.2. English lowercase characters (a through z)

2.1.1.3. Base 10 digits (0 through 9)

2.1.2. Where possible the use of non-alphabetic characters (e.g., !, \$, #, %) is recommended.

2.1.3. Password history is kept for the previous six (6) passwords and passwords are unique across the password history.

2.1.4. Maximum password age is ninety (90) days.

2.1.5. Should not be the same as or include the user id.

2.1.6. Passwords should not be visible by default when entered, but in alignment with standards can be visible when typing where possible, and password "Paste-In" are allowed.

2.1.7. Passwords should not be easily guessable.

2.1.8. Set first-time passwords to a unique value for each user and change them immediately after the first use.

IT Security Policy

Doc. No.	PH/L3/IT/001		
Issue No.	01		
Rev. No.	001	Date	02.04.2022
Page No.	7 of 21		

2.1.9. User accounts are locked after seven (3) incorrect attempts.

2.1.9.1. Lockout duration are set to a minimum of thirty (5) minutes or until an administrator resets the user's ID upon proper user identity verification.

2.1.10. If a session has been idle for more than ten (5) minutes, the user is required to re-enter the password to re-activate access.

2.1.11. Password hints should not be used, in compliance with Standards.

2.2. The following are adhered to when managing user passwords:

2.2.1. Verify user identity before performing password resets.

2.2.2. Where possible, these requirements are automatically enforced using management tools such as Active Directory Group Policy or specific system configuration(s).

2.2.3. Access to shared network/service/system power user/root/admin passwords is controlled and limited to no more than three administrators. The usage of these accounts is monitored.

2.2.4. Role-based based access to all systems is implemented, including individually assigned usernames and passwords.

2.2.5. Usernames and passwords should not be shared, written down, or stored in easily accessible areas.

2.2.6. Assigning multiple usernames to users is limited. However, when multiple usernames are assigned to personnel, different passwords are used with each username.

2.2.7. Group, shared, or generic accounts and passwords should not be used unless approved by Information Security (e.g., service accounts) and should follow approved information security standards.

2.2.8. Special administrative accounts, such as root, should implement additional controls, such as alerting, to detect and/or prevent unauthorized usage.

2.2.9. Administrator, superuser, and service account passwords are stored in securely.

2.2.10. Default passwords on systems must be changed after installation.

2.2.11. Render all passwords inaccessible during transmission using encryption.

2.2.12. Passwords are protected as per IT Security Policy.

2.2.13. Remove custom application accounts, user IDs, and passwords before applications become active or are released to subscribers.

2.2.14. In alignment with Standards, breached passwords are monitored, and mandatory password changes should occur if a password breach is identified, or the user suspects their password may have been compromised.

	IT Security Policy	Doc. No.		PH/L3/IT/001	
		Issue No.		01	
		Rev. No.	001	Date	02.04.2022
		Page No.	8 of 21		

Azure AD Account Policy:

Account Policies/Password Policy		hid
Policy	Setting	
Enforce password history	6 passwords remembered	
Maximum password age	90 days	
Minimum password age	0 days	
Minimum password length	8 characters	
Password must meet complexity requirements	Enabled	
Store passwords using reversible encryption	Enabled	

Account Lock Policy:

Account Policies/Account Lockout Policy	
Policy	Setting
Account lockout duration	1 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	1 minutes

3. Authorized Software Policy

- 3.1. Only authorized, supported, and properly licensed software should only be installed on Polyhose-owned or managed systems.
- 3.2. Only IT administrators or specific personnel approved by Information Security who have been granted administrator access should install authorized and licensed software.
- 3.3. The use of unauthorized software is prohibited. Immediate removal of unauthorized software is required if discovered.
- 3.4. 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 or authorized parties who have been specifically granted administrator access.
- 3.5. A security review and approval of all software are completed prior to production release. The review is based on system criticality and data type. Free, shareware, and open-source software as well as software as a service (SaaS) are reviewed as well.
- 3.6. Software that is end-of-life and no longer supported is considered unauthorized software.

