Promptly Health, S.A.

Rua das Condominhas, 15, 4150-222 Porto

Information Security & Acceptable Use

Owner: Promptly health

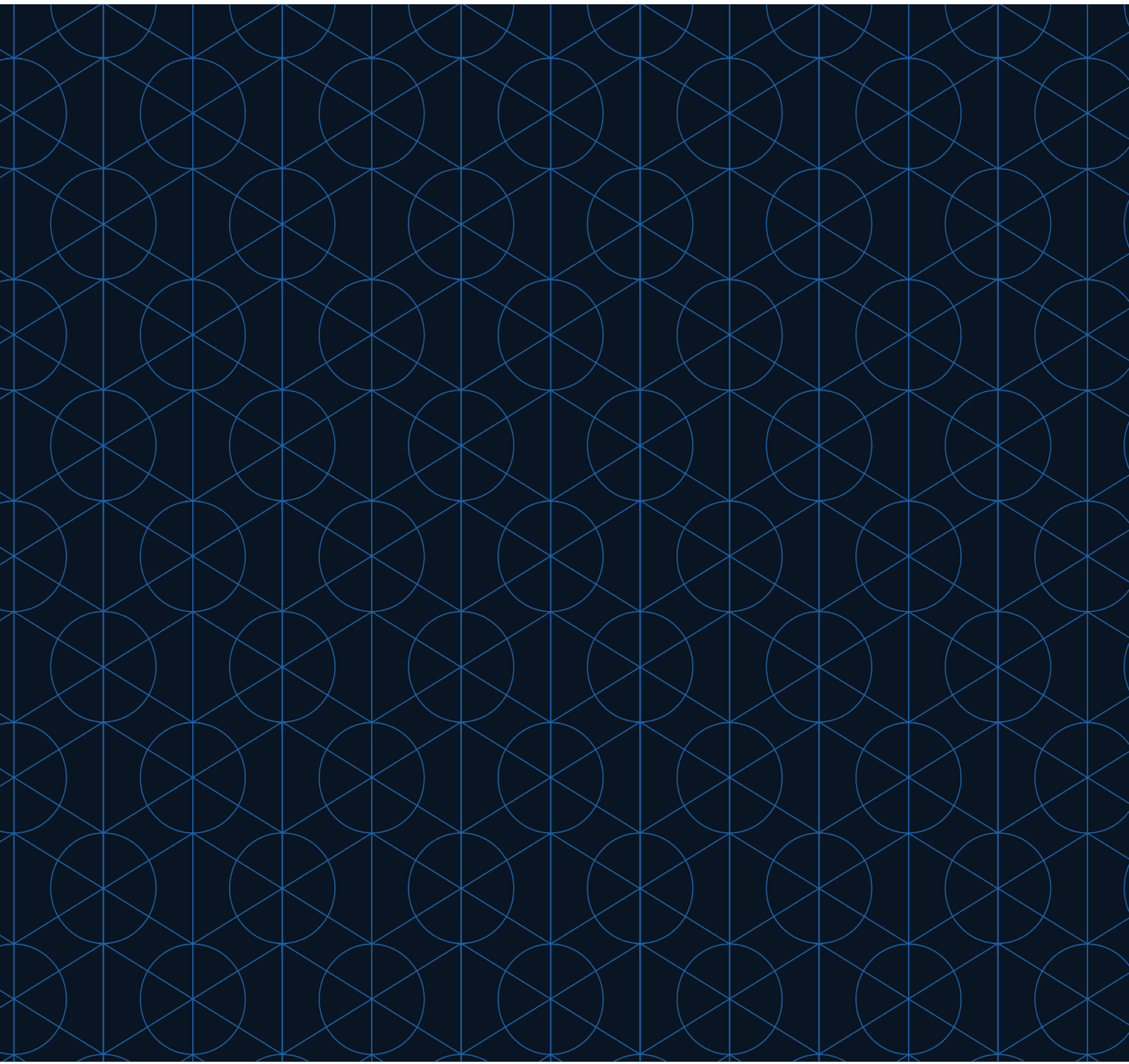
Approver: Ivan Pereira

Classification: Company Internal

Document ID: POL-04

Version: 1.0

Effective Date: 28/06/2023



Promptly Health, S.A.

