Broome-Tioga BOCES
Parents' Bill of Rights for Data Privacy and Security

Broome-Tioga BOCES is committed to protecting the privacy and security of student, teacher and principal data. In accordance with New York Education Law §2-d, BOCES wishes to inform the community of the following:

- A student's personally identifiable information cannot be sold or released for any commercial purposes.
- Parents have the right to inspect and review the complete contents of their child's education record.
- State and federal laws protect the confidentiality of personally identifiable information and safeguards associated with industry standards and best practices, including, but not limited to, encryption, firewalls, and password protection must be in place when data is stored or transferred.
- A complete list of all student data elements collected by the state is available for public review at http://www.nysed.gov/data-privacy-security/student-data-inventory, or by writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
- Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY, 12234. Complaints may also be directed to the Chief Privacy Officer via email at: privacy@nysed.gov.
- The BOCES will promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect personally identifiable information.

Appendix
Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services, BroomeTioga BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data" as those terms are defined by law.

Each contract BOCES enters into with a third-party contractor, where the third-party contractor receives student data or teacher or principal data, will include the following information:

- The exclusive purposes for which the student data or teacher or principal data will be used.
- How the third-party contractor will ensure that the subcontractors, persons or entities that the thirdparty contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements.
- When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement.
- If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected.
- Where the student, teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

This section to be completed by the Third-Party Contractor and returned to Broome-Tioga BOCES

https://www.btboces.org/Downloads/Parents%20Bill%20of%20Rights%20edit.pdf

Section 1: Does the Third-Party Contractor have access to student data and/or teacher or principal data as those terms are defined by law?

☑ Yes
Please complete Sections 2, 3 and 4

☐ No
Please complete Section 3

Section 2: Supplemental Information Details
Third-Party Contractors subject to New York Education Law § 2-d – please complete the table below

SUPPLEMENTAL INFORMATION ELEMENT	SUPPLEMENTAL INFORMATION
Please list the exclusive purpose(s) for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract (or list the section(s) in the contract where this information can be found)	The sole purpose is the implementation of Pathful products which provides college and career readiness software to K-12 schools. Only necessary data is collected in order for educators and students to access and effectively use the platform. We do not rent or sell Personal Information that we collect from users with third parties.
Please list how the contractor will ensure that any other entities with which it shares the protected data, if any, will comply with the data protection and security provisions of law, regulation and this contract (or list the section(s) in the contract where this information can be found)	All data is encrypted in transit (SSL v1.2+) and at rest (AES 256-bit). Further, all fields containing PII data within our database employ dynamic masking requiring high level access to even see the data. Whereas a very limited set of contracted third parties do have database access in order to provide maintenance and 24x7 coverage, none of these parties have access to the masked fields. Our agreements with these Contractors contain confidentiality and non-disclosure provisions requiring that such Contractors maintain the confidentiality of any personally identifiable information that may be disclosed or made available to them so that Pathful can use Contractor's product or services.
Please list when the agreement expires and what happens to the protected data when the agreement expires (or list the section(s) in the contract where this information can be found)	Pathful certifies that a pupil's records shall not be retained or available to Pathful upon completion of the relationship with the local educational agency. Within 30 days or upon request, all protected data will be deleted by Pathful.
Please list how a parent, student, or eligible student may challenge the accuracy of the protected data that is collected; if they can challenge the accuracy of the data, describe how (or list the section(s) in the contract where this information can be found)	All protected data stored by Pathful is transmitted by the school to Pathful, either via a rostering/sso service (Clever, Classlink, OneRoster, etc) or via secure bulk upload. Pathful does not modify, nor does any user function within Pathful modify this data. Any changes to this data should be made with the school, and such changes will then be communicated to Pathful as part of the regular rostering process.

Please list where the protected data will be stored (described in a way that protects data security), and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated (or list the section(s) in the contract where this information can be found)	All Pathful data is stored within a SOC 2 compliant, secure cloud environment and kept within the continental United States. All data is encrypted in transit (SSL v1.2+) and at rest (AES 256-bit). Further, all fields containing PII data within our database employ dynamic masking requiring high level access to even see the data. Access is granted internally on a "Need to Know" basis, only assigned customer support personnel can access customer records, and all customer support personnel undergo regular background checks.
Please list how the data will be protected using encryption (or list the section(s) in the contract where this information can be found)	See attached Pathful Policies documents for details, but in general all data is stored in a SOC2 compliant environment and encrypted at rest using AES 256 bit encryption. Further all identified PII fields use dynamic data masking. All PII data is deleted within 30 days of customer request or contract termination, whichever is earlier.

Section 3: Agreement and Signature

By signing below, you agree:

- The information provided in this document by the Third-Party Contractor is accurate
- To comply with the terms of Broome-Tioga BOCES Parents' Bill of Rights for Data Privacy and Security (applicable to Third-Party Contractors subject to New York Education Law § 2-d only)

Company Name: Pathful, Inc. Product Name: Pathful Connect

Printed Name: Rosie Munoz Signature Rosie Munoz Date: 02/28/2024

Section 4: Data Privacy Rider for All Contracts Involving Protected Data Pursuant to New York State Education Law §2-C and §2-D

BOCES and the Third-Party Contractor agree as follows:

1. Definitions:
    a. Protected Information means personally identifiable information of students from student education records as defined by FERPA, as well as teacher and Principal data regarding annual professional performance reviews made confidential under New York Education Law §3012-c and §3012-d;
    b. Personally Identifiable Information (PII) means the same as defined by the regulations implementing FERPA (20 USC §1232-g);

2. Confidentiality of all Protected Information shall be maintained in accordance with State and Federal Law and the BOCES's Data Security and Privacy Policy;

3. The Parties agree that the BOCES's Parents' Bill of Rights for Data Security and Privacy are incorporated as part of this agreement, and the Third-Party Contractor shall comply with its terms;

4. The Third-Party Contractor agrees to comply with New York State Education Law §2-d and its implementing regulations;

5. The Third-Party Contractor agrees that any officers or employees of the Third-Party Contractor, and its assignees who have access to Protected Information, have received or will receive training on Federal and State law governing confidentiality of such information prior to receiving access;

6. The Third-Party Contractor shall:
    a. limit internal access to education records to those individuals that are determined to have legitimate educational interests;
    b. not use the education records for any other purposes than those explicitly authorized in its contract or written agreement. Unauthorized use specifically includes, but is not limited to, selling or disclosing personally identifiable information for marketing or commercial purposes or permitting, facilitating, or disclosing such information to another Third-Party for marketing or commercial purposes;
    c. except for authorized representatives of the Third-Party Contractor to the extent they are carrying out the contract or written agreement, not disclose any personally identifiable information to any other party;
        i. without the prior written consent of the parent or eligible student; or
        ii. unless required by statute or court order and the party provides notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by statute or court order;
    d. maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
    e. use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the Secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law §111-5;
    f. adopt technology, safeguards and practices that align with the NIST Cybersecurity Framework;
    g. impose all the terms of this rider in writing where the Third-Party Contractor engages a subcontractor or other party to perform any of its contractual obligations which provides access to Protected Information.

Agreement and Signature

By signing below, you agree to the Terms and Conditions in this Rider:

Company Name: Pathful, Inc. Product Name: Pathful Platform

Printed Name: Rosie Munoz Signature: Rosie Munoz Date: 02/28/2024

Policies

Standards and Policies

Exported on
03/05/2024

Table of Contents

The following documents comprise the standard policies by which Pathful operates. Policies are public information (see page 0) and can be shared upon request to potential and current customers

The status of the documents will progress as follows:

WORKING DRAFT → **READY FOR REVIEW** → **REVISE** (if necessary, else) → **ENACTED**

All policies published below should be considered in force barring those specific sections of each policy that are indicated as under revision.

All policies will be reviewed annually and will revert to **READY FOR REVIEW** during that process.

Policy	Status	Owner	Last Review	
Acceptable Use Policy (see page 14)	ENACTED	Information Security Committee	Abel Lineberger (97 days ago)	
Asset Management Policy (see page 23)	ENACTED	Information Security Committee	Abel Lineberger (97 days ago)	
Auditing Policy (see page 28)	ENACTED	Information Security Committee	Abel Lineberger (97 days ago)	
Breach Notification Policy (see page 30)	ENACTED	Information Security Committee	Abel Lineberger (60 days ago)	
Change Control Policy (see page 33)	ENACTED	Information Security Committee	Abel Lineberger (60 days ago)	
Continuity and Recovery Policy (see page 36)	ENACTED	Information Security Committee	Abel Lineberger (97 days ago)	
Encryption Management Policy (see page 39)	ENACTED	Information Security Committee	Abel Lineberger (97 days ago)	
Identity and Access Management Policy (see page 42)	ENACTED	Information Security Committee	Abel Lineberger (97 days ago)	5
Incident Management Policy (see page 47)	ENACTED	Information Security Committee	Abel Lineberger (97 days ago)	

Policy	Status	Owner	Last Review	
Information and Data Retention Policy (see page 52)	ENACTED	Information Security Committee	Abel Lineberger (97 days ago)	
Information Classification and Management Policy (see page 54)	ENACTED	Information Security Committee	Abel Lineberger (97 days ago)	1
Information Security Policy (see page 60)	ENACTED	Information Security Committee	Abel Lineberger (97 days ago)	2
Network Management Policy (see page 65)	ENACTED	Information Security Committee	Abel Lineberger (97 days ago)	2
Personnel Security and Awareness Training Policy (see page 69)	ENACTED	Information Security Committee	Abel Lineberger (97 days ago)	
Physical Security Policy (... page 72)	ENACTED	Information Security Committee	Abel Lineberger (97 days ago)	
Risk Management Policy (see page 76)	ENACTED	Information Security Committee	Abel Lineberger (97 days ago)	
System Development and Procurement Policy (see page 78)	ENACTED	Information Security Committee	Abel Lineberger (97 days ago)	2
Teleworking Policy (see ... 81)	ENACTED	Information Security Committee	Abel Lineberger (97 days ago)	6
Vendor Management Policy (see page 85)	ENACTED	Information Security Committee	Abel Lineberger (97 days ago)	1
Vulnerability Management Policy (see page 88)	ENACTED	Information Security Committee	Abel Lineberger (97 days ago)	

1 Acceptable Use Policy

Status	**ENACTED**
Owner	Information Security Committee
Last Review	@Abel Lineberger (97 days ago)

1.1 Index

1.2 Acceptable Use

- Personnel are responsible for complying with Pathful policies when using Pathful information resources and/or on Pathful time. If requirements or responsibilities are unclear, please seek assistance from the Information Security Committee.

- Personnel must promptly report harmful events or policy violations involving Pathful assets or information to their manager or a member of the IT or Engineering Teams. Events include, but are not limited to, the following:
    - Technology incident: any potentially harmful event that may cause a failure, interruption, or loss in availability to Pathful Information Resources.
    - Data incident: any potential loss, theft, or compromise of Pathful information.
    - Unauthorized access incident: any potential unauthorized access to a Pathful Information Resource.
    - Facility security incident: any damage or potentially unauthorized access to a Pathful owned, leased, or managed facility.
    - Policy violation: any potential violation to this or other Pathful policies, standards, or procedures.
- Personnel should not purposely engage in activity that may
    - harass, threaten, impersonate, or abuse others;
    - degrade the performance of Pathful Information Resources;
    - deprive authorized Pathful personnel access to a Pathful Information Resource;
    - obtain additional resources beyond those allocated;
    - or circumvent Pathful computer security measures.
- Personnel should not download, install, or run security programs or utilities that reveal or exploit weakness in the security of a system without authorization from the Information Security Committee. For example, Pathful personnel should not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any Pathful Information Resource.
- All inventions, intellectual property, and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information, developed on Pathful time and/or using Pathful Information Resources are the property of Pathful.
- Use of encryption should be managed in a manner that allows designated Pathful personnel to access all data promptly.
- Pathful Information Resources are provided to facilitate company business and should not be used for personal financial gain.
- Personnel are expected to cooperate with incident investigations, including any federal or state investigations.
- Personnel are expected to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using Pathful Information Resources.
- Personnel should not intentionally access, create, store or transmit material that Pathful may deem to be offensive, indecent, or obscene.