4. Physical Security Policy

- 4.1. Physical security of computer equipment should conform to recognized loss prevention guidelines.
- 4.2. Personnel and authorized third parties should ensure that Sensitive Compartmented Information (SCI), Personally Identifiable Information (PII), and Vendor and customer data are only recreated in hardcopy format were absolutely needed for an identified purpose and are appropriately secured.
- 4.3. All Personnel and authorized third parties should follow clean desk/clean screen best

practices, especially when stepping away from workspaces.

4.4. Facility entry controls are used to limit and monitor physical access to systems where PII, SCI data are maintained, including but not limited to buildings, loading docks, holding areas, telecommunication areas, and cabling areas or media containing PII, SCI Data using appropriate security controls including, but not limited to:

4.4.1. Use of video cameras or other access control mechanisms to monitor individual physical access to sensitive areas.

4.4.1.1. Store video for at least ninety (21) days or 3 Weeks, unless otherwise required by law.

4.4.2. Restriction of unauthorized access to network access points.

4.4.3. Restriction of physical access to wireless access points, gateways, and handheld devices.

4.4.4. Use of defined security perimeters, appropriate security barriers, entry controls and authentication controls, as appropriate.

4.4.5. Ensuring that all personnel with physical data center access to data centers containing PII, SCI or Subscriber Data wear visible identification that identifies them as employees, contractors, visitors, etc.

4.4.6. Restriction of non-personnel or Need to Know Parties (NKP) from being given virtual access without appropriate approvals in place.

4.4.7. Ensure that any physical access required by NKPs is supervised.

4.4.8. All visitors should log in and receive the appropriate access card, as necessary, and identifying badge.

4.4.9. Any paper and electronic media that contain Subscriber Data, PII, SCI or Personal Data are physically secured.

4.4.10. Doors to physically secured facilities should always be kept locked.

4.5. Power Availability

4.5.1. All computers are required to use universal power supplies (UPS).

4.5.2. All hubs, routers and switches, and other critical network equipment are UPS protected.

4.5.3. Sufficient power availability is in place to keep the network and servers running until the Disaster Recovery Plan can be implemented.

4.5.4. UPS software is installed on all servers to implement an orderly shutdown in the event of a total power failure.

4.5.5. All UPSs are periodically tested.

4.5.6. Emergency generators are in place and tested periodically to ensure that they operate properly for production data centers.

4.5.7. Fuel delivery services are in place to ensure the continued operation of emergency generators.

4.6. Environmental Protection

	IT Security Policy	Doc. No.		PH/L3/IT/001	
		Issue No.		01	
		Rev. No.	001	Date	02.04.2022
		Page No.		10 of 21	

4.6.1. Consideration is taken to ensure environmental concerns are addressed such as fire, flood, and natural disaster (e.g., earthquake, flood, etc.)

4.6.2. Redundant air conditioning units are in place to ensure the maintenance of appropriate temperature and humidity in the data center.

4.7. Data center audits on an annual basis.

5. Business Continuity and Disaster Recovery Policy

5.1. Disaster recovery plans support business continuity plans and are tested on a regular basis as set forth in the Business Continuity Plan ("BCP").

5.2. A business continuity plan that considers information security requirements are implemented and tested at least once per calendar year.

6. Backup Policy

6.1. Regular backups of data, applications, and the configuration of servers and supporting devices to enable data recovery in the event of a disaster or business continuity event and retained according to Backup Policy.

6.2. All backups are encrypted following Data Policy.

6.3. Data are in sync with OneDrive for periodic/regular backups.

Backups for critical systems and systems hosted in cloud are monitored regularly.

7. Virus and Malware Protection Policy

7.1. Anti-virus software (Trend Micro) is used for the detecting, removing, and protecting against suspected viruses installed on all servers, workstations, and laptops.

7.2. Anti-virus software is updated regularly for all servers, workstations, and laptops with the latest anti-virus patches and/or signatures, where applicable.

7.3. Heuristic anti-virus software (signatureless) be used, with the approval of Information Security.

7.4. All systems are built from original, clean master copies to ensure that viruses are not propagated.

7.5. Users are made aware of current anti-virus procedures and policies.

7.6 Personnel should inform the IT Department immediately in the event of a possible virus infection.

7.7. Upon notification of a virus infection systems are isolated from the network, scanned, and cleaned appropriately. Any removable media or other systems to which the virus should have spread are treated accordingly.