Rua das Condominhas, 15, 4150-222 Porto

Table of contents

ISO 27001 Coverage

C.5.1; C.5.2; C.7.2; C.7.3; A.5.1.1; A.5.1.2; A.6.2.1; A.6.2.2; A.7.1.2; A.7.2.1; A.7.2.3; A.8.1.3; A.8.2.3; A.9.2.4; A.9.3.1; A.11.2.6; A.11.2.8; A.11.2.9; A.12.5.1; A.12.6.2; A.16.1.3

1 Version History

Version #	Date	Author	Change detail
v1.0	25 Aug 2021	Nuno Salgado	Initial proposal

2 Document Goal

This document is for internal use only. Distribution of this document outside of Promptly requires approval from Information Security Management Leader at security@promptlyhealth.com

The purpose of this document is to outline the acceptable and unacceptable use of information and IT assets provided or managed by Promptly. The acceptable use rules are in place to protect Promptly, it's employees, partners and customers from various information security risks like virus attacks, compromise of IT assets & services, unauthorized disclosure or theft of personal and business sensitive information potentially leading to legal & regulatory non-compliance, reputational damage, operational disruption and/or financial loss. These best practices also provide valuable guidance to the users in protecting their personal digital identity online, which remains users' responsibility.

Promptly has designated a senior level information security official as Chief Information Security Officer's (hereafter referred to as Information Security Management Leader) responsible for direction and oversight of the security program. Information Security Management Leader's intentions for publishing an Information Security Policy are not to impose restrictions that are contrary to Promptly's established culture of openness, trust and integrity. Information Security Management Leader is committed to protecting Promptly's employees and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including, but not limited to computer equipment, mobile devices, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing and Cloud computing, that are provided by Promptly are the property of Promptly. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Promptly employee and affiliates who deal with information and/or IT assets. It is the responsibility of every Employee, consultant, contractor and other third-party who use Promptly information and IT assets to know the requirements stated in this policy, and to conduct their activities accordingly.

Promptly management is committed to continuously invest and improve ISMS controls and efforts with appropriate human, technical and procedural support, as well as ensure that all required elements are met in order to establish, implement, maintain and continually improve the ISMS.

2.1 Scope of the document

This document applies to all Employees, consultants, contractors and other third-parties who use Promptly information and IT assets (hereafter referred to as IT Users).

2.2 Audience and roles

- Managing directors are responsible for approving the Policy.

- Information Security Management Leader is responsible for creating, reviewing, and updating the Policy.
- Implementation responsibilities are defined in each segment respectively.
- All employees are responsible for reading, acknowledging and practicing requirements in this Policy segment.

2.3 System Owners

- System owners are responsible for a specific system used to support Promptly business goals, by ensuring the system is functioning properly and is used for intended business purpose, access to the system is strictly regulated, reviewed and access granted based on least-privilege and need-to-know principles.
- System owner role is assigned by Information Security Management Leader to an individual most familiar with the system they have been assigned for and with relevant experience and training to manage the system in question.
- System Owners are responsible to assist Information Security Management Leader in the quarterly User Access review process.

2.4 Table of definitions, terms and abbreviations

Term	Description
Business Sensitive Information	Promptly information which is classified as “Internal” or “Confidential”, per classification matrix in POL-14 Data Management, will be considered as business sensitive information. It includes anything that poses a risk to the company if discovered by a competitor or general public. Such information includes trade secrets, acquisition plans, financial data and supplier and customer information, among other possibilities. For the purpose of this document, Sensitive Personally Identifiable Information (PII) and Protected Health Information (PHI) are also included in this broad definition of Business Sensitive Information.
IT User	The term “IT User” refers to any person authorized to access the IT tools, resources of Promptly (and those of its entities) and to make use of them: Employees(staff), contractors, temporary personnel, service provider personnel, etc.
IT Asset	The term “IT Asset” refers to any information, system or hardware that is used in the course of business activities. It can be a device such as a notebook, smartphone, network equipment, conferencing equipment and an information system such as an information or communication technology used by Promptly or authorized third party to provide a service i.e. AWS cloud hosting platform, third party applications, internally developed systems. This refers to company-owned assets, acquired third party assets and personal assets that are subject to BYOD policy in this document.