1.3 Access Management

- Access to information is based on a "need to know".
- Personnel are permitted to use only those network and host addresses issued to them by Pathful IT or Engineering and should not attempt to access any data or programs contained on Pathful systems for which they do not have authorization or explicit consent.
- All remote access connections made to internal Pathful networks and/or environments must be made through approved and Pathful-provided virtual private networks (VPNs).
- Personnel should not divulge any access information to anyone not specifically authorized to receive such information, including IT support personnel.
- Personnel must not share their (personal) authentication information, including:
    - Account passwords,
    - Personal Identification Numbers (PINs),
    - Security Tokens (i.e. Smartcard),
    - Multi-factor authentication information

    - Access cards and/or keys,
    - Digital certificates,
    - Similar information or devices used for identification and authentication purposes.
- Access cards and/or keys that are no longer required must be returned to Human Resources personnel.
- Lost or stolen access cards, security tokens, and/or keys must be reported to Human Resources personnel as soon as possible.
- A service charge may be assessed for access cards, security tokens, and/or keys lost, stolen, or not returned.

1.4 Authentication/Passwords

- All personnel are required to maintain the confidentiality of personal authentication information.
- Any group/shared authentication information must be maintained solely among the authorized members of the group.
- All passwords, including initial and/or temporary passwords, must be constructed and implemented according to the following Pathful rules:
    - Must meet all requirements, including minimum length, complexity, and reuse history.
    - Must not be easily tied back to the account owner by using things like username, social security number, nickname, relative's names, birth date, etc.
    - Must not be the same passwords used for non-business purposes.
    - Must be stored with company provided password management application if access to such has been provided.
    - Must not be stored within individual browser password stores (Chrome, Firefox, Safari, Apple, etc.).
- Unique passwords should be used for each system whenever possible.
- User account passwords must not be divulged to anyone. Pathful support personnel and/or contractors should never ask for user account passwords.
- If the security of a password is in doubt, the password should be changed immediately.
- Personnel should not circumvent password entry with application remembering, embedded scripts or hard-coded passwords in client software, except for Pathful assigned password management tools.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with Pathful, if issued.

1.5 Clear Desk/Clear Screen

- Personnel should log off from applications or network services when they are no longer needed.
- Personnel should log off or lock their workstations and laptops when their workspace is unattended.
- Confidential or internal information should be removed or placed in a locked drawer or file cabinet when the workstation is unattended and at the end of the workday if physical access to the workspace cannot be secured by other means.
- Personal items, such as phones, wallets, and keys, should be removed or placed in a locked drawer or file cabinet when the workstation is unattended.
- File cabinets containing confidential information should be locked when not in use or when unattended.
- Physical and/or electronic keys used to access confidential information should not be left on an unattended desk or in an unattended workspace if the workspace itself is not physically secured.
- Laptops should be either locked with a locking cable or locked away in a drawer or cabinet when the work area is unattended or at the end of the workday if the laptop is not encrypted.
- Passwords must not be posted on or under a computer or in any other physically accessible location.

- Copies of documents containing confidential information should be immediately removed from printers and fax machines.

1.6 Data Security

- Personnel should use approved encrypted communication methods whenever sending confidential information over public computer networks (Internet).
- Confidential information transmitted via USPS or other mail service must be secured in compliance with the Information Classification and Management Policy (see page 54).
- Only authorized cloud computing applications may be used for sharing, storing, and transferring confidential or internal information.
- Information must be appropriately shared, handled, transferred, saved, and destroyed based on the information sensitivity.
- Personnel should not have confidential conversations in public places or over insecure communication channels, open offices, and meeting places.
- Confidential information must be transported either by a Pathful employee or a courier approved by IT Management.
- All electronic media containing confidential information must be securely disposed. Please contact IT for guidance or assistance.

1.7 Email and Electronic Communication

- Auto-forwarding electronic messages outside the Pathful internal systems is prohibited.
- Electronic communications should not misrepresent the originator or Pathful.
- Personnel are responsible for the accounts assigned to them and for the actions taken with their accounts.
- Accounts must not be shared without prior authorization from Pathful IT, with the exception of calendars and related calendaring functions.
- Employees should not use personal email accounts to send or receive Pathful confidential information.
- Any personal use of Pathful provided email should not:
    - Involve solicitation.
    - Be associated with any political entity, excluding any Pathful-sponsored PAC.
    - Have the potential to harm the reputation of Pathful.
    - Forward chain emails.
    - Contain or promote anti-social or unethical behavior.
    - Violate local, state, federal, or international laws or regulations.
    - Result in unauthorized disclosure of Pathful confidential information.
    - Or otherwise violate any other Pathful policies.
- Personnel should only send confidential information using approved secure electronic messaging solutions.
- Personnel should use caution when responding to, clicking on links within, or opening attachments included in electronic communications.
- Personnel should use discretion in disclosing confidential or internal information in Out of Office or other automated responses, such as employment data, internal telephone numbers, location information or other sensitive data.

1.8 Hardware and Software

- All hardware must be formally approved by IT Management before being connected to Pathful internal networks.
- Software installed on Pathful office equipment must be approved by IT Management and installed by Pathful IT personnel.
- All Pathful assets taken off-site should be physically secured at all times.
- Personnel traveling to a High-Risk location, as defined by FBI and Office of Foreign Asset control, must contact IT for approval to travel with corporate assets.
- Employees should not allow family members or other non-employees to access Pathful Information Resources.

1.9 Internet

- The Internet must not be used to communicate Pathful confidential or internal information, unless the confidentiality and integrity of the information is ensured and the identity of the recipient(s) is established.
- Use of the Internet with Pathful networking or computing resources must only be used for business-related activities. Unapproved activities include, but are not limited to:
    - Accessing or distributing pornographic or sexually oriented materials,
    - Attempting or making unauthorized entry to any network or computer accessible from the Internet.
    - Or otherwise violate any other Pathful policies.
- Access to the Internet from outside the Pathful network using a Pathful owned computer must adhere to all of the same policies that apply to use from within Pathful facilities.

1.10 Mobile Devices and Bring Your Own Device (BYOD)

- All personally owned laptops and/or workstations must have approved virus and spyware detection/protection software along with personal firewall protection active.
- Mobile devices that access Pathful email must have a PIN or other authentication mechanism enabled.
- Confidential information should only be stored on devices that are encrypted in compliance with the Pathful Encryption Standard.
- Pathful confidential information should not be stored on any personally owned mobile device.
- Theft or loss of any mobile device that has been used to create, store, or access confidential or internal information must be reported to the Pathful IT Support Team immediately.
- All mobile devices must maintain up-to-date versions of all software and applications.
- All personnel are expected to use mobile devices in an ethical manner.
- Jail-broken or rooted devices should not be used to connect to Pathful Information Resources.
- In the event that there is a suspected incident or breach associated with a mobile device, it may be necessary to remove the device from the personnel's possession as part of a formal investigation.
- All mobile device usage in relation to Pathful Information Resources may be monitored, at the discretion of Pathful IT Management.
- Pathful IT support for personally owned mobile devices is limited to assistance in complying with this policy. Pathful IT support may not assist in troubleshooting device usability issues.
- Use of personally owned devices must be in compliance with all other Pathful policies.

- Pathful reserves the right to revoke personally owned mobile device use privileges in the event that personnel do not abide by the requirements set forth in this policy.
- Texting or emailing while driving is not permitted while on company time or using Pathful resources. Only hands-free talking while driving is permitted, while on company time or when using Pathful resources.

1.11 Physical Security

- Personnel will not engage in door propping, and any other activities to circumvent door access controls are prohibited.
- Visitors accessing access-controlled areas of facilities must be always accompanied by authorized personnel.

1.12 Privacy

- Information created, sent, received, or stored on Pathful Information Resources are not private and may be accessed by Pathful IT or Engineering employees at any time, under the direction of Pathful executive management and/or Human Resources, without knowledge of the user or resource owner.
- Pathful may log, review, and otherwise utilize any information stored on or passing through its Information Resource systems.
- Systems Administrators, Pathful IT, and other authorized Pathful personnel may have privileges that extend beyond those granted to standard business personnel. Personnel with extended privileges should not access files and/or other information that is not specifically required to carry out an employment related task.

1.13 Removable Media

- The use of removable media for storage of Pathful information must be supported by a reasonable business case.
- All removable media use must be approved by Pathful IT prior to use.
- Personally owned removable media use is not permitted for storage of Pathful information.
- Personnel are not permitted to connect removable media from an unknown origin without prior approval from the Pathful IT.
- Confidential and internal Pathful information should not be stored on removable media without the use of encryption.
- All removable media must be stored in a safe and secure environment.
- The loss or theft of a removable media device that may have contained any Pathful information must be reported to the Pathful IT.

1.14 Security Training and Awareness

- All new personnel must complete an approved security awareness training class prior to, or at least within 30 days of, being granted access to any Pathful Information Resources.
- All personnel must be provided with and acknowledge they have received and agree to adhere to the Pathful Information Security Policies before they are granted to access to Pathful Information Resources.
- All personnel must complete the annual security awareness training.

1.15 Social Media

- Communications made with respect to social media should be made in compliance with all applicable Pathful policies.
- Personnel are personally responsible for the content they publish online.
- Creating any public social media account intended to represent Pathful, including accounts that could reasonably be assumed to be an official Pathful account, requires the permission of the Pathful Communications Departments.
- When discussing Pathful or Pathful -related matters, you should:
    - Identify yourself by name,
    - Identify yourself as an Pathful representative, and
    - Make it clear that you are speaking for yourself and not on behalf of Pathful, unless you have been explicitly approved to do so.
- Personnel should not misrepresent their role at Pathful.
- When publishing Pathful-relevant content online in a personal capacity, a disclaimer should accompany the content. An example disclaimer could be; “The opinions and content are my own and do not necessarily represent Pathful’s position or opinion.”
- Content posted online should not violate any applicable laws (i.e. copyright, fair use, financial disclosure, or privacy laws).
- The use of discrimination (including age, sex, race, color, creed, religion, ethnicity, sexual orientation, gender, gender expression, national origin, citizenship, disability, or marital status or any other legally recognized protected basis under federal, state, or local laws, regulations, or ordinances) in published content that is affiliated with Pathful will not be tolerated.
- Confidential information, internal communications and non-public financial or operational information may not be published online in any form.
- Personal information belonging to customers may not be published online.
- Personnel approved to post, review, or approve content on Pathful social media sites must follow the Pathful Social Media Management Procedures.

1.16 VoiceMail

- Personnel should use discretion in disclosing confidential or internal information in voicemail greetings, such as employment data, internal telephone numbers, location information or other sensitive data.
- Personnel should not access another user’s voicemail account unless it has been explicitly authorized.
- Personnel must not disclose confidential information in voicemail messages.

1.17 Incidental Use

- As a convenience to Pathful personnel, incidental use of Information Resources is permitted. The following restrictions apply:
    - Incidental personal use of electronic communications, Internet access, fax machines, printers, copiers, and so on, is restricted to Pathful approved personnel; it does not extend to family members or other acquaintances.
    - Incidental use should not result in direct costs to Pathful.
    - Incidental use should not interfere with the normal performance of an employee’s work duties.

    - No files or documents may be sent or received that may cause legal action against, or embarrassment to, Pathful or its customers.
- Storage of personal email messages, voice messages, files and documents within Pathful Information Resources must be nominal
- All information located on Pathful Information Resources are owned by Pathful may be subject to open records requests and may be accessed in accordance with this policy.