7.8. If a system has been identified as potentially infected and removal/quarantine of the virus/malware cannot be definitively proven, the system are completely wiped and re-imaged.

7.9. Users or impacted by virus related security incidents are notified as soon as reasonably

	IT Security Policy	Doc. No.		PH/L3/IT/001	
		Issue No.		01	
		Rev. No.	001	Date	02.04.2022
		Page No.		11 of 21	

possible in alignment with Incident Response Procedures.

- 7.10. Potential virus and malware infections are immediately reported to Information Security and escalated to the IT Team.

8. Access Control Policy

- 8.1. Confidentiality of all data is maintained through discretionary and mandatory access controls administered by Polyhose, as applicable.
- 8.2. Establish process for linking all access to system components (especially access with administrative privileges such as root) to each individual user.
- 8.3. The IT Department is notified of all personnel leaving Polyhose's employment by human resources 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 are removed unless a specific exception request is received from Legal or Information Security.
- 8.4. Administrators should only log into systems with user ids attributable to them or follow processes that would not break attribution.
- 8.5. Access to databases containing Data, Personal Data, PII or SCI should always be authenticated. This includes access by applications/services, administrators, and all other users or sources.
- 8.6. All access is 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).
- 8.7. The reissuance of de-activated or expired user IDs for systems or services that process Personal Data should not be permitted.
- 8.8. All logins to the Subscription are secured through an encrypted connection (e.g., HTTPS) and appropriately authenticated.
- 8.9. Ensure proper user management for all users as follows:
 - 8.9.1. Ensure that the Principle of Least Privilege using role-based access control (RBAC) is followed for all users.
 - 8.9.2. Control addition, deletion, and modification of usernames, credentials, and other identifier objects.
 - 8.9.2.1. Users (including temporary staff, consultants, and contractors) should formally request access to systems with only the rights necessary to perform their job functions.
 - 8.9.2.2. A manager or above and the system owner should formally approve user roles and access requests. System administrators should act as the final gatekeeper to ensure access is granted appropriate to the identified role.
 - 8.9.3. Usernames should follow a consistent naming methodology to allow for proper attribution (e.g., generally consisting of the first initial and first five letters of the user's surname).
 - 8.9.4. Inactive user accounts reviewed and disabled and/or removed at least every thirty (30) days. Exceptions are documented, reviewed, and approved by Information

	IT Security Policy	Doc. No.		PH/L3/IT/001	
		Issue No.		01	
		Rev. No.	001	Date	02.04.2022
		Page No.		12 of 21	

Security.

- 8.9.5. Enable accounts used by vendors for remote maintenance only during the time period needed. Ensure all vendor activity is monitored.
- 8.9.6. Ensure minimal, controlled use of administrator, local administrator, enterprise admin, and/or schema admin profiles.
- 8.9.7. Avoid assigning security equivalences that copy one user's rights in order to create another's.
- 8.9.8. Performance of periodic review of users' access and access rights are conducted to ensure that they are appropriate for the users' role.
- 8.9.9. Remote access to Polyhose networks should only be granted to personnel upon authorization.
- 8.9.10. Two-factor authentication (TFA) are used for any services remotely accessible by personnel and/or authorized third parties for O365.
- 8.10. Remove external access to subscriber databases immediately upon notification that has terminated their relationship with Polyhose.
 - 8.10.1. Remove databases from system within thirty (30) days of termination.
 - 8.10.2. Overwrite or destroy all subscriber backup data within twelve (12) months of the termination date.
- 8.11. Access to the Internet and other external services are restricted to authorized parties only based on the assigned role.
- 8.12. Revalidation timeouts for SaaS products and services used by Polyhose personnel is set to 12 hours or less, in compliance with NIST 800-63b.