3 General Information Security Policy

Protect Promptly's informational and IT assets (including but not limited to all computers, mobile devices, networking equipment, software and sensitive data) against all internal, external, deliberate or accidental threats and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems;

Ensure information will be protected against any unauthorized access. Users shall only have access to resources that they have been specifically authorized to access. The allocation of privileges shall be strictly controlled and reviewed regularly.

Protect CONFIDENTIALITY of information. When we talk about confidentiality of information, we are talking about protecting the information from disclosure to unauthorized parties;

Ensure INTEGRITY of information. Integrity of information refers to protecting information from being modified by unauthorized parties;

Maintain AVAILABILITY of information for business processes. Availability of information refers to ensuring that authorized parties can access the information when needed.

Comply with and, wherever possible, exceed, national legislative and regulatory requirements, standards and best practices;

Develop, **Maintain** and **Test** business continuity plans to ensure we stay on course despite all obstacles that we may come across. It is about "keeping calm and carrying on!";

Raise awareness of information security by making information security training available for all Employees. Security awareness and targeted training shall be conducted consistently, security responsibilities reflected in job descriptions, and compliance with security requirements shall be expected and accepted as a part of our culture;

Ensure that no action will be taken against any employee who discloses an information security concern through reporting or in direct contact with Information Security Management Leader, unless such disclosure indicates, beyond any reasonable doubt, an illegal act, gross negligence, or a repetitive deliberate or willful disregard for regulations or procedures;

Report all actual or suspected information security breaches to security@promptlyhealth.com or by using the form linked in POL-17 Incident Management, Appendix B

3.1 Enforcement, Exceptions and Complaints

Non-conformance to policy and standard statements in this Policy could result in disciplinary action including, but not limited to, informal or formal warnings, up to termination of contract. Any exceptions to what is governed will require written authorization by email from Information Security Management Leader. Exceptions granted will be issued a policy waiver for a defined period of time. All target users of this Policy can submit complaints to its contents to Information Security Management Leader at any point. All complaints will be filed and processed accordingly where Information Security Management Leader will respond within 14 days of initial submission. Requests

for exceptions to this policy as well as complaint submissions will be addressed to Information Security Management Leader at email.

4 Acceptable Use of Promptly IT Assets

4.1 Roles in scope

- Information Security Management Leader and Department heads are jointly responsible for Implementation of this Policy segment in their respective teams.
- All IT Users are obliged to read, acknowledge and comply with the rules defined in this segment.

4.2 Basic rules

1. Promptly's **Business Sensitive Information** (see Table of definitions on page 3) and IT assets remain the sole property of Promptly. Every IT User shares a responsibility to protect it from unauthorized disclosure, loss, modification, tampering and/or destruction. This is applicable for personal devices approved to be used for business purposes.
2. IT Users are accountable for the actions performed using their access credentials provided by the company to access Promptly Business Sensitive Information and IT assets. All access requests shall be approved by the IT Users supervisor and managed by Information Security Management Leader. Please see POL-11 Access Control
3. Only reviewed and approved software shall be used for business purposes, reviewed and approved by Information Security Management Leader based on internal privacy and security requirements and applicable regulations. Full list of approved software is appended in *Appendix A - List of approved software*. Any requirement for new software shall be directed to Information Security Management Leader for formal review and approval.
4. Promptly Business Sensitive Information and IT assets must be used primarily for business purposes and in accordance with the principles of need-to-know and need-to-have and least privilege.
5. Limited personal usage of IT assets (like email, Internet, etc.) is permitted if such use is occasional, of reasonable duration, does not adversely affect the business and performance, does not violate security policies of Promptly, local and International laws, and is not otherwise prohibited by applicable legislations and regulations.
6. All persons who have been given temporary or permanent Promptly access control cards should keep them on their persons at all times while staying in Promptly premises. Giving the access control card to another person is strictly prohibited. If an access control card is lost or stolen, the IT User shall be under the obligation to immediately report the incident to Information Security Management Leader at security@promptlyhealth.com. If an access card is forgotten, a temporary access control card will be provided at the reception desk or