1.18 Definitions

See Appendix A: Definitions

1.19 References

- ISO 27002: 6, 7, 8, 9, 11, 12, 13, 16, 18
- NIST CSF: PR.AC, PR.AT, PR.DS, DE.CM, DE.DP, RS.CO
- Asset Management Policy (see page 23)
- Encryption Management Policy (see page 39)
- Encryption Standard
- Identity and Access Management Policy (see page 42)
- Incident Management Policy (see page 47)
- Information Classification and Management Policy (see page 54)
- Mobile Device Acknowledgement
- Personnel Security and Awareness Policy (see page 69)
- Physical Security Policy (see page 72)
- Social Media Management Procedure
-

1.20 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

1.21 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

1.22 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments

1.0.0	September 2023		Pathful	Document Origination

2 Asset Management Policy

Status	**ENACTED**
Owner	Information Security Committee
Last Review	@Abel Lineberger (97 days ago)

2.1 Index

2.2 Purpose

The purpose of the Pathful Asset Management Policy is to establish the rules for the control of hardware, software, applications, and information used by Pathful.

2.3 Audience

The Pathful Asset Management Policy applies to individuals who are responsible for the use, purchase, implementation, and/or maintenance of Pathful Information Resources.

2.4 Policy

2.4.1 Hardware, Software, Applications, and Data

- All hardware, software and applications associated with Pathful internal information resources must be approved and purchased by Pathful IT. Hardware, software, and applications associated with ongoing engineering works or external information resources will be approved and purchased by the Pathful Engineering department.
- Installation of new hardware or software, or modifications made to existing hardware or software must follow approved Pathful procedures and change control processes.
- Installation of new hardware or software, or modifications made to existing hardware or software must follow approved Pathful procedures and change control processes.
- All purchases must follow the defined Pathful (Technology) Purchasing Standard.
- Software used by Pathful employees, contractors and/or other approved third parties working on behalf of Pathful, must be properly licensed.
- Software installed on Pathful internal computing equipment, outside of that noted in the Pathful Standard Software List, must be approved by IT Management and installed by Pathful IT personnel.
- Only authorized cloud computing applications may be used for sharing, storing, and transferring confidential or internal information.
- The use of cloud computing applications must be done in compliance with all laws and regulations concerning the information involved, e.g. personally identifiable information (PII), protected health information (PHI), corporate financial data, etc.
- Two-factor authentication is required for external cloud computing applications with access to any confidential information for which Pathful has a custodial responsibility.
- Contracts with cloud computing applications providers must address data retention, destruction, data ownership and data custodian rights.
- Hardware, software, and application inventories must be maintained continually and reconciled no less than annually.
- A general inventory of information (data) must be mapped and maintained on an ongoing basis.
- All Pathful assets must be formally classified with ownership assigned.
- Maintenance and repair of internal organizational assets must be performed and logged in a timely manner and managed by Pathful IT Management.
- Pathful assets exceeding a set value, as determined by management, are not permitted to be removed from Pathful's physical premises without management approval.
- All Pathful physical assets exceeding a set value, as determined by management, must contain asset tags or a similar means of identifying the equipment as being owned by Pathful.
- If a Pathful asset is being taken to a High-Risk location, as defined by the FBI and Office of Foreign Asset Control, it must be inspected and approved by IT before being taken offsite and before reconnecting to the Pathful network.
- Confidential information must be transported either by an Pathful employee or a courier approved by IT Management.
- Upon termination of employment, contract, or agreement, all Pathful assets must be returned to Pathful IT Management.

2.4.2 Mobile Devices

- The use of a personally owned mobile devices to connect to the Pathful network is a privilege granted to employees only upon formal approval of IT Management.
- Mobile devices that access Pathful email must have a PIN or other authentication mechanism enabled.
- Confidential data should only be stored on devices that are encrypted in compliance with the Pathful Encryption Standard.
- All mobile devices should maintain up-to-date versions of all software and applications.

2.4.3 Media Destruction & Re-Use

- Media that may contain confidential or internal information must be adequately obscured, erased, destroyed, or otherwise rendered unusable prior to disposal or reuse.
- Media reuse and destruction practices must be conducted in compliance with Pathful's Media Reuse and Destruction Standards.
- All decommissioned media must be stored in a secure area prior to destruction.
- Media reuse and destruction practices must be tracked and documented.
- All information must be destroyed when no longer needed, included encrypted media.

2.4.4 Backup

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the information owner.
- The Pathful backup and recovery process for each system must be documented and periodically reviewed according to the defined review schedule.
- The vendor(s) providing offsite backup storage for Pathful must be formally approved to handle the highest classification level of information stored.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest Pathful sensitivity level of information stored.
- A process must be implemented to verify the success of the Pathful electronic information backup.
- Backups must be periodically tested to ensure that they are recoverable in accordance with the backup standard.
- Multiple copies of valuable data should be stored on separate media to further reduce the risk of data damage or loss.
- Procedures between Pathful and the offsite backup storage vendor(s) must be reviewed at least annually.
- Backups containing confidential information must be encrypted in accordance with the Encryption Standard

2.4.5 Removable Media

- The use of removable media for storage of Pathful Information must be supported by a reasonable business case.
- All removable media use must be approved by Pathful IT prior to use.
- Personally owned removable media use is not permitted for storage of Pathful information.

- Users are not permitted to connect removable media from an unknown origin, without prior approval from Pathful IT.
- Confidential and internal Pathful information should not be stored on removable media without the use of encryption.
- The loss or theft of a removable media device that may have contained any Pathful information must be reported to the Pathful IT.
- Pathful will maintain inventory logs of all media and conduct media inventories at least annually.
- The transfer of information to removable media will be monitored.

2.4.6 Definitions

See Appendix A: Definitions

2.4.7 References

- ISO 27002: 8, 14, 18
- NIST CSF: ID.AM, PR.DS, PR.IP
- Authentication Standard
- Data Retention Schedule
- Information Labelling Standard
- Media Reuse and Destruction Standard

2.4.8 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

2.4.9 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

2.5 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2023		Pathful	Document Origination

Confidential | For Purposes of Due Diligence Only

3 Auditing Policy

Status	**ENACTED**
Owner	Information Security Committee
Last Review	@Abel Lineberger (97 days ago)

3.1 Index

3.2 Purpose

The purpose of the Pathful Auditing Policy is to establish the requirements for conducting audit-related reviews of information security-resources at Pathful.

3.3 Audience

The Pathful Auditing Policy applies to any individual or process that participates in Pathful Information Security audits in any tangible manner.

3.4 Policy

- All information resources that create, collect, store, and/or process confidential information must be audited on a regular basis, according to a documented schedule.
- The scope and conduct of information resource audits must be done in accordance with documented standards and/or procedures.
- System security audits must be led by information security personnel with the specialized training necessary to conduct such audits.
- Personnel conducting system security audits should communicate the following information to information resource owners, custodians, and users, prior to conducting an audit:
    - The date in which the audit will begin,
    - The date in which the audit will end,
    - The scope of the audit,
    - The purpose of the audit,
    - The potential, even if slight, of service disruption.
- Information resource owners and custodians must provide reasonable access to information resources in order for audit personnel to conduct security audits in accordance with the documented purpose and scope of the audit.
- All pertinent security audit activities and results must be documented.

- Every security audit deficiency must be accompanied with a recommendation.
- Audit summary reports must be created for each system security audit conducted, and the reports must be provided to management at the conclusion of the audit.
- The security of exchanges of information, are the subject of policy development and compliance audits.

3.5 Definitions

See Appendix A: Definitions

3.6 References

- ISO 27002: 12, 18
- NIST CSF: PR.IP, PR.PT, DE.AE, DE.CM, RS.MI
- Incident Management Policy (see page 47)
- Change Control Policy (see page 33)
- Logging Standard
- Vulnerability Management Standard

3.7 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

3.8 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

3.9 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2023		Pathful	Document Origination

4 Breach Notification Policy

Status	**ENACTED**
Owner	Information Security Committee
Last Review	@Abel Lineberger (60 days ago)

4.1 Index

4.2 Purpose

The purpose of the Pathful Breach Notification Policy is to describe the requirements for dealing with a security breach and to comply with applicable state and federal laws and regulations governing notice to affected persons in the event of a security breach.

4.3 Audience

The Pathful Breach Notification Policy applies to individuals that use any Pathful Information Resource.

4.4 Policy

4.4.1 Breach/Incident Reporting

- Any suspected breach of confidential information must be reported to the Chief Product and Technology Officer and the Chief Financial Officer upon detection.
- If applicable, the Pathful Incident Response Plan, Appendix 04 - Notification Requirements procedure must be followed.
- A suspected breach must be considered an information security incident and follow the “incident reporting” outlined in the Pathful Incident Management Policy (see page 47).

- Any suspected breach of COPPA or FERPA protected PII, must follow the procedures contained in the Pathful Incident Management Policy (see page 47).
- Personnel are required to promptly report possible or known information security and confidentiality violations to an external information resource to Pathful Engineering, including the following:
    - Infrastructure incident: any event considered to be a malicious action that causes a failure, interruption, or loss in availability to any Pathful External Information Resource.
    - Data incident: any loss, theft, or compromise of Pathful information.
    - Unauthorized access incident: any unauthorized access to a Pathful External Information Resource.
- Personnel are required to promptly report possible or known information security and confidentiality violations related to an internal information resource to Pathful IT, including the following:
    - Infrastructure incident: any event considered to be a malicious action that causes a failure, interruption, or loss in availability to any Pathful Internal Information Resource.
    - Data incident: any loss, theft, or compromise of Pathful information.
    - Physical asset incident: any loss, theft or compromise of a physical Pathful information asset such as a mobile device, PC/laptop, USB drive, etc.
    - Unauthorized access incident: any unauthorized access to a Pathful Internal Information Resource.
- All reported information security incidents must be assessed by Pathful IT and Engineering to determine the threat type and activate the appropriate response procedures.

4.4.2 Definitions

See Appendix A: Definitions

4.4.3 References

- ISO 27002: 5, 6, 7, 18
- NIST CSF: ID.AM, ID.BE, ID.GV, PR.AT, PR.IP
- Incident Management Policy (see page 47)

4.4.4 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

4.4.5 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

4.5 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments

1.0.0	September 2023		Pathful	Document Origination

5 Change Control Policy

Status	**ENACTED**
Owner	Information Security Committee
Last Review	@Abel Lineberger (60 days ago)

5.1 Index

5.2 Purpose

The purpose of the Pathful Change Control Policy is to establish the rules for the creation, evaluation, implementation, and tracking of changes made to Pathful Information Resources.

5.3 Audience

The Pathful Change Control Policy applies to any individual, entity, or process that create, evaluate, and/or implement changes to Pathful Information Resource.

5.4 Policy

- Changes to production Pathful Information Resources must be documented and classified according to their:
  - Importance,
  - Urgency,
  - Impact, and
  - Complexity.
- Change documentation must include, at a minimum:
  - Date of submission and date of change,
  - Owner and custodian contact information,
  - Nature of the change,
  - Change requestor,
  - Change classification(s),
  - Roll-back plan,
  - Change approver,
  - Change implementer, and
  - An indication of success or failure.
- Changes with a significant potential impact to Pathful Information Resources must be scheduled.

- Pathful Information Resource owners must be notified of changes that affect the systems they are responsible for.
- Authorized change windows must be established for changes with a high potential impact.
- Changes with a significant potential impact and/or significant complexity must have usability, security, and impact testing and back out plans included in the change documentation.
- Change control documentation must be maintained in accordance with the Pathful Information Asset Registry Retention Schedule.
- Changes made to Pathful customer environments and/or applications must be communicated to customers, in accordance with governing agreements and/or contracts.
- All changes must be approved by the Information Resource Owner, Senior VP of Engineering, or Change Control Board (if one is established).
- Emergency changes (i.e. break/fix, incident response, etc.) may be implemented immediately and complete the change control process retroactively.

