

Title: Acceptable Use
 Approved by: System Director, Cybersecurity Risk and Assurance
 Approval Date: 12/7/2023
 Next Review Date: 12/7/2024
 Effective Date: 12/7/2023
 Standard Number: HR-ST-2.0.05-R4.0
 Supersedes: None
 Originating Department: Information Security
 Contributing Departments: I&T
 Manual: Information Security Manual
 Section: 2.0 Human Resources Workforce Member Security
 Revision: 4.0

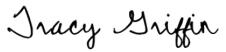
DocuSigned by:

 391A327B3618463...
 12/7/2023

Table of Contents

I. Scope 2

II. Intended Audience 2

III. Purpose 2

IV. Standard 2

V. Standard Details 2

 A. General Requirements 2

 B. Confidential Information 4

 C. User ID and Passwords 4

 D. Communications-Email, Voicemail, Instant Messaging, Texting, and Faxing 5

 E. Computers - Workstations, PCs, Laptops 7

 F. Software 8

 G. Protecting Electronic Devices 9

 H. Internet Usage 10

 I. Social Media 11

 J. Mobile Devices 12

 K. Unacceptable Use 12

VI. Authority/Enforcement 14

VII. Exceptions 14

VIII. Definitions 14

IX. Attachments 14

X. Related Policies, Standards & References 14

XI. Version Control 15

 Appendix A 16

I. Scope

This Bon Secours Mercy Health's (BSMH) Information & Technology (I&T) standard applies to all workforce members and governs all data and systems (whether owned by or operated for BSMH business through contractual arrangements).

II. Intended Audience

This standard, in conjunction with the supporting policies, standards, and procedures is primarily intended for use by:

- Workforce members, including all employees, medical staff, volunteers, trainees, students, agents, contractors, and individuals who have access to BSMH systems per an agreement, and other persons whose conduct, in the performance of work for BSMH, is under the direct management of BSMH, whether or not they are paid by BSMH. All Workforce members are expected to comply with the controls outlined by the Information Security Program's Policies, Standards, Procedures, and Guidelines. Workforce member compliance most often will be enforced through system architecture and technical controls. In situations where system architecture and technical controls cannot enforce compliance, workforce members will be informed using administrative controls, such as through annual training and awareness initiatives.

III. Purpose

The purpose of this standard is to supply clear and concise rules for the acceptable use of BSMH technology assets by all workforce members. BSMH Information & Technology (I&T) implements security measures and these acceptable use requirements to secure and protect BSMH systems.

IV. Standard

BSMH's technology assets (data, information systems, and network connected technology not traditionally considered as information technology such as networked medical technology, and facilities management systems) must be protected and secured by all BSMH workforce members. Inappropriate use of technology assets exposes BSMH to risks including virus attacks, compromise of network systems and services, and legal issues. These acceptable use requirements must be followed and adhered to in order to secure and protect BSMH assets and systems.

V. Standard Details

A. General Requirements

1. All BSMH employees must complete an annual mandatory security awareness training on the acceptable use of BSMH technology assets. Acknowledgement and agreement to adhere to the requirements in this standard is needed during the training by completing the Privacy/Security Attestation agreement.