by Information Security Management Leader. The temporary access control card is valid one day, and shall be returned at the end of working hours.

7. For security and maintenance purposes only, authorized personnel within Promptly and/or its authorized third-parties may audit and monitor equipment, systems and network traffic.
8. IT Users shall not tamper with any operational controls or attempt to prove any weakness in the systems without adequate authorization. Malicious hackers, snoopers, password stealers, virus installers, data erasers, and anyone involved in such activity will be subject to disciplinary actions.
9. IT Users are responsible to promptly report any suspicious or malicious events, theft, loss, or unauthorized access/disclosure of Business Sensitive Information and IT assets to security@promptltyhealth.com.
10. All Employees are responsible for completing the security awareness courses, which are periodically organized by the HR department and executed by Information Security Management Leader.
11. Special attention shall be paid so that contents which include, but are not limited to, pornographic, insulting, racist or other contents of discriminatory character are not allowed to be downloaded, distributed, visited, used or browsed using Promptly's IT assets. Unauthorised use and copying of copyright-protected materials, including, but not limited to digitalisation and distribution of photos from magazines, books or other sources protected by copyrights of music, films and other multimedia contents protected by copyrights and installation of software for which Promptly doesn't have a valid licence, shall be strictly prohibited.
12. The unauthorised use or attempt to use Promptly IT assets shall not be allowed. This includes unauthorised access, processing and/or distribution of Business Sensitive Information.
13. Disclosing one's own access parameters (e.g. username, password, PIN code) to other personnel shall not be permitted without written approval from Information Security Management Leader. Unauthorised use or attempts to use other IT users' access parameters shall be strictly prohibited. Access parameters are created per companies Acceptable and Unacceptable Use of User Accounts and Passwords segment in this document. Exceptions to these two rules can only be distributed in written form by Information Security Management Leader.
14. Every violation of and/or deviation from the rules provided herein, failure to observe them and/or abuse of rights and authority hereunder granted to IT users shall constitute a violation of work duty and, therefore, may lead to disciplinary action up to termination of contract.

4.3 Compliance with Legal Obligations

IT users are subject to specific obligations, based on applicable external and internal requirements, to protect Promptly IT assets and reputation of Promptly. IT Users are required to comply with applicable legal and regulatory provisions in this area, including those that penalize contraventions of accepted

moral standards, the diffusion of defamatory or racist statements, piracy or computer fraud, non-compliance with copyright, or other similar examples of inappropriate behaviour.

1. Violations will be investigated by Promptly's Information Security Management Leader. Employees who report violations or suspected violations will be protected from retaliation.
2. Users authorized by Promptly must comply with local and national laws and regulations that govern the use, exportation and importation of Personally Identifiable Information (PII) and Protected Health Information (PHI).
3. Employees agree to cooperate with federal or state investigations or disciplinary proceedings.

NOTICE: All users are aware and agree that certain actions performed on company assets and networks are monitored and logged strictly for security purposes and only actions that are directly identified as a violation of policy or a direct threat in a form of malicious code or cyber attack attempt are observed. Access to these logs is restricted only to roles in charge of security at Promptly. For more information contact Information Security Management Leader at security@promptlyhealth.com.