5.5 Definitions

See Appendix A: Definitions

5.6 References

- ISO 27002: 12.1.2
- NIST CSF: PR.IP-3
- Network Management Policy (see page 65)
- Information Asset Registry Retention Schedule

5.7 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

5.8 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

5.9 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2023		Pathful	Document Origination

Confidential | For Purposes of Due Diligence Only

6 Continuity and Recovery Policy

Status	**ENACTED**
Owner	Information Security Committee
Last Review	@Abel Lineberger (97 days ago)

6.1 Index

6.2 Purpose

The purpose of the Pathful Continuity and Recovery Policy is to provide direction and general rules for the creation, implementation, and management of the Pathful Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).

6.3 Audience

The Pathful Continuity and Recovery Policy applies to individuals accountable for ensuring business continuity and disaster recovery processes are developed, supported, tested, and maintained.

6.4 Policy

6.4.1 Business Continuity

Business Continuity focuses on sustaining the organization's critical business processes during and after a disruption.

- Pathful must create and implement a Business Continuity Plan ("BCP").
- The BCP must be periodically tested and the results should be shared with executive management.
- The BCP must be reviewed and updated upon any relevant change to the organization, at the conclusion of plan testing, or least annually.
- The BCP must be communicated and distributed to all relevant internal personnel and executive management.
- Business continuity planning should ensure that:
    - the safety and security of personnel is the first priority;

    - an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience, and competence;
    - documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event.
- The BCP must include, at a minimum:
    - A risk assessment for critical business processes and operations (Business Impact Analysis);
    - An inventory of critical systems and records, and their dependencies;
    - Requirements for ensuring information security throughout the process;
    - Identification of supply chain relationships and the organization's role to support critical infrastructure;
    - Processes to ensure the safety of personnel;
    - Communication strategies for communications both inside and outside the organization;
    - Mitigation strategies and safeguards to reduce impact;
    - Strategies to address and limit the reputational impact from an event;
    - Contingency plans for different types of disruption events;
    - Protection and availability of plan documentation;
    - Procedures for plan tests, review, and updates.

6.4.2 Disaster Recovery

Disaster Recovery focuses on restoring the technology systems that support both critical and day-to-day business operations.

- Pathful must create and implement a Disaster Recovery Plan ("DRP") to support business objectives outlined in the (BCP/critical processes identified by a Business Impact Analysis).
- The DRP must be tested annually, at a minimum.
- The DRP must be reviewed and updated upon any relevant change to IT Infrastructure, at the conclusion of plan testing, or least annually.
- The DRP must be communicated and distributed to all relevant internal personnel and executive management.
- The Pathful DRP must include at a minimum:
    - Roles and responsibilities for implementing the disaster recovery plan;
    - List of potential risks to critical systems and sensitive information;
    - Procedures for reporting disaster events, event escalation, recovery of critical operations, and resumption of normal operations;
    - Requirements for ensuring information security throughout the process;
    - An inventory of backups and offsite storage locations;
    - Contingency plans for different types of disruption events;
    - Protection and availability of plan documentation;
    - Procedures for plan tests, review, and updates.

6.5 Definitions

See Appendix A: Definitions

6.6 References

- ISO 27002: 17

- NIST CSF: ID.BE, PR.IP, RS.RP, RS.CO, RS.IM, RS.RP, RC.IM, RC.CO
- Information Classification and Management Policy (see page 54)
- Business Continuity Plan
- Disaster Recovery Plan

6.7 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

6.8 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

6.9 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2023		Pathful	Document Origination

7 Encryption Management Policy

Status	**ENACTED**
Owner	Information Security Committee
Last Review	@Abel Lineberger (97 days ago)

7.1 Index

7.2 Purpose

The purpose of the Pathful Encryption Management Policy is to establish the rules for acceptable use of encryption technologies relating to Pathful Information Resources.

7.3 Audience

The Pathful Encryption Management Policy applies to individuals responsible for the setup or maintenance of Pathful encryption technology.

7.4 Policy

All encryption technologies and techniques used by Pathful must be approved by Pathful Engineering for external information resources or by Pathful IT for internal information resources.

7.4.1 External Information Resources

- Pathful Engineering is responsible for the distribution and management of all encryption keys, other than those managed by Pathful customers.
- All use of encryption technology should be managed in a manner that permits properly designated Pathful personnel to promptly access all data, including for purposes of investigation and business continuity.
- Only encryption technologies that are approved, managed, and distributed by Pathful Engineering may be used in connection with Pathful external Information Resources, other than those managed by Pathful customers.
- Pathful Engineering and IT teams will create and publish the Pathful Encryption Standards, which must include, at a minimum:
    - The type, strength, and quality of the encryption algorithm required for various levels of protection.
    - Key lifecycle management, including generation, storing, archiving, retrieving, distributing, retiring, and destroying keys.
- All Pathful information classified as confidential must be encrypted when:
    - Transferred electronically over public networks.
    - Stored on mobile storage devices.
    - Stored on laptops or other mobile computing devices.
    - At rest.
- The use of proprietary encryption algorithms is not permitted, unless approved by Pathful Engineering.
- The use of encryption for any data transferred outside of the United States must be formally approved by Pathful Engineering prior to transfer.

7.4.2 Internal Information Resources

- Pathful IT is responsible for the distribution and management of all encryption keys, other than those managed by Pathful customers.
- All use of encryption technology should be managed in a manner that permits properly designated Pathful personnel to promptly access all data, including for purposes of investigation and business continuity.
- Only encryption technologies that are approved, managed, and distributed by Pathful IT may be used in connection with Pathful internal Information Resources, other than those managed by Pathful customers.
- Pathful IT and Engineering teams will create and publish the Pathful Encryption Standards, which must include, at a minimum:
    - The type, strength, and quality of the encryption algorithm required for various levels of protection.
    - Key lifecycle management, including generation, storing, archiving, retrieving, distributing, retiring, and destroying keys.
- All Pathful information classified as confidential must be encrypted when:
    - Transferred electronically over public networks.
    - Stored on mobile storage devices.
    - Stored on laptops or other mobile computing devices.
    - At rest.
- The use of proprietary encryption algorithms is not permitted, unless approved by Pathful IT.
- The use of encryption for any data transferred outside of the United States must be formally approved by Pathful IT prior to transfer.

7.4.3 Definitions

See Appendix A: Definitions

7.4.4 References

- ISO 27002: 10, 14, 18
- NIST CSF: PR.DS
- Information Classification and Management Policy (see page 54)
- Encryption Standard

7.4.5 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

7.4.6 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

7.5 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2023		Pathful	Document Origination
1.0.1	October 2023		Pathful	Shift responsibility from IT to Engineering.

8 Identity and Access Management Policy

Status	**ENACTED**
Owner	Information Security Committee
Last Review	@Abel Lineberger (97 days ago)

8.1 Index

8.2 Purpose

The purpose of the Pathful Identity and Access Management Policy is to establish the requirements necessary to ensure that access to and use of Pathful Information Resources is managed in accordance with business requirements, information security requirements, and other Pathful policies and procedures.

8.3 Audience

The Pathful Identity and Access Management Policy applies to individuals who are responsible for managing Pathful Information Resource access, and those granted access privileges, including special access privileges, to any Pathful Information Resource.

8.4 Policy

8.4.1 Access Control

- Access to Pathful Information Resources must be justified by a legitimate business requirement prior to approval.
- Where multi-factor authentication is employed, user identification must be verified in person before access is granted.
- Pathful Information Resources must have corresponding ownership responsibilities identified and documented.
- Access to confidential information is based on a "need to know".
- Confidential data access must be logged.
- Access to the Pathful network must include a secure log-on procedure.
- Workstations and laptops must force an automatic lock-out after a pre-determined period of inactivity.
- Documented user access rights and privileges to Information Resources must be included in disaster recovery plans, whenever such data is not included in backups.

8.4.2 Account Management

- All personnel must sign the Pathful Information Security Policy Acknowledgement before access is granted to an account or Pathful Information Resources.
- All accounts created must have an associated, and documented, request and approval.
- Segregation of duties must exist between access request, access authorization, and access administration.
- Information Resource owners are responsible for the approval of all access requests.
- User accounts and access rights for all Pathful Information Resources must be reviewed and reconciled at least annually, and actions must be documented.
- All accounts must be uniquely identifiable using the username assigned by Pathful IT or Engineering and include verification that redundant user IDs are not used.
- All accounts, including default accounts, must have a password expiration that complies with the Pathful Authentication Standard.
- Only the level of access required to perform authorized tasks may be approved, following the concept of “least privilege”.
- Whenever possible, access to Information Resources should be granted to user groups, not granted directly to individual accounts.
- Shared accounts must not be used. Where shared accounts are required, their use must be documented and approved by the Information Resource owner and use compensating controls to ensure non-repudiation.
- User account set up for third-party cloud computing applications used for sharing, storing and/or transferring Pathful confidential or internal information must be approved by the resource owner and documented.
- Upon user role changes, access rights must be modified in a timely manner to reflect the new role.
- Creation of user accounts and access right modifications must be documented and/or logged.
- Any accounts that have not been accessed within a defined period of time will be disabled.
- Accounts must be disabled and/or deleted in a timely manner following employment termination, according to a documented employee termination process.
- System Administrators or other designated personnel:
    - Are responsible for modifying and/or removing the accounts of individuals that change roles with Pathful or are separated from their relationship with Pathful.

- Must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes, and permission changes.
- Must have a documented process for periodically reviewing existing accounts for validity.
- Are subject to independent audit review.
- Must provide a list of accounts for the systems they administer when requested by authorized Pathful IT management personnel.
- Must cooperate with authorized Pathful Information Security personnel investigating security incidents at the direction of Pathful executive management.

8.4.3 Administrator/Special Access

- Administrative/Special access accounts must have account management instructions, documentation, and authorization.
- Administrative/Special access accounts must employ multi-factor authentication for all account logins.
- Personnel with Administrative/Special access accounts must refrain from abuse of privilege and must only perform the tasks required to complete their job function.
- Personnel with Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- Shared Administrative/Special access accounts should only be used when no other option exists.
- The password for a shared Administrative/Special access account must change when an individual with knowledge of the password changes roles, moves to another department or leaves Pathful altogether.
- In the case where a system has only one administrator, there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
- Special access accounts for internal or external audit, software development, software installation, or other defined need, must be administered according the Pathful Authentication Standard.

8.4.4 Authentication

- All passwords, including initial and/or temporary passwords, must be constructed according to the Pathful Authentication Standard,
- Unique passwords should be used for each system, whenever possible.
- Where other authentication mechanisms are used (i.e. security tokens, smart cards, certificates, etc.) the authentication mechanism must be assigned to an individual, and physical or logical controls must be in place to ensure only the intended account can use the mechanism to gain access.
- Stored passwords are classified as confidential and must be encrypted.
- All vendor-supplied default passwords should be immediately updated and unnecessary default accounts removed or disabled before installing a system on the network.
- User account passwords must not be divulged to anyone. Pathful support personnel and/or contractors should never ask for user account passwords.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with Pathful, if issued.
- If the security of a password is in doubt, the password should be changed immediately.
- Administrators/Special Access users must not circumvent the Pathful Authentication Standard for the sake of ease of use.

- Users should not circumvent password entry with application remembering, embedded scripts or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the Pathful IT Management.
- If a password management system is employed, it must be used in compliance with the Pathful Authentication Standard.
- Computing devices should not be left unattended without enabling a password protected screensaver or logging off of the device.
- Pathful IT Support password change procedures must include the following:
    - authenticate the user to the helpdesk before changing password
    - change to a strong password
    - require the user to change password at first login.
- In the event that a user's password is compromised or discovered, the password must be immediately changed, and the security incident reported to Pathful IT support.