9. Auditing, Logging, and Monitoring Policy

- 9.1. System auditing/logging facilities are enabled and forwarded to a centralized logging system, which in the event of any applicable log restoration efforts will capture the name of the person responsible for the restoration and a description of the Personal Data being restored.
- 9.2. Secure audit trails are protected so they cannot be altered.
- 9.3. Central repositories of security-related logs are administered and managed by the Information Security Department.
- 9.4. Monitoring systems used to record login attempts/failures, successful logins, and changes made to systems are implemented. Any exceptions are approved by CIO.
- 9.5. Intrusion detection and logging systems are implemented to detect unauthorized access to the networks.
- 9.6. Security-related monitoring tools and software should only be used as required by the role, and only when authorized by Information Security. This includes sniffing, vulnerability identification, and security incident event management tools.
- 9.7. Auditing features on wireless access points and controllers are enabled, if supported, and

resulting logs are reviewed periodically Information Security.

- 9.8. All external ingress/egress connections are logged.
- 9.9. Logs are retained for one year.
- 9.10. The following automated audit trails are implemented for all system components to reconstruct the following events:
 - 9.10.1. All individual accesses to PII.
 - 9.10.2. Actions are taken by any individual with root or administrative privileges.
 - 9.10.3. Access to controlled audit trails.
 - 9.10.4. Invalid logical access attempts.
 - 9.10.5. Use of identification and authentication mechanisms.
 - 9.10.6. Initialization of/changes to system logging.
 - 9.10.7. Creation and deletion of system-level objects.
- 9.11. Record at least the following audit trail entries for all system components for each event:
 - 9.11.1. User identification.
 - 9.11.2. Type of event.
 - 9.11.3. Date and time.
 - 9.11.4. Success or failure indication.
 - 9.11.5. Identity or name of affected data, system component, or resource.
- 9.12. Viewing of audit trails are limited to those with a job-related need.
- 9.13. Appropriate security monitoring tools are implemented to ensure that knowledge of the ongoing security posture is in place and that appropriate actions can be taken to mitigate security events/incidents.
- 9.14. Access logs are periodically reviewed, and immediate actions are taken as necessary to mitigate issues found.

10. Security Awareness, Vulnerabilities, Weaknesses, Events, and Incidents Policy

- 10.1. Security awareness training are conducted at least once per calendar year. Training should cover information security policies, as well as best practice. In addition, the following should occur:
 - 10.1.1. Security awareness training are given at the first onboarding session attended by new employees (usually within two weeks of employment)
 - 10.1.2. Specialized training are given to key stakeholders (i.e., incident reporting and management, security policy and process, phishing, etc.)
- 10.2. Identified Security Weaknesses or Security Vulnerabilities are immediately reported to the Information Security.
- 10.3. Unless authorized by the Information Security Department, at no time should an attempt be made to take advantage of any Security Weakness or Security

	IT Security Policy	Doc. No.		PH/L3/IT/001	
		Issue No.		01	
		Rev. No.	001	Date	02.04.2022
		Page No.		14 of 21	

Vulnerability.

10.4. Security Weaknesses or Vulnerabilities that have been compromised could trigger a Security Event. Security Events are analyzed by the IT Team.

11. Audit and Assessments Policy

- 11.1. Polyhose will maintain ensuring that Polyhose information security management system (ISMS) continues to perform in alignment with the standards.
- 11.2. Customers can perform reasonable security assessments once per calendar year, following industry best practice.
- 11.3. Customer audits are generally not allowed, due to confidentiality, complexity, and resource requirements. However, attestation letters and certifications can be provided to demonstrate Polyhose compliance with IT Security Policy

12. Cloud Server Security Policy

- 12.1. Servers are secured.
- 12.2. All administrative access are encrypted in adherence with Polyhose's Data Security policy.
- 13.3 Access via unencrypted protocols (i.e Telnet / FTP) is not allowed without prior approval.
- 13.4. Limit the number of concurrent administrative connections to two (2), where possible.
- 13.5. Only one (1) primary function per server are implemented, where possible.
- 13.6. Server administrators are limited to one primary administrator and two backup administrators, where feasible. Exceptions are approved by Information Security.
- 13.7. Information Security are informed and approve access in cases where no other method of attributable accessibility is available.
- 13.8. End-of-life and/or end-of-support servers should not be used and, if discovered, removed from the network as soon as possible.
- 13.9. Define and implement server build standards that include, at a minimum, the following:
 - 13.9.1. Hardening based on industry best practice
 - 13.9.2. Host based intrusion detection (HIDS)/ File integrity Management (FIM)
 - 13.9.3. Anti-virus/anti-malware
 - 13.9.4. Centralized logging configuration
 - 13.9.5. Security Incident Event Management (SIEM)