4.4 Acceptable and Unacceptable use of Email Services and instant messaging

Acceptable Use:

1. Use of Promptly email addresses in public websites, forums and/or blogs is allowed for business purposes only.
2. Always ensure emails are sent to intended recipients only. Remove unwanted attachments or information from the email trails when forwarding or responding to email messages.
3. Validate the received emails for following before taking any action:
    1. Verify that the received emails are from trustworthy sources; i.e. verify that they are sent from a known email address by checking the source email address.
    2. If an unexpected email is received from a trustworthy address and/or contains any unexpected attachments and/or links, then validate the email by checking verbally with the sender before opening the email or clicking on any attachment or link.
4. Report suspicious or untrustworthy emails to security@promptlyhealth.com by means of forwarding the original email and permanently delete such emails from your inbox.
5. Use only approved instant messaging services for business use.

Unacceptable Use:

1. Open/click the attachment and/or hyperlink in suspicious or untrustworthy emails.
2. Send emails to distribution lists without a business need.
3. Use of public/private email services (like Gmail, Yahoo, Hotmail, etc.) to exchange Business Sensitive Information.
4. The following are some examples of activities that are prohibited and may result in disciplinary action:
    1. Automatic forwarding of Promptly emails to non-business related email addresses.

2. Unauthorized use, or forging, of email header information and email signatures.
3. Originating, forwarding or distributing chain letters, offensive, junk, or unsolicited email.
4. Transmit messages or images that may be construed as harassing, offensive or threatening to others.
5. Usage of profanity, obscenities, or derogatory remarks in any of the email messages discussing business related matters.
6. Sending documents, software, videos and/or audio files that violate copyright laws.
7. Making fraudulent offers of products, items, or services using any Promptly account.

4.5 Acceptable and Unacceptable Use of Internet Services

Acceptable Use:

1. Access to the Internet is neither anonymous or confidential; any action undertaken is identifiable as having originated within Promptly.
2. IT Users may consult websites that are directly connected to and necessary for their activities. However, occasional and reasonable use, for personal reasons, of websites with respect to which the content is not contrary to the law and/or accepted moral standards and does not pose a risk to the image and reputation of the company, will be permitted if it does not hinder the accomplishment of the employees' tasks nor the security of the IT network of Promptly.
3. Connection to the Internet from company provided devices shall be made via Promptly network, equipped with suitable security controls to prevent and/or detect malicious/inappropriate websites and content. Where this is not possible, IT Users shall take reasonable steps to protect themselves as well as Promptly by accessing protected networks.
4. Usage of social media and internet services for private purposes is allowed on company devices only in a way that it does not obstruct regular business duties and is performed with the same security awareness and behaviour as with company internet services. Company social media accounts are managed by dedicated team members and should never be used without proper authorization.
5. Use of Internet services shall be performed prudently and in context of assigned job responsibilities.
6. Use of Internet-based peer-to-peer file sharing services like BitTorrent, uTorrent etc. is prohibited.
7. Use of public storage services like DropBox, BOX for transferring and/or storing Promptly Business Sensitive Information is not permitted. OneDrive should be used in this context. OneDrive should not be used for transferring and/or storing costumer data. IT Users shall only use approved storage mediums for transferring and/or storing Promptly Business Sensitive Information. Users shall seek advice from Information Security Management Leader (by contacting at security@promptlyhealth.com) where there is a legitimate business

need to use such services. Full list of approved software is appended in *Appendix A - List of approved software*.

Unacceptable Use:

1. Disclose Business Sensitive Information on Internet-based or publicly accessible services like newsgroups, social media, blogging sites, forums, etc.
2. Post text or messages on Internet sites that may be construed as harassing, offensive or threatening to others.
3. Bypass Promptly security controls to gain access to websites, which are otherwise blocked.
4. Downloading copyrighted or intellectual property materials, software programs, audio, video, data files, etc. violating any copyright restrictions.
5. Visit Internet sites that contain obscene, hateful or other objectionable materials.
6. Use of security circumvented devices to access corporate WiFi (jailbreak, root, etc.) is strictly prohibited. Use of any smartphones not approved by Information Security Management Leader to access corporate WiFi is strictly prohibited.