8.4.5 Remote Access

- All remote access connections to the Pathful networks will be made through the approved remote access methods employing data encryption and multi-factor authentication.
- Remote users may connect to the Pathful networks only after formal approval by the requestor's manager or Pathful Management.
- The ability to print or copy confidential information remotely must be disabled.
- Users granted remote access privileges must be given remote access instructions and responsibilities.
- Remote access to Information Resources must be logged.
- Remote sessions must be terminated after a defined period of inactivity.
- A secure connection to another private network is prohibited while connected to the Pathful network unless approved in advance by Pathful IT management.
- Non-Pathful computer systems that require network connectivity must conform to all applicable Pathful IT standards and must not be connected without prior written authorization from IT Management.
- Remote maintenance of organizational assets must be approved, logged, and performed in a manner that prevents unauthorized access.

8.4.6 Vendor Access

- Vendor access must be uniquely identifiable, provide non-repudiation, and comply with all existing Pathful policies.
- External vendor access activity must be monitored.
- All vendor maintenance equipment on the Pathful network that connects to the outside world via the network, telephone line, or leased line, and all Pathful Information Resource vendor accounts will remain disabled except when in use for authorized maintenance.

8.5 Definitions

See Appendix A: Definitions

8.6 References

- ISO 27002: 6, 7, 8, 9, 12, 15
- NIST CSF: PR.AC, PR.IP, PR.MA, PR.PT, DE.CM
- Information Classification and Management Policy (see page 54)
- Continuity and Recovery Policy (see page 36)
- Information Security Policy (see page 60) Acknowledgement

8.7 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

8.8 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

8.9 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2023		Pathful	Document Origination

9 Incident Management Policy

Status	**ENACTED**
Owner	Information Security Committee
Last Review	@Abel Lineberger (97 days ago)

9.1 Index

9.2 Purpose

The purpose of the Pathful Incident Management Policy is to describe the requirements for dealing with information security incidents.

9.3 Audience

The Incident Management Policy applies to executive management and other individuals responsible for protecting Pathful Information Resources.

9.4 Policy

9.4.1 Incident Handling Team (IHT)

- An Incident Handling Team (IHT) will be established, consisting of legal experts, risk managers, and other department managers who should be involved in decisions related to incident response.
- The IHT is responsible for:
    - Ensuring that incident response activities are carried out in accordance with legal, contractual, and regulatory requirements.
    - Internal and external communications pertaining to information security incidents.
    - Ensuring that personnel are trained on how to report a potential incident.

9.4.1.1 Response Team

- An Incident Response Commander will be appointed to oversee and direct Pathful incident response activities.
- The Incident Response Commander will assemble and oversee a Cyber Security Incident Response Team (CSIRT).
- The CSIRT will respond to identified cyber security incidents following the Incident Response Plan.
- The Incident Response Commander is responsible for appropriately reporting incidents to the CIO/IHT.

9.4.1.2 Incident Response Plan (IRP)

- The Incident Response Commander is responsible for overseeing the creation, implementation, and maintenance of an Incident Response Plan (IRP).
- The Incident Response Plan must be tested by the CSIRT and IHT no less than annually.

9.4.1.3 Incident Reporting

- Management must provide a means for all personnel to report potential incidents. Reporting methods should ensure that a potential incident is promptly escalated to the appropriate person.
- IT is responsible for monitoring event logging, vulnerability management, and other logs for suspicious activities for Pathful internal information assets.
- Engineering is responsible for monitoring event logging, vulnerability management, and other logs for suspicious activities for Pathful external information assets.
- All reported incidents must be assessed by a member of the CSIRT or IHT to determine the threat type and activate the appropriate response procedures. All members of the CSIRT or IHT must be familiar with how to assess and escalate a potential incident.
- All reported incidents must be recorded in the Incident Handling Log by a member of the CSIRT.
- The Incident Response Commander must report the incident to senior leadership.
- Senior leadership must report any potential breaches and/or incidents involving customer data to the Incident Handling Team (IHT) promptly.

9.4.2 Notification and Communication

The IHT is responsible for ensuring that notification and communication both internally and with third parties (customers, vendors, law enforcement, etc.) based on legal, regulatory, and contractual requirements take place in a timely manner.

All Information concerning an incident is considered confidential, and at no time should any information be discussed with anyone outside of Pathful without approval of executive management and our legal counsel.

9.4.2.1 Personnel

- Personnel should be notified whenever an incident or incident response activities may impact their work activities.
- Internal communications should aim to avoid panic, avoid the spread of misinformation, and notify personnel of appropriate communication channels.

9.4.2.2 Interaction with Law Enforcement

- Interaction between law enforcement and emergency services personnel should be coordinated by the Incident Response Commander or a member of the IHT.
- Legal counsel should be consulted in communications with law enforcement.

9.4.2.3 Customers and Partners

- All customers and partners who are affected by the incident must be notified according to applicable contract language, service level agreements (SLAs), applicable statutes and/or regulations.
- Communications with customers and partners must be consistent, with the same or similar message delivered to each.

9.4.2.4 Regulatory Authorities

- Only members of the IHT are permitted to discuss the nature and/or details of an incident with any regulatory agencies.
- The IHT must contact regulators as required or as soon as practical. (See Incident Response Plan Appendix IV)

9.4.2.5 Public Media

- The IHT or executive management will assign a designated spokesperson responsible for communication with the media.
- Inquiries from media agencies must be directed to the designated spokesperson and the IHT.

Refer to Incident Response Plan: Appendix 05 for guidance in communicating with the Media.

9.5 Definitions

See Appendix A: Definitions

9.6 References

- ISO 27002: 16
- NIST CSF: PR.IP, DE.DP, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS-IM, RC.CO
- Incident Response Plan
- Vulnerability Management Policy (see page 88)
- Logging Standard
- Vulnerability Management Standard

9.7 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

9.8 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

9.9 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2023		Pathful	Document Origination

10 Information and Data Retention Policy

Status	**ENACTED**
Owner	Information Security Committee
Last Review	@Abel Lineberger (97 days ago)

10.1 Index

10.2 Purpose

The purpose of the Pathful Information and Data Retention Policy is to establish the requirements for when to keep and purge information and data resources at Pathful.

10.3 Audience

The Pathful Information and Data Retention Policy applies to any individual or service at Pathful that processes, stores, or otherwise interacts with data on or in various media.

10.4 Policy

- All information stored by Pathful must be retained and purged or destroyed in accordance with the Information Asset Registry Retention Schedule.
- All information maintained by Pathful must include a documented timestamp or include a timestamp as part of metadata.
- Information that is no longer required to be maintained by Pathful is classified as “Expired” and must be purged or destroyed in accordance with the Destruction Standard.
    - Hard Copy Documents - hard copy documents must be shredded.
    - Electronic Records - electronic records at a minimum must be deleted and removed from system recycle bins. (Note: in some cases the media or storage space may required a formal overwrite to ensure complete removal of data. Data owners must determine if the data needs to be overwritten.)
- Data owners should be consulted prior to information destruction and may have the opportunity to extend Information expiration, given business needs and/or requirements for the extended retention.
- Company vendors may have their own information retention requirements that supersede Pathful’s requirements. Such customer requirements should be documented in contractual language.
- Questions regarding this policy or the Information Asset Registry Retention Schedule should be directed to the Pathful IT or Engineering teams.

10.5 Definitions

See Appendix A: Definitions

10.6 References

- ISO 27002: 8, 14, 18
- NIST CSF: ID.AM, PR.DS, PR.IP
- Data Retention Schedule
- Labelling Standard
- Media Reuse and Destruction Standard

10.7 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

10.8 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

10.9 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2023		Pathful	Document Origination

11 Information Classification and Management Policy

Status	**ENACTED**
Owner	Information Security Committee
Last Review	@Abel Lineberger (97 days ago)

11.1 Index

11.2 Purpose

The purpose of the Pathful Information Classification and Management Policy is to provide a system for classifying and managing Information Resources according to the risks associated with its storage, processing, transmission, and destruction.

11.3 Audience

The Pathful Information Classification and Management Policy applies to any individual, entity, or process that interacts with any Pathful Information Resource.

11.4 Responsibilities

11.4.1 Information User

- The person, organization or entity that interacts with Information for the purpose of performing an authorized task.
- Have a responsibility to use Information in a manner that is consistent with the purpose intended and in compliance with policy.

11.4.2 Information Owner

- The person responsible for, or dependent upon, the business process associated with an information resource.
- Is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.
- Determines the appropriate value and classification of information generated by the owner or department.
- Must communicate the information classification when the information is released outside of the department and/or Pathful.
- Controls access to their information and must be consulted when access is extended or modified.
- Must communicate the information classification to the Information Custodian so that the Information Custodian may provide the appropriate levels of protection.
- Must periodically review their information to ensure the proper classification is applied.

11.4.3 Information Custodian

- Maintains the protection of Information according to the information classification associated to it by the Information Owner.
- Delegated by the Information Owner and is usually Information Technology personnel.

11.5 **Policy**

11.5.1 Information Classification

Information owned, used, created or maintained by Pathful should be classified into one of the following three categories:

- Public
- Internal
- Confidential

11.5.1.1 Public Information

- Is information that may or must be open to the general public.
- has no existing local, national, or international legal restrictions on access or usage.
- While subject to Pathful disclosure rules, is available to all Pathful employees and all individuals or entities external to the corporation.
- *Examples of **Public Information** include:*
    - Publicly posted press releases,
    - Publicly available marketing materials,
    - Publicly posted job announcements.

11.5.1.2 Internal Information

- Is information that must be guarded due to proprietary, ethical, or privacy considerations.
- Must be protected from unauthorized access, modification, transmission, storage or other use and applies even though there may not be a civil statute requiring this protection.
- Is restricted to personnel designated by Pathful, who have a legitimate business purpose for accessing such Information.
- *Examples of **Internal Information** include:*
    - Employment Information,
    - Business partner information where no more restrictive confidentiality agreement exists,
    - Internal directories and organization charts,
    - Planning documents,
    - Contracts.

11.5.1.3 Confidential Information

- Is information protected by statutes, regulations, Pathful policies or contractual language. Information Owners may also designate Information as Confidential.
- Is sensitive in nature, and access is restricted. Disclosure is limited to individuals on a “need-to-know” basis only.
- Disclosure to parties outside of Pathful must be authorized by executive management, approved by the Director of Information Technology and/or General Counsel, or covered by a binding confidentiality agreement.
- *Examples of **Confidential Information** include:*
    - Customer data shared and/or collected during the course of a engagement,

- Student Personally Identifiable Information gathered through execution of a contract,
- Financial information, including credit card and account numbers,
- Social Security Numbers,
- Personnel and/or payroll records,
- Any Information identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction,
- Any Information belonging to an Pathful customer that may contain personally identifiable information,
- Patent information.

11.5.2 Information Handling

- All Information should be labelled according to the Pathful Labelling Standard.
- **Public:**
  - Disclosure of Public Information must not violate any pre-existing, signed non-disclosure agreements.
- **Internal:**
  - Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.
  - Must be protected by a confidentiality agreement before access is allowed.
  - Must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
  - Is the "default" classification level if one has not been explicitly defined.
- **Confidential:**
  - When stored in an electronic format must be protected with a minimum level of authentication to include strong passwords as defined in the Authentication Standard.
  - When stored on mobile devices and media, must be encrypted.
  - Must be encrypted at rest.
  - Must be stored in a locked drawer, room, or area where access is controlled by a cipher lock and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.
  - Must not be transferred via unsecure communication channels, including, but not limited to:
    - Unencrypted email
    - Text messaging
    - Instant Messaging
    - Unencrypted FTP
    - Mobile devices without encryption
  - When sent via fax, must be sent only to a previously established and used address or one that has been verified as using a secured location.
  - When transmitted via USPS or other mail service, must be enclosed in a sealed security envelope.
  - Must not be posted on any public website.
  - Pathful Management must be notified in a timely manner if Information classified as Confidential has been or is suspected of being lost or disclosed to unauthorized parties.