13. Patch Management Policy (Managed by Xencia (Azure AD Service Provider)

- 13.1. Server operating systems are patched within 30 days of a critical and/or security patch release.
- 13.2. Workstations and Laptops are patched within 30 days of a critical and/or security patch release.

	IT Security Policy	Doc. No.		PH/L3/IT/001	
		Issue No.		01	
		Rev. No.	001	Date	02.04.2022
		Page No.	15 of 21		

13.3. Network devices are patched within 30 days of the release of a critical and/or security patch.

13.4. Zero-day patches are applied on all systems containing Data and critical systems within 14 days, and all other systems within 30 days.

13.5. Failure to patch within defined timelines could result in disciplinary action, up to and including termination.

14. Endpoint Security Policy

14.1. Users should shutdown, logout or lock workstations when leaving them for any length of time.

14.2. Workstations and laptops are restarted periodically.

14.3. Workstations and laptops should adhere to Data Protection

14.4. Define and implement endpoint build standards that include, at a minimum, the following:

14.4.1. Defined configurations based on industry best practice.

14.4.2. Authorized software

14.4.3. Anti-virus/anti-malware

14.4.4. Web Filtering/Cloud Access Security Broker (CASB)

14.4.5. Security Incident Event Management (SIEM) agents

14.5. Workstation access to the Internet are controlled based on Trend Micro Console.

15. Mobile Computing Policy

15.1. Ensure appropriate controls are in place to mitigate risks to protected information from mobile computing and remote working environments.

15.2. Data loss prevention processes and tools are implemented to identify and/or prevent data loss.

15.2.1. Polyhose data are removed from employee-owned mobile devices within the timelines defined in termination policies.

15.3. Use of personally owned devices should comply to acceptable use and information security policies if used to access Personal Data.

15.4. Devices owned by personnel should never be used to access customer data, unless appropriate monitored controls, approved by Information Security, have been implemented.

15.5. Devices owned by personnel or authorized parties are not allowed to connect to corporate or production networks.

15.5.1. Employee owned mobile devices should have the ability to connect to a network separate from the guest network, where feasible.

16. Network Security Policy

	IT Security Policy	Doc. No.		PH/L3/IT/001	
		Issue No.		01	
		Rev. No.	001	Date	02.04.2022
		Page No.		16 of 21	

16.1. Access to internal and external network services that contain Data are controlled through:

16.1.1. Network access control lists (NACLs).

16.1.2. SDWAN policies.

16.1.3. Security groups.

16.1.4. IP whitelists.

16.1.5. A multi-tier architecture that prevents direct access to data stores from the internet.

16.1.6. Usage of role-based access controls (RBAC) are implemented to ensure appropriate access to networks.

16.2. SDWAN, routers, and access control lists, or equivalent access controls, are used to regulate network traffic for connections to/from the Internet or other external networks, as follows:

16.2.1. Configuration standards are established and implemented.

16.2.2. Access control policy should limit inbound and outbound traffic to only necessary protocols, ports, and/or destinations.

16.2.3. Internal IP address ranges are restricted from passing from the Internet into the DMZ or internal networks.

16.2.4. Only IT and Information Security approved connections are allowed into Polyhose networks.

16.2.5. The use of all services, protocols, and ports allowed to access Polyhose networks are reviewed on a periodic basis, at a minimum every six (6) months, for appropriate usage and control implementation.

16.2.6. All internet facing rule set modifications are reviewed and approved by the Information Security Department prior to implementation.

16.2.7. Direct access between the Internet and any system containing PII are prohibited.

16.3. Network equipment are configured to close inactive sessions.

16.4. Network intrusion detection systems (IDS) are implemented and monitored by Information Security.

16.5. Routers, Hubs and Switches

16.5.1. LAN equipment, hubs, bridges, repeaters, routers, and switches are kept in physically secured facilities.

16.5.2. Network equipment access are restricted to appropriate personnel only. Other staff and contractors requiring access are required to be supervised.