Note: Where there is a requirement to disclose Promptly information in public forums or services for business purposes, IT Users shall abide by requirements defined in Section – *Acceptable and Unacceptable Use of Use of Business Sensitive Information* below.

4.6 Acceptable and Unacceptable Use of Business Sensitive Information

Acceptable Use:

1. Classify data whenever it is created, received, or modified into appropriate classification levels in accordance with the *Information classification, Handling and Labelling matrix referenced in POL-14 Data Management document.*
2. Authorization for access to Promptly Business Sensitive Information is subject to approval from the IT User's line management and must be formally renewed in the event of a change of position or a transfer.
3. Promptly's Business Sensitive Information must be stored only in systems that are provided and/or approved by Promptly
4. IT Users shall share Business Sensitive Information with other users based on need-to-know principle and request access revocation when the need is no longer there.
5. **Special care shall be given to transfer of PII data** - No more than 50 records shall be transmitted via collaboration platform messaging system internally to a single recipient; No PII data shall be transmitted via email outside of the Promptly; Transfer of PII data outside of the Promptly shall be done with specific approval and in accordance with the contractual clauses and regulatory requirements meeting specific security technical requirements during the transfer. Contact Information Security Management Leader for support on this matter.
6. Before destroying or retaining company data, users must consult Information Security Management Leader at security@promptlyhealth.com .
7. IT Users shall protect Business Sensitive Information in the form of hard copies against theft and unauthorized access by ensuring the following:
    1. Business Sensitive Information in the form of hardcopies must be adequately protected and placed in locked and secure cabinets, when not in use.

2. Personally attend and collect the printouts immediately from the printers.
3. Never leave copies of printouts containing Business Sensitive Information unattended in meeting rooms, desks, etc.
4. All unwanted paper copies of sensitive information must be disposed off securely using a paper shredder.

Unacceptable Use:

1. Exchanging or storing Business Sensitive Information on third-party systems or locations that are not reviewed and approved by Information Security Management Leader. Full list of approved software is appended in *Appendix A - List of approved software*.
2. Business Sensitive Information is left unattended or available for unauthorized individuals to access, including on desks, printers, copiers, fax machines, and computer monitors
3. Using official business cloud storage and/or other authorized file storage and sharing systems for storing personal files related to photos, music, videos, personal documents, etc.
4. Using business sensitive information for personal purposes and personal gain.
5. Following are some actions that users avoid with regard to Business Sensitive Information:
    1. Record 'confidential' information type on answering machines/voice mail systems or 'out of office' messages.
    2. Disclose Business Sensitive Information without validating the identity of the recipients.
    3. Leave Business Sensitive Information at the workplace unattended.

4.7 Acceptable and Unacceptable Use of User Accounts and Passwords

Acceptable Use:

1. All new accounts must be created as a result from a properly filled Access Request Form in Appendix A of this document, pre-approved by the IT Users supervisor.
2. Necessary precautions shall be taken to protect your user accounts and passwords, provided to access the systems and network from unauthorized access/misuse.
3. All account credentials (Passwords, PINs, etc.) shall be stored in the company approved password management system (Bitwarden)
4. All account credentials that fulfil sharing requirements (test accounts, temporary passwords) shall be shared **only** using the company approved password management system.
5. Use secure passwords to access Promptly IT assets. Promptly follows the updated password guidelines outlined in NIST 800-63B, which can be found in the Access Control policy under Password Policy.
6. IT Users must immediately change their passwords if:
    1. It is the first-time use;
    2. Password has been reset by system administrator;
    3. They know or suspect that their password has been obtained or used by others.
7. Any disclosure or compromise of passwords must be reported to Information Security Management Leader at security@promptlyhealth.com.