11.5.3 Information Retention & Destruction

- All information stored by Pathful must be stored in accordance with the Pathful Data Retention Schedule.
- All information maintained by Pathful must include a documented timestamp or include a timestamp as part of metadata.

- Information that is no longer required to be maintained by Pathful is classified as “Expired” and must be destroyed in accordance with the Pathful Media Reuse and Destruction Standard.
- Information owners should be consulted prior to information destruction and may have the opportunity to extend Information expiration, given business needs and/or requirements for the extended retention.
- Pathful customers may have their own information retention requirements that supersede Pathful’s requirements. Such customer requirements should be documented in contractual language, and recorded within the Pathful Notification Log.

11.5.4 Definitions

See Appendix A: Definitions

11.5.5 References

- ISO 27002: 8, 14, 18
- NIST CSF: ID.AM, PR.DS, PR.IP
- Authentication Standard
- Data Retention Schedule
- Information Labelling Standard
- Media Reuse and Destruction Standard

11.5.6 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

11.5.7 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

11.6 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2023		Pathful	Document Origination

12 Information Security Policy

Status	**ENACTED**
Owner	Information Security Committee
Last Review	@Abel Lineberger (97 days ago)

12.1 Index

12.2 Introduction

Information security is a holistic discipline, meaning that its application, or lack thereof, affects all facets of an organization or enterprise. The goal of the Pathful Information Security Program is to protect the Confidentiality, Integrity, and Availability of the data employed within the organization while providing value to the way we conduct business. Protection of the Confidentiality, Integrity, and Availability are basic principles of information security, and can be defined as:

- **Confidentiality** – Ensuring that information is accessible only to those entities that are authorized to have access, many times enforced by the classic “need to know” principle.
- **Integrity** – Protecting the accuracy and completeness of information and the methods that are used to process and manage it.

- **Availability** – Ensuring that information assets (information, systems, facilities, networks, and computers) are accessible and usable when needed by an authorized entity.

Pathful has recognized that our business information is a critical asset and as such our ability to manage, control, and protect this asset will have a direct and significant impact on our future success.

This document establishes the framework from which other information security policies may be developed to ensure that the enterprise can efficiently and effectively manage, control and protect its business information assets and those information assets entrusted to Pathful by its stakeholders, partners, customers and other third parties.

The Pathful Information Security Program is built around the information contained within this policy and its supporting policies.

12.3 Purpose

The purpose of the Pathful Information Security Policy is to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to Pathful, its business partners, and its stakeholders.

12.4 Audience

The Pathful Information Security Policy applies equally to any individual, entity, or process that interacts with any Pathful Information Resource.

12.5 Responsibilities

12.5.1 Executive Management

- Ensure that an appropriate risk-based Information Security Program is implemented to protect the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of Pathful.
- Ensure that information security processes are integrated with strategic and operational planning processes to secure the organization's mission.
- Ensure adequate information security financial and personnel resources are included in the budgeting and/or financial planning process.
- Ensure that the Security Team is given the necessary authority to secure the Information Resources under their control within the scope of the Pathful Information Security Program.
- Designate an Information Security Officer and delegate authority to that individual to ensure compliance with applicable information security requirements.
- Ensure that the Information Security Officer, in coordination with the Information Security Committee, reports annually to Executive Management on the effectiveness of the Pathful Information Security Program.

12.5.2 Information Security Officer

- Chair the Information Security Committee and provide updates on the status of the Information Security Program to Executive Management.

- Manage compliance with all relevant statutory, regulatory, and contractual requirements.
- Participate in security related forums, associations and special interest groups.
- Assess risks to the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of Pathful.
- Facilitate development and adoption of supporting policies, procedures, standards, and guidelines for providing adequate information security and continuity of operations.
- Ensure that Pathful has trained all personnel to support compliance with information security policies, processes, standards, and guidelines. Train and oversee personnel with significant responsibilities for information security with respect to such responsibilities.
- Ensure that appropriate information security awareness training is provided to company personnel, including contractors.
- Implement and maintain a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of Pathful.
- Develop and implement procedures for testing and evaluating the effectiveness of the Pathful Information Security Program in accordance with stated objectives.
- Develop and implement a process for evaluating risks related to vendors and managing vendor relationships.
- Report annually, in coordination with the Information Security Committee, to Executive Management on the effectiveness of the Pathful Information Security Program, including progress of remedial actions.

12.5.3 Information Security Committee

In accordance with the *Information Security Committee Charter*:

- Ensure compliance with applicable information security requirements.
- Formulate, review and recommend information security policies.
- Approve supporting procedures, standards, and guidelines related to information security.
- Assess the adequacy and effectiveness of the information security policies and coordinate the implementation of information security controls.
- Review and manage the information security policy waiver request process.
- Identify and recommend how to handle non-compliance.
- Provide clear direction and visible management support for information security initiatives.
- Promote information security education, training, and awareness throughout Pathful, and initiate plans and programs to maintain information security awareness.
- Educate the team and staff on ongoing legal, regulatory and compliance changes as well as industry news and trends.
- Identify significant threat changes and vulnerabilities.
- Evaluate information received from monitoring processes.
- Review information security incident information and recommend follow-up actions.
- Report annually, in coordination with the Information Security Officer, to Executive Management on the effectiveness of the Pathful Information Security Program, including progress of remedial actions.

12.5.4 All Employees, Contractors, and Other Third-Party Personnel

- Understand their responsibilities for complying with the Pathful Information Security Program.
- Formally sign off and agree to abide by all applicable policies, standards, and guidelines that have been established.
- Use Pathful Information Resources in compliance with all Pathful Information Security Policies.

- Seek guidance from the Information Security Team for questions or issues related to information security.

12.6 Policy

Pathful maintains and communicates an Information Security Program consisting of topic-specific policies, standards, procedures and guidelines that:

- Serve to protect the Confidentiality, Integrity, and Availability of the Information Resources maintained within the organization using administrative, physical and technical controls.
- Provide value to the way we conduct business and support institutional objectives.
- Comply with all regulatory and legal requirements, including:
    - Children's Online Privacy Protection Act (COPPA)
    - Federal Educational Rights and Privacy Act (FERPA)
    - State breach notification laws,
    - Information Security best practices, including ISO 27002 and NIST CSF,
    - Contractual agreements,
    - All other applicable federal and state laws or regulations.
- The information security program is reviewed no less than annually or upon significant changes to the information security environment.

12.7 Definitions

See Appendix A: Definitions

12.8 References

- ISO 27002: 5, 6, 7, 18
- NIST CSF: ID.AM, ID.BE, ID.GV, PR.AT, PR.IP
- Information Security Committee Charter

12.9 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

12.10 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

12.11 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2023		Pathful	Document Origination

13 Network Management Policy

Status	**ENACTED**
Owner	Information Security Committee
Last Review	@Abel Lineberger (97 days ago)

13.1 Index

13.2 Purpose

The purpose of the Pathful Network Management Policy is to establish the rules for the maintenance, expansion, and use of the network infrastructure.

13.3 Audience

The Pathful Network Management Policy applies to individuals who are involved in the configuration, maintenance, or expansion of the Pathful network infrastructure.

13.4 Policy

13.4.1 General

- Pathful IT owns and is responsible for the Pathful internal network infrastructure and will continue to manage further developments and enhancements to the infrastructure.
- Pathful Engineering owns and is responsible for the Pathful external production, development, and testing environment network infrastructure and will continue to manage further developments and enhancements to the external production, development, and testing environments..

- To provide a consistent network infrastructure capable of leveraging new networking developments, all cabling for internal network infrastructure must be installed by Pathful IT or an approved contractor.
- Information security requirements must be included in any new information system or enhancements to the existing system.
- Appropriate technical controls and solutions must be implemented to protect Confidential information from unauthorized transfer, modification, or disclosure (i.e. next-gen firewalls, IDS/IPS, DLP).
- A map or diagram of the network and data flow, including external connections, must be maintained. This map or diagram must be updated after any changes to the network occur. This diagram should be reviewed every 6 months to ensure it continues to represent the network architecture
- All systems on the internal network must be authenticated. Connections to the network must be authorized by IT.
- All systems on the external production, development, and testing environments must be authenticated. Connections to the related networks must be authorized by Engineering.
- All hardware connected to the Pathful internal network is subject to Pathful IT management and monitoring standards.
- Documented baseline configurations must be maintained for all Information Resources that create, collect, store, and/or process confidential or internal information and all network connected resources must be configured to these specifications.
- Operating procedures for activities associated with information processing must be documented and made available to personnel who need access to them.
- Resource usage must be monitored to ensure the required system performance.
- Information processing facilities must address redundancy sufficient to meet availability requirements.
- Changes to the configuration of active network management devices must be made according to the Change Control Policy (see page 33).
- The Pathful internal network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by Pathful IT Management.
- The Pathful external production, development, and testing network infrastructure support a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by Pathful Engineering Management.
- All connections of the internal network infrastructure to external third-party networks are the responsibility of Pathful IT.
- Groups of information services, users and information systems must be segregated on the network. The perimeter of each domain should be well defined and based on the relevant security requirements.
- Network devices must be installed and configured following Pathful implementation standards.
- The use of departmental network devices is not permitted without the written authorization from Pathful IT Management.
- Personnel are not permitted to access or alter existing network hardware in any way.

13.4.2 Wireless Networking

- All wireless access points or devices that provide access to the Pathful wireless network must be approved by management.
- Wireless access points must be placed in secure locations.
- Wireless networks must be segmented using appropriate technical controls.
- Authentication settings (passwords, encryption keys, etc.) must be changed on a periodic basis as well as anytime it is suspected that such information has been compromised or if anyone with knowledge of the information leaves the organization.

- All wireless network traffic must be encrypted in accordance with the Pathful Encryption Policy (see page 39) and supporting standards, regardless of information sensitivity.
- The Pathful Wireless Network must not be used inappropriately; in particular, persons must not use the network to:
    - Intercept or attempt to intercept other wireless transmissions for the purposes of eavesdropping.
    - Access or run utilities or services which might negatively impact on the overall performance of the network or deny access to the network, e.g. RF jamming, Denial of Service (DoS).
- Pathful wireless network users must not tamper with network access points or security settings.
- Users must not connect to another wireless network and the Pathful wireless network simultaneously.
- Pathful will conduct scans of wireless access points and identify all authorized and unauthorized wireless access points at least quarterly.

13.4.3 Network Cabling

- Core and distribution racks must be secured and not located in visible areas.
- All networking cabling must be protected from unauthorized interception, organized, tied down and labeled.
- All network closets must be secured with auditable controls.
- Demarcation points need to be secured with adequate segregation or isolation.
- All ports on switches must be reconciled and inventoried regularly. Where this is not possible, compensating controls must be used and documented.

13.5 Definitions

See Appendix A: Definitions

13.6 References

- ISO 27002: 6, 9, 11, 12, 13, 17
- NIST CSF: PR.AC, PR.DS, PR.IP, PR.PT, DE.CM
- Change Control Policy (see page 33)
- Vulnerability Management Policy (see page 88)
- Asset Management Policy (see page 23)
- Identity and Access Management Policy (see page 42)
- Encryption Management Policy (see page 39)
- Encryption Standard

13.7 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

13.8 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

13.9 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2023		Pathful	Document Origination

14 Personnel Security and Awareness Training Policy

Status	**ENACTED**
Owner	Information Security Committee
Last Review	@Abel Lineberger (97 days ago)

14.1 Index

14.2 Purpose

The purpose of the Pathful Personnel Security and Awareness Training Policy is to ensure that all personnel with access to Pathful Information Resources are adequately vetted, qualified, and trained according to their role.