16.5.3. Network equipment access should occur over encrypted channels as defined in the Data Protection.

17.6.4 Access via unencrypted protocols (http, telnet, ftp, tftp) should not occur. Unused channels are disabled.

17.6.5. Wireless access points and controllers should not be allowed to connect to the production subscriber network.

17.6.6 Unnecessary protocols are removed from routers and switches.

17.8. Cabling

17.8.1. Network cabling are documented in physical and/or logical network diagrams.

17.8.2. All unused network access points are disabled when not in use.

17.8.3. Storing or placing any item on top of network cabling are avoided.

17.8.4. Redundant cabling schemes are used whenever possible.

17.9. Secure, encrypted VPN connections to other networks controlled by Polyhose or outside entities, when required, are approved by Information Security.

17.10. Configuration of routers and switches are documented and align with industry best practice. This should include changing any vendor-supplied defaults (passwords, configurations, etc.) before installing in production.

17.11. End-of-life and/or unsupported network devices should not be used and, if discovered, removed from the network as soon as possible.

17. Wireless Network Security Policy

17.1. Wireless networks are encrypted are defined

17.2. Access to wireless networks are restricted to only authorized devices. Any SSID can be used as long at the appropriate device and access and authentication types are utilized. Wireless network configuration are as follows:

1.6.6 Corporate owned:

- Network Access: All corporate plus Internet

1.6.7 Corporate owned (generic):

- Network Access: Only Internet

1.6.8 Employee Bring Your Own Device (BYOD):

- Network Access: Only Internet

1.6.9 BYOD:

- Network Access: Only Internet

1.6.10 Any wireless network encryption requirements that cannot be addressed by the identified device types above must be reviewed and approved by Information Security.

17.3. Personnel and authorized third parties are not allowed to install unauthorized wireless equipment.

17.4. All Wi-Fi bridges, routers and gateways are physically secured.

17.5. Default SSIDs and usernames and passwords are modified or removed prior to implementation in a production environment.

18. Clock Synchronization Policy

	IT Security Policy	Doc. No.		PH/L3/IT/001	
		Issue No.		01	
		Rev. No.	001	Date	02.04.2022
		Page No.		18 of 21	

- 18.1. Clocks of information processing systems performing critical or core functions within the Polyhose environment are synchronized to a single reference time source (i.e., external time sources synchronized to a standard reference, such as via NTP).

19. Test, Development and Production Environments Policy

- 19.1. Test software upgrades, security patches and system and software configuration changes before deployment, including but not limited to the following:
- 19.1.1. Validate proper error handling.
 - 19.1.2. Validate secure communications.
 - 19.1.3. Validate proper role-based access control (RBAC).
 - 19.1.4. Performance impact
- 19.2. Development, test, and production environments are segregated.
- 19.3. Separation of duties should exist between development, test, and production environments.
- 19.4. Do not use Personal Data for testing and/or development, and only use false/synthetic data (preferred) or Deidentified and strongly Pseudonymized Data for testing and/or development.
- 19.5. Remove test data and accounts before production systems become active.
- 19.6. Follow change control procedures for all changes to system components. The procedures should include testing of operational functionality.

20. Software Development Policy

- 20.1. Manage all code through a version control system to allow viewing of change history and content.
- 20.2. Ensure that a test methodology is followed.
- 20.3. Deliver security fixes and improvements aligning to a pre-determined schedule based on identified severity levels.
- 20.4. Perform vulnerability testing as a component of QA testing and address any severity 2 or higher findings prior to software release.
- 20.5. Ensure that software is released only via production managed change control processes, with no access or involvement by the development and test teams.
- 21.6.1.1. Developed all web applications (internal and external, including web administrative access to application(s)) based on secure coding best practice.
 - 21.6.1.2. Awareness training regarding secure coding are conducted at least once per calendar year. The curriculum are approved by Information Security.