Unacceptable Use:

1. Share Promptly provided user account and password with others inside or outside Promptly without prior approval from Information Security Management Leader.
2. Reuse the same password across multiple systems. Use passwords that are used for personal purposes in systems like personal emails, social networks, etc. on Promptly systems.

3. Store their passwords in any computer file, emails, and mobile phones or on paper unless electronically encrypted or physically secured.

4.8 Acceptable and Unacceptable Use of Company Workstations – Desktops and Laptops

Acceptable Use:

1. Use the company's laptops primarily for business purposes.
2. Every company laptop shall have up-to-date antivirus software provided and managed by Promptly and configured according to baseline security requirements defined and maintained by the Information Security Management Leader.
3. Every company laptop's operating system and installed software shall be kept up-to-date and regularly patched.
4. Never leave desktops/laptops unattended for an extended period unless it has been properly safeguarded with controls like screen lock.
5. Only approved software is allowed to be installed on company workstations and from approved sources. Full list of approved software is appended in *Appendix A - List of approved software*.
6. In the event where desktop/laptop equipment are required to be sent to IT workshops for repairing purpose, the IT User of the device shall contact Information Security Management Leader for guidance on securing the data on the device prior to sending.
7. Physically secure your laptops when not in use.
8. Company laptops must always be carried in person and not be checked in as baggage while travelling.

Unacceptable Use:

1. Connect removable storage media, external hard drives or USB devices to company provided desktop and/or laptops.
2. Disabling or tampering with implemented security features such as Corporate Antivirus, Email security, Local firewall, Wireless access points etc.
3. Using Promptly provided computing assets to engage in activities that are in violation of corporate policies and applicable local or internal laws and regulations.
4. Dispose laptop and/or desktop equipment outside of the established process for equipment disposal. Users can contact Information Security Management Leader at <email> for the required guidance.
5. Connect laptops to untrusted networks, like free and public Wi-Fi Hotspots without the use of company provided VPN. Home WiFi networks are considered safe if protected with a strong passphrase and at least WPA2 security protocol. It is highly recommended that VPN be used in all cases except when connected directly to the corporate WIFI network in the office.
6. Downloading and/or installing unapproved software applications onto Promptly workstations is prohibited. If you require a software or a tool that is not listed in the Approved Software List appended in Appendix B, please contact Information Security Management Leader at security@promtlyhealth.com for requested software evaluation.

4.9 Acceptable and Unacceptable Use of Teleworking

Teleworking means that information and communication equipment is used to enable employees to perform their work outside the Promptly. Teleworking does not include the use of mobile phones outside the Promptly's premises.
Teleworking must be authorized by an employee Manager with written or verbal approval.

Acceptable Use:

1. Use only approved devices for work (company laptop, approved personal device for work.
2. Connect to the home WiFi network or a private mobile hotspot protected with a secure password (see **Acceptable and Unacceptable Use of User Accounts and Passwords**)
3. Lock device when not in use.
4. Use device in a separate room with appropriate space to do your work and have remote video calls.

Unacceptable Use:

1. Share company device (and/or approved personal devices for work) with members of the household/visitors.
2. Leave device unattended in public spaces (coffee shops, airports, etc.).
3. Use unsecure/open and public internet access points.

4.10 Acceptable and Unacceptable Use of Personal Devices (Bring Your Own Device)

Acceptable Use:

1. Register your BYOD device for approval with Information Security Management Leader by providing device information and intended business use;
2. **Right to audit: By accepting this BYOD policy you accept that Information Security Management Leader can audit your device for compliance requirements enlisted in this section at any point during your engagement at Promptly for security purposes. You agree to comply with providing Information Security Management Leader any required system/application logs from your device in case of a security incident and need for investigation.**
3. Connect to corporate applications using Promptly approved technologies only, such as VPN and with an approved BYOD device;
4. Store all Promptly Business Sensitive Information on Promptly provided cloud storage platform;
5. Protection of IT User’s personal devices will not be Promptly’s responsibility. However, Promptly requires that all personal devices (Laptops, Tablets, Smartphones) that are used to connect to corporate applications have the following security mechanisms enabled:
    1. Latest operating system, software and security patches with automatic updates turned on;
    2. Up to date anti-virus software;
    3. Specific Promptly provided anti-virus software installation is mandatory on an approved BYOD device in case of IT user regular access to **PHI** data as part of their role at Promptly
    4. Lockscreen access control using a password, PIN or biometric as applicable;
    5. Remote locate and wipe capability implemented/turned on;
    6. Auto-lock device option set to no more than 15 minutes of inactivity;