14.3 Audience

The Pathful Personnel Security and Awareness Training Policy applies to all individuals responsible for hiring, onboarding, offboarding, and training of personnel given access to Pathful Information Resources.

14.4 Policy

14.4.1 General

- For all roles within Pathful, the hiring process should ensure the candidate has the necessary competence to perform the role and can be trusted to take on the role, especially for roles related to the use, management or protection of information security.
- Information security responsibilities must be communicated to employees as part of the on-boarding process.
- All employees are required to sign a Confidentiality/Non-Disclosure Agreement before being granted access to any information resource.

- Upon termination of employment, personnel must be reminded of confidentiality and non-disclosure requirements.
- Pathful will provide all employees an anonymous process for reporting violations of information security policies or procedures.

14.4.2 Background Checks

- Background checks are required prior to employing Pathful employees, regardless of if a competitive recruitment process is used.
- Background checks may be required for employees who change positions in the company, obtaining more sensitive duties, as determined by Human Resources or the hiring manager.
- Background checks may be required for employees at any time after the employment start date, at the discretion of Human Resources or Executive Management.
- Contractors with access to Pathful confidential information must have a process in place for conducting background checks on applicable staff. An agreement must be put in place specifying the responsibilities for conducting background checks if a procedure is not currently being followed or in question.

14.4.3 Training and Awareness

- All new personnel must complete an approved Security Awareness training prior to, or within 30 days of, being granted access to any Pathful Information Resources.
- All personnel, including third parties and contractors must be provided with relevant information security policies to allow them to properly protect Pathful Information Resources.
- All personnel, including third parties and contractors, must acknowledge they have received and agree to adhere to the Pathful Information Security Policies before they are granted to access to Pathful Information Resources.
- All personnel must complete the annual security awareness training.

14.5 Definitions

See Appendix A: Definitions

14.6 References

- ISO 27002: 7, 13
- NIST CSF: PR.AT, PR.IP, DE.CM
- Information Security Policy (see page 60)
- Confidentiality/Non-Disclosure Agreement

14.7 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

14.8 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

14.9 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2023		Pathful	Document Origination

15 Physical Security Policy

Status	**ENACTED**
Owner	Information Security Committee
Last Review	@Abel Lineberger (97 days ago)

15.1 Index

15.2 Purpose

The purpose of the Physical Security Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to Pathful Information Resource facilities.

15.3 Audience

The Physical Security Policy applies to all individuals that install, support, maintain, or are otherwise responsible for the physical security of Pathful Information Resources.

15.4 Policy

15.4.1 General

- Physical security systems must comply with all applicable regulations including but not limited to building codes and fire prevention codes.

- Physical access to all Pathful restricted facilities must be documented and managed.
- All Information Resource facilities must be physically protected in proportion to the criticality or importance of their function at Pathful.
- Access to Information Resources facilities must be granted only to Pathful support personnel and contractors whose job responsibilities require access to that facility.
- All facility entrances, where unauthorized persons could enter the premises, must be controlled.
- Secure areas must be protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. This includes:
- information processing facilities handling confidential information should be positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use;
- controls should be adopted to minimize the risk of potential physical and environmental threats;
- environmental conditions, such as temperature and humidity, should be monitored for conditions which could adversely affect the operation of information processing facilities.
- Equipment must be protected from power failures and other disruptions caused by failures in utilities.
- Restricted access rooms and locations must have no signage or evidence of the importance of the location.
- All Information Resources facilities that allow access to visitors will track visitor access with a sign in/out log.
- Card access records and visitor logs for Information Resource facilities must be kept for routine review based upon the criticality of the Information Resources being protected.
- Visitors in controlled areas of Information Resource facilities must be accompanied by authorized personnel at all times.
- Personnel responsible for Information Resource physical facility management must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.

15.4.2 Access Cards

- The process for granting card and/or key access to Information Resource facilities must include the approval of physical security personnel.
- Each individual that is granted access to an Information Resource facility must sign the appropriate access and non-disclosure agreements.
- Cards must not be reallocated to another individual, bypassing the return process.
- Physical security personnel must remove the card and/or key access rights of individuals that change roles within Pathful or are separated from their relationship with Pathful.
- Physical security personnel must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.

15.4.3 Utility Systems

- All utility systems in use at the facility must be identified and documented with detailed procedures for overall maintenance requirements.
- Maintenance and testing activities must be performed in accordance to manufacturers specifications and must be documented to provide an audit trail of all activities.
- Utility systems must be secured from unauthorized access.
- Utility systems must be set to alarm on malfunctions.

- Emergency systems, lighting, fire suppression, and emergency power systems, must be in place and tested regularly to ensure functionality.
- Critical utilities must be configured in a redundant manner to ensure continued functionality.

15.4.4 Housekeeping (if third party)

- Housekeeping/cleaning staff must go through standard information security **awareness** training.
- Where external or third parties are used for cleaning services, the third party must be insured and bonded.
- Housekeeping/cleaning staff must have adequate and approved background checks performed.
- Housekeeping/cleaning staff must be (supervised/monitored) while performing required duties.
- Housekeeping/cleaning staff must wear uniforms, badges, and be assigned a unique identifier that provides an audit trail on access to areas of the facility.
- If housekeeping/cleaning staff need to gain access to restricted areas specific clearance from security staff must be obtained.

15.4.5 Loading Docks

- Procedures for delivery and receipt of packages must be documented.
- Delivery areas must be secured and isolated from public areas.
- External doors of the delivery area must be secured when internal doors are open.
- Delivery areas must be locked when unattended. Unauthorized personnel must be accompanied at all times within delivery areas.
- Surveillance cameras must be secured and adequately cover delivery areas.
- Incoming deliveries must be registered, isolated, and inspected for evidence of tampering before being moved to internal areas.
- All discovered evidence of tampering must immediately be reported to physical security personnel.

15.5 Definitions

See Appendix A: Definitions

15.6 References

- ISO 27002: 7, 9, 11, 13, 16
- NIST CSF: PR.AC, PR.IP, PR.PT, DE.CM
- Continuity and Recovery Policy (see page 36)
- Incident Management Policy (see page 47)

15.7 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

15.8 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

15.9 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2023		Pathful	Document Origination

16 Risk Management Policy

Status	ENACTED
Owner	Information Security Committee
Last Review	@Abel Lineberger (97 days ago)

16.1 Index

16.2 Purpose

The purpose of the Pathful Risk Management Policy is to establish the requirements for the assessment and treatment of information security-related risks facing Pathful.

16.3 Audience

The Pathful Risk Management Policy applies to all Pathful individuals that are responsible for management, implementation, or treatment of risk activity.

16.4 Policy

Formal organization-wide risk assessments will be conducted by Pathful no less than annually or upon significant changes to the Pathful environment.

- Risk assessments must account for administrative, physical, and technical risks.
- Information security risk management procedures must be developed and include the following (at a minimum):
    - Risk Assessment
    - Risk Treatment
    - Risk Communication
    - Risk Monitoring and Review
- Risk evaluation criteria should be developed for evaluating the organization's information security risks considering the following:
    - The strategic value of the business information process.
    - The criticality of the information assets involved.
    - Legal and regulatory requirements, and contractual obligations.
    - Operational and business importance of availability, confidentiality, and integrity.
    - Stakeholders expectations and perceptions, and negative consequences for goodwill and reputation.
- All risks will be classified and prioritized according to their importance to the organization, and recorded in the Risk Log.

- Periodically, Pathful may contract with a third-party vendor to conduct an independent risk assessment and/or to validate the effectiveness of the Pathful risk management process.

16.5 Definitions

See Appendix A: Definitions

16.6 References

- ISO 27002: 18
- NIST CSF: ID.GV, ID.RA, ID.RM, PR.IP

16.7 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

16.8 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

16.9 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2023		Pathful	Document Origination

17 System Development and Procurement Policy

Status	**ENACTED**
Owner	Information Security Committee
Last Review	@Abel Lineberger (97 days ago)

17.1 Index

17.2 Purpose

The purpose of the Pathful System Development and Procurement Policy is to establish the rules for evaluating, developing, and/or deploying Information Resources.

17.3 Audience

The System Development and Procurement Policy applies to individuals who participate in the procurement, development, or operation of any Pathful Information Resource.

17.4 Policy

17.4.1 General

- Applications created or deployed inside the Pathful IT environment must follow a standardized application lifecycle established by management.

- Applications should be actively maintained and require periodic updates to address vulnerabilities. If an application is no longer supported by the vendor, developer, or another party, it must be evaluated for replacement.
- At the onset of the acquisition or design planning phase security requirements must be identified and provided in the System Security Requirements Form.
- All software developed must be based on the Secure Software Development Lifecycle Standard.
- Development, testing, and operational environments must be separated.
- Separation of duties and access controls must exist between personnel assigned to the development/test environments and those assigned to the production environment.
- Changes to the system must be made according to the Pathful Change Control Policy (see page 33).
- The production data source must be sanitized before use in development or test environment and production/ test access controls must comply with production standards.
- Test data and accounts must be removed before a production system becomes active.

17.4.2 Secure Software Development

- All software development personnel must receive training in writing secure code for their specific development environment.
- A Secure Software Development Lifecycle Standard must be developed and implemented.
- Access to program source code should be restricted based on principle of least privilege.
- For applications that store or transmit confidential information, security controls must be implemented to limit output to minimum necessary as defined by the user.
- Any outsourced software development should comply with the Secure Software Development Lifecycle Standard recommendations.
- Modifications to externally developed software packages must be limited to necessary changes and all changes should be strictly controlled.
- All newly developed software and updates or revisions to existing software must be fully tested and accepted prior to deployment to the production environment.

17.4.3 System Procurement

- Procurement of new hardware and software must be authorized by Information Technology and requested through the company procurement process.
- Information Technology must perform a review of all new hardware or software prior to final purchase commitment to ensure that necessary security controls can be configured.
- All newly procured hardware and software must be fully tested and accepted prior to deployment to the production environment.
- Deployment of new hardware and software to the production environment must be in accordance with the Change Control Policy (see page 33).

17.4.4 System Acceptance

- Acceptance criteria must be provided by the application\resource owner and should specify:
    - operational and functional requirements of the application,
    - performance and capacity requirements,
    - data classification,

    - hardware specifications, if applicable.
- All acceptance criteria must be satisfied before any system or application can move into a production environment.

17.5 Definitions

See Appendix A: Definitions

17.6 References

- ISO 27002: 7, 9, 12, 14
- NIST CSF: PR.AT, PR.DS, PR.IP
- Change Control Policy (see page 33)
- Secure Software Development Lifecycle Standard
- System Security Requirements Form

17.7 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

17.8 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

17.9 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2023		Pathful	Document Origination

18 Teleworking Policy

Status	**ENACTED**
Owner	Information Security Committee
Last Review	@Abel Lineberger (97 days ago)

18.1 Index

18.2 Purpose

This policy aims to establish the rules and conditions under which short and long-term telecommuting may occur to maintain acceptable practices regarding the use and protection of Pathful Information Resources.

18.3 Audience

The Pathful Teleworking Policy applies to anyone connecting remotely to Pathful information resources.

18.4 Policy

18.4.1 General Requirements

- Personnel must be approved by their manager and IT prior to remote access or teleworking. Under no circumstance is a person permitted to work remotely without prior permission.
- Personnel are responsible for complying with Pathful policies when working using Pathful Information Resources and/or on Pathful time. If requirements or responsibilities are unclear, please seek assistance from the Security Committee. (duplicate from AUP (see page 14))
- All inventions, intellectual property, and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information, developed on Pathful time and/or using Pathful Information Resources are the property of Pathful. (duplicate from AUP (see page 14))
- The teleworker is responsible for ensuring that non-employees do not access Pathful data, including in print or electronic form.
- The team member will be required to maintain a regular schedule. All hours of work must be recorded according to regular Pathful policies. Overtime and time off must have advance approval according to the regular policies of Pathful.
- Equipment and information must be protected according to their classification and in alignment with the Information Classification and Management (see page 54) policy. Teleworkers are responsible for protecting Pathful equipment and information from theft, damage, or other loss while in transit or at the remote work location. At no time should documents or company equipment be left unattended in a public area.
- Personnel are expected to follow Pathful's Acceptable Use policy (see page 14) when using Pathful devices remotely.