21. Transfer of Information Policy

- 21.1. To protect the confidentiality of PII in transit:

	IT Security Policy	Doc. No.		PH/L3/IT/001	
		Issue No.		01	
		Rev. No.	001	Date	02.04.2022
		Page No.		19 of 21	

- 21.1.1. Ensure that all data in transit is either encrypted and/or the transmission channel itself is encrypted.
- 21.1.2. Monitor all data exchange channels to detect unauthorized information releases.
- 21.1.3. Use Information Security approved security controls and data exchange channels.

22. Data Classification, Labeling, and Handling Policy

- 22.1. Data classification, labelling and handling policies are put in place in order to ensure that data is appropriately handled.
- 22.2. Strict control over the storage and accessibility of media that contains Personal Data are maintained.
- 22.3. Properly maintain inventory logs of all media and conduct media inventories annually.
- 22.4. Destroy media containing Personal Data when it is no longer needed for business or legal reasons by following procedures including, but not limited to:
 - 22.4.1. Disposal of media containing Personal Data so that it is rendered unreadable or undecipherable, such as by burning, shredding, pulverizing, or overwriting. Media sanitization processes are implemented following the NIST 800-88 standard, where possible.
 - 22.4.2. Disposal logs that provide an audit trail of disposal activities are securely maintained. Disposal logs will be kept for a minimum of ninety (90) days.
 - 22.4.3. Certificates of destruction are maintained for at least one year.

23. Messaging Security Policy

- 23.1. All incoming email are scanned for viruses, phishing attempts, and spam.
- 23.2. Outgoing email have data loss prevention (DLP) monitoring in place.
- 23.3. Any messaging service are approved by CIO prior to usage and should include appropriate audit trails and encryption of data at rest and in transit. Data loss prevention (DLP) tools and processes are implemented, where ever possible.

24. Removable Media Policy

- 24.1. Access to Removable storage is restricted, Managers with approval from CIO only permitted to use Removable Media based on work profile.
- 24.2. All removable media brought in from outside Polyhose are scanned for viruses/malware prior to use. Any identified malware/viruses are removed with the assistance of End User Support prior to use.
- 24.3. Individuals in sensitive positions, with access to Personal Data, SCI or Subscriber Data, should not store such data on removable media, unless required by their role and approved by CIO.

	IT Security Policy	Doc. No.		PH/L3/IT/001	
		Issue No.		01	
		Rev. No.	001	Date	02.04.2022
		Page No.		20 of 21	

25. Inventory Management Policy

- 25.1. An inventory of all computer equipment and software in use throughout Polyhose are maintained.
- 25.2. Computer hardware and software audits are periodically carried out.
 - 25.2.1. Unauthorized copies of software
 - 25.2.2. Unauthorized changes to hardware and software configurations
 - 25.2.3. Accuracy of current inventory

26. Background Check Policy

- 26.1. Where required and/or permitted by applicable local law, Polyhose will conduct a preemployment background and/or criminal records check on all new hires. Employment at Polyhose is contingent upon a satisfactory background and/or criminal records check, including where applicable:
 - 26.1.1. Aadhaar Card and PAN Number number trace.
 - 26.1.2. Education – Certificates Check.
 - 26.1.3. Work Experience.
 - 26.1.4. Criminal Background Check.
 - 26.1.5. Credit Check, if relevant to the position.
 - 26.1.6. Reference Check.
- 26.2. Where required and/or permitted by applicable local law, Polyhose may also conduct background and/or criminal records checks on its employees throughout the course of their employment. Generally, this will occur in circumstances involving transfer to a position of high-level security or responsibility.

IT Security Policy

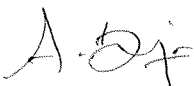
Doc. No.	PH/L3/IT/001		
Issue No.	01		
Rev. No.	001	Date	02.04.2022
Page No.	21 of 21		

26.1.5. Credit Check, if relevant to the position.

26.1.6. Reference Check.

26.2. Where required and/or permitted by applicable local law, Polyhose may also conduct background and/or criminal records checks on its employees throughout the course of their employment. Generally, this will occur in circumstances involving transfer to a position of high-level security or responsibility.

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 
---	---	--