7. Auto-lock device option after 5 failed attempts.
8. Lockout duration should not be below 15 minutes.
9. Personal firewall (Laptops only);
10. Local storage encryption turned on;

For guidance and support in implementing these controls contact Information Security Management Leader at security@promptlyhealth.com .

Unacceptable Use:

1. Access corporate applications with a non-approved BYOD device;
2. Store Promptly Business Sensitive Information on personal devices local storage;

4.11 Acceptable and Unacceptable Use of Company office space and facilities

1. Use of company office space for business and company event purposes only.
2. Maintaining clean desk and screen policy at your working space, avoiding leaving any business sensitive data on papers at the desk or visible at the screen when leaving the desk area. This includes avoiding leaving printouts with business sensitive data in printers or around common office space unattended.
3. Maintaining a “leave it as you’ve found it” approach to meeting rooms, making sure there are no documents left in the meeting room or data written on the whiteboard when you leave the room.
4. All visitors to the Promptly office shall be properly recorded in the visitors log available in *Appendix C - Visitors Log.*
5. There shall be a person at Promptly responsible for each Visitor during their visit keeping them company and/or doing business with them, escorting them to appropriate meeting rooms until the end of their visit.

Unacceptable Use:

1. Using office space for personal storage or personal events without explicit approval from the management.
2. Providing access to office space to unauthorized personnel (not official visitors) either by sharing your access card or keeping the door open for people you do not know or know that they do not work at Promptly.

For detailed information regarding office etiquette and life at Promptly please refer to Code of Conduct document.

4.12 Exceptions

Any exceptions to this standard will require written authorization by email from Information Security Management Leader. Exceptions granted will be issued a policy waiver for a defined period of time. Requests for exceptions to this policy should be addressed to Information Security Management Leader at security@promtplyhealth.com.

4.13 Governance and Enforcement

Non-conformance to this standard could result in disciplinary action including, but not limited to, informal or formal warnings, up to termination of contract.

Appendix A - List of Approved Software

List of approved software is a maintained by System Owners and can be accessed here:
https://www.notion.so/Authorized-Software-Policy-c74ec0da7723495386f64dec2f20b7c8

Appendix B - Information Security Incident Report Form

For submitting an incident report please use the form below.
Direct link:
https://proefgroup.sharepoint.com/:w:/r/sites/promptlyhealth/_layouts/15/Doc.aspx?sourcedoc=%7BFA4A612A-249E-4864-A7EF-4B46189B0D6B%7D&file=Information%20Security%20Incident%20form.docx&action=default&mobileredirect=true

Alternatively, you can contact Information Security Management Leader directly via email at security@promptlyhealth.com. If the security incident permits you from accessing your email you can use your private email or reach Information Security Management Leader on Slack or at phone +351 916303502.

Appendix C - Visitors Log

Please record every visitor in the Visitors log.
Direct Link to database:
https://proefgroup.sharepoint.com/:x:/r/sites/promptlyhealth/_layouts/15/Doc.aspx?sourcedoc=%7B24983D4E-6D61-4457-8285-FB096A182E49%7D&file=Visitors%20log.xlsx&action=default&mobileredirect=true

Appendix D - Requirements implementation Procedure for Unmanaged company devices and BYODs

For correct implementation of Promptly BYOD requirements stated in section 4.10 Acceptable and Unacceptable Use of Personal Devices (Bring Your Own Device) in this document seek assistance from IT personnel by contacting them at security@promptlyhealth.com .