18.4.2 Internet Connection

- Personnel must not connect to an unsecured Wi-Fi network with Pathful equipment or to perform Pathful work.
- Wi-Fi connections must be secured with strong encryption (WPA2). The use of WPA or WAP is not allowed.
- When connecting to a Wi-Fi network, personnel must use only the pre-approved VPN solution.
- Users must not connect to another wireless network and the Pathful wireless network simultaneously.
- The use of split-tunnel VPN is prohibited.
- For long-term or home office networks:
    - A high-speed Internet connection is required. Personnel will provide the Internet service at their own expense. The internet connection must be of sufficient bandwidth to allow the team member to perform their regular job functions efficiently.
    - ~~IT will determine if the person's network is secure or whether a company-issued wireless router will be needed OR teleworkers will comply with [Teleworking Procedures] for implementing wireless networks securely.~~
    - Wireless networks must be secured with a strong password, consisting of 16 or more characters.
    - When possible, the home network used with Pathful Information Resources should be isolated from other devices and computers in the home.

18.4.3 Equipment

- ~~Only Pathful-provided computing devices, such as desktops and laptops, may be used for working remotely.~~
- Computing devices must be secured with Pathful provided or approved:
    - Active and up-to-date antivirus software
    - Active local firewall
    - Full-disk encryption
    - Automatic screen lock
- Personnel are responsible for regularly rebooting their device to allow software patches and updates to be installed.
- Personally owned devices, including but not limited to USB memory, portable hard drives, mobile phones, MP3 players, iPods/iPads, and smart gadgets, are not allowed to be connected to Pathful equipment, including wireless connections.
- Maintenance of Pathful-provided equipment must be provided or preapproved by IT.

18.4.4 Printing

- The printing of any non-public Pathful information must be preapproved by the Information Owner.
- The printing of any non-public Pathful information to a public printer is prohibited.
- Personnel must be preapproved by IT Technology and their manager for printing at a remote location. Personnel approved to print must have (or be supplied with) a shredder.
    - IT will determine if the person's network is secure or whether a company-issued wireless router will be needed.
    - The device used to print must be directly connected to the printer used. Wireless printing must be pre-approved by Information Technology and requires the use of strong encryption.
- All non-public Pathful information must secured when not in use and shredded when no longer needed in accordance with Pathful's Information Classification and Management policy.
- The printing of Confidential information at a remote location is not permitted.

18.4.5 Telephone

- Remote personnel must use the Pathful provided phone or headset for all Pathful related calls.
- When other people are present in the remote work location, a headset must be used to safeguard the conversation.

18.4.6 Office Requirements

- Workspaces must be secured to protect all Pathful equipment and maintain the confidentiality of all information related to the organization and/or its customers.
- Personnel must allow IT to inspect and/or retrieve the equipment provided to them at any time.
- The Pathful may inspect and/or retrieve any Pathful information maintained at home by personnel.
- The use of personal video surveillance on home entrances and exits is encouraged.

18.5 Definitions

See Appendix A: Definitions

18.6 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

18.7 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

18.8 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2023		Pathful	Document Origination

19 Vendor Management Policy

Status	**ENACTED**
Owner	Information Security Committee
Last Review	@Abel Lineberger (97 days ago)

19.1 Index

19.2 Purpose

The purpose of the Pathful Vendor Management Policy is to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to Pathful, its business partners, and its stakeholders from any of its vendors.

19.3 Audience

The Pathful Vendor Management Policy applies to any individuals that interacts, set up or manage any Pathful vendors.

19.4 Policy

19.4.1 Assessments

- Vendors granted access to Pathful Information Resources must sign the Pathful Vendor Non-Disclosure Agreement/Business Associate Agreement.
- Vendors must be evaluated prior to the start of any service and thereafter on an annual basis.
- High risk findings must be followed up to verify remediation.
- A vendor risk assessment must be performed on vendors with physical or logical access to confidential information or that are considered critical vendors.
- Risk assessments must be performed on all requested cloud providers before approval.
- Vendors with PCI DSS compliance requirements must have their status reviewed on an annual basis.

19.4.2 Management

- Vendor agreements and contracts must specify:
  - The Pathful information the vendor should have access to,
  - How Pathful information is to be protected by the vendor,
  - How Pathful information is to be transferred between Pathful and the vendor,
  - Acceptable methods for the return, destruction or disposal of Pathful information in the vendor's possession at the end of the contract,
  - Minimum information security requirements,
  - Incident response requirements,
  - Right for Pathful to audit vendor.
- If a vendor subcontracts part of the information and communication technology service provided to Pathful, the vendor is required to ensure appropriate information security practices throughout the supply chain and to notify Pathful.
- The vendor must only use Pathful Information Resources for the purpose of the business agreement.
- Work outside of defined parameters in the contract must be approved in writing by the appropriate Pathful point of contact.
- Vendor performance must be reviewed annually to measure compliance to implemented contracts or SLAs. In the event of non-compliance with contracts or SLAs regular meetings will be conducted until performance requirements are met.
- Vendor's major IT work activities must be entered into or captured in a log and available to Pathful IT management upon request. Logs must include, but are not limited to, events such as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.
- Any other Pathful information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others.
- Vendor personnel must report all security incidents directly to the appropriate Pathful IT personnel within the timeframe defined in the contract.
- In the case of works on Pathful internal information resources Pathful IT will provide a technical point of contact for the vendor. The point of contact will work with the vendor to make certain the vendor is in compliance with these policies.
- In the case of works on Pathful external information resources Pathful Engineering will provide a technical point of contact for the vendor. The point of contact will work with the vendor to make certain the vendor is in compliance with these policies.
- New vendors must provide Pathful a list of key personnel working on the contract.
- Vendors with logical access to information resources must provide non-repudiation authentication mechanisms.
- Vendors must provide Pathful with notification of key staff changes within 24 hours of change.
- Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to Pathful or destroyed within 24 hours.
- Upon termination of contract, vendors must be reminded of confidentiality and non-disclosure requirements.
- Upon termination of contract or at the request of Pathful, the vendor must surrender all Pathful badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized Pathful IT management.

19.5 Definitions

See Appendix A: Definitions

19.6 References

- ISO 27002: 7, 13, 15, 16
- NIST CSF: DE.CM
- Vendor Non-Disclosure Agreement/Business Associate Agreement

19.7 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

19.8 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

19.9 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2023		Pathful	Document Origination
1.1.0	November 2023		Pathful	Split areas of responsibility between IT and Engineering

20 Vulnerability Management Policy

Status	**ENACTED**
Owner	Information Security Committee
Last Review	@Abel Lineberger (97 days ago)

20.1 Index

20.2 Purpose

The purpose of the Pathful Vulnerability Management Policy is to establish the rules for the review, evaluation, application, and verification of system updates to mitigate vulnerabilities in the IT and Engineering environments and the risks associated with them.

20.3 Audience

The Pathful Vulnerability Management Policy applies to individuals who are responsible for Information Resource management.

20.4 Policy

20.4.1 Endpoint Protection (Anti-Virus & Malware)

- All Pathful owned and/or managed internal Information Resources must use the Pathful IT management approved endpoint protection software and configuration.
- All Pathful owned and/or managed external Information Resources must use the Pathful Engineering management approved endpoint protection software and configuration.
- All non-Pathful owned workstations and laptops must use Pathful IT management approved endpoint protection software and configuration, prior to any connection to a Pathful internal Information Resource.
- All non-Pathful owned workstations and laptops must use Pathful Engineering management approved endpoint protection software and configuration, prior to any connection to a Pathful external Information Resource.
- The endpoint protection software must not be altered, bypassed, or disabled.
- Each email gateway must utilize Pathful IT management approved email virus protection software and must adhere to the Pathful rules for the setup and use of this software, which includes, but is not limited to, scanning of all inbound and outbound emails.
- Controls to prevent or detect the use of known or suspected malicious websites must be implemented.
- All files received over networks or from any external storage device must be scanned for malware before use.
- Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to Pathful IT Support.

20.4.2 Logging & Alerting

- Documented baseline configurations for Information Resources must include log settings to record actions that may affect, or are relevant to, information security.
- Event logs must be produced based on the Pathful Logging Standard and sent to a central log management solution.
- A review of log files must be conducted periodically.
- All exceptions and anomalies identified during the log file reviews must be documented and reviewed.
- Pathful will use file integrity monitoring or change detection software on logs and critical files to alert personnel to unauthorized modification.
- Log files must be protected from tampering or unauthorized access.
- All servers and network equipment must retrieve time information from a single reference time source on a regular basis so that timestamps in logs are consistent.
- All log files must be maintained for at least one year.

20.4.3 Misconfigurations

- Security reviews of all cloud systems, codebases, application programming interfaces (APIs), and any other systems or tools must be conducted at least annually or after any significant change occurs.
- Security reviews will consider common cloud security vulnerabilities, conduct user access reviews, and reference recognized security hardening standards and guides (i.e., CIS Benchmarks).

- All code developed by Pathful must be assessed regularly for misconfigurations, security concerns, and any other potential issues via both dynamic and static code analysis.

20.4.4 Patch Management

- The Pathful IT team maintains overall responsibility for patch management implementation, operations, and procedures for internal information resources.
- The Pathful Engineering team maintains overall responsibility for patch management implementation, operations, and procedures for external information resources.
- All Information Resources must be scanned on a regular basis to identify missing updates.
- All missing software updates must be evaluated according to the risk they pose to Pathful.
- Missing software updates that pose an unacceptable risk to Pathful Information Resources must be implemented within a time period that is commensurate with the risk as determined by the Pathful Vulnerability Management Standard.
- Software updates and configuration changes applied to Information Resources must be tested prior to widespread implementation and must be implemented in accordance with the Pathful Change Control Policy (see page 33).
- Verification of successful software update deployment will be conducted within a reasonable time period as defined in the Pathful Vulnerability Management Standard.

20.4.5 Penetration Testing

- Penetration testing of the internal network, external network, web applications, and hosted applications must be conducted at least annually or after any significant changes to the environment.
- Penetration tests will look for common vulnerabilities in identified systems, including those that interact with sensitive data (i.e., PII data).
- Any exploitable vulnerabilities found during any penetration test will be corrected and re-tested to verify the vulnerability was corrected.

20.4.6 Vulnerability Scanning

- Vulnerability scans of the internal and external network must be conducted at least quarterly or after any significant change to the network.
- Failed vulnerability scan results rated at Critical or High will be remediated and re-scanned until all Critical and High risks are resolved.
- Any evidence of a compromised or exploited Information Resource found during vulnerability scanning must be reported to the Pathful Information Security Officer and IT support.
- Upon identification of new vulnerability issues, configuration standards will be updated accordingly.

20.5 Definitions

See Appendix A: Definitions

20.6 References

- ISO 27002: 12, 18
- NIST CSF: PR.IP, PR.PT, DE.AE, DE.CM, RS.MI
- Incident Management Policy (see page 47)
- Change Control Policy (see page 33)
- Logging Standard
- Vulnerability Management Standard

20.7 Waivers

Waivers from certain policy provisions may be sought following the Pathful Waiver Process.

20.8 Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

20.9 Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2023		Pathful	Document Origination
1.1.0	November 2023		Pathful	Split areas of responsibility between IT and Engineering