2. All information created on BSMH's technology assets remains the property of BSMH.
3. All BSMH resources (e.g., computers, copiers/scanners, fax machines, tablets, mobile devices, pagers) must be used for business purposes only, except for limited personal use, provided such personal use does not interfere with work assignments and/or create network performance issues.
4. All workforce members have an ethical and legal duty to maintain and preserve BSMH confidential information (as defined below in Section B) regardless of form (verbal, written or electronic) both during and after their association with BSMH. Confidential information, such as but not limited to, Protected Health Information (PHI), Payment Card Industry Information (PCI), and Personally Identifiable Information (PII), must not be accessed or disclosed to unauthorized individuals or parties inside or outside of BSMH.
5. Every workforce member is responsible for the use of their BSMH account and equipment (PC, laptop, desktop, cell phone, etc.) and will be held responsible for any violations that are traced to their account or equipment.
6. Willful destruction of information, unauthorized access, modification to or disclosure of confidential information (as defined below in Section B), or violations of any of the terms listed in this standard may result in access privileges being revoked and further disciplinary action up to and including the potential for suspension or termination from BSMH (see BSMH-HR-CUL_014 Corrective Action Policy, and Sanctions Policy).
7. A workforce member that uses BSMH's systems may become personally subject to civil and criminal legal action and financial penalties resulting from privacy, security, and confidentiality breaches that they have committed.
8. BSMH I&T may monitor equipment, systems, email, text, instant messaging, Internet usage and network traffic at any time and without your consent or knowledge.
9. BSMH reserves the right to audit networks and systems on a periodic basis to ensure compliance with BSMH policies and standards.
10. Any lost or stolen information, electronic resource, or device must be reported immediately to the BSMH Service Desk (833-691-4357 or 833-MY1 HELP) so that the organization can initiate proper corrective action.
11. BSMH management shall approve the use of information assets and take action when unauthorized activity occurs.
12. If a BSMH workforce member has any complaints or concerns about compliance with the BSMH's security policies, standards, or procedures, the workforce member should contact the BSMH Ethics Help line (<http://www.bsmhethicsshelpline.org/>).

B. Confidential Information

1. Workforce members must take all necessary steps to prevent unauthorized access to information that could be classified as confidential (i.e., corporate strategies, trade secrets, customer lists, Protected Health Information (PHI), Payment Card Industry Information (PCI), and Personally Identifiable Information (PII)).
2. Workforce members will not access or use confidential information beyond what is provided or what is required to perform their job duties.
3. Workforce members must properly handle, store, and dispose of confidential information according to CS-ST-9.0.07 Media Handling Standard.
 - a. Confidential information (PHI, PII, PCI, etc.) in paper form must always be shredded prior to disposal or placed in a secure disposal receptacle.
 - b. Credit card information must never be stored either electronically or in paper form. Credit card information must never be included in email, FAX, text, or Instant Messaging (IM) as these technologies are not secure.
4. Covered or critical information must be protected when using internal or external (e.g., USPS) mail services.

C. User ID and Passwords

1. Access to systems is only granted when one has a legitimate business reason and must be necessary for the workforce member to conduct their job functions.
2. A workforce member's assigned ID is equal to a written signature and the assigned workforce member is responsible for all access and work completed under the authority of that ID.
3. Workforce members are responsible for keeping their passwords secure. Do not show or share passwords or logon accounts with any other person, including family members, or technology support staff.
4. Do not write, email, or store passwords in easily accessible locations. Storing passwords in a secure password vault is acceptable if the password vault is encrypted.
5. If an assigned user ID or password has been compromised, stolen, or used inappropriately, then immediately call the BSMH I&T Service Desk (833-691-4357 or 833-MY1-HELP) and change your password.
6. BSMH workforce members are prohibited from circumventing user authentication or security mechanisms of any host, network, or account.
7. BSMH workforce members must not use the "Save Password" option available on software applications and internet web browsers.

8. BSMH workforce members are responsible for constructing and using strong passwords (see the Authorized Access to Technology Assets Standard for more details). A strong password must meet the following guidelines:
 - a. It is at least 12 characters in length
 - b. It uses at least 3 of the 4 classes of characters:
 - i. Lowercase letters
 - ii. Uppercase letters
 - iii. Numerical digits
 - iv. Special characters (e.g. !, \$, %, &)
 - c. A password must not be:
 - i. A word in any language, slang, dialect, jargon, etc.
 - ii. Based on personal information (e.g., name of family member, pet, birthday, address, Social Security Numbers, etc.)
 - iii. Any common variation of a word found in a dictionary (e.g., P@ssw0rd for Password)
 - iv. Sequential numbers or letters. For example, do not use 1234, jklm, 6789, etc.
 - d. Consider using a passphrase as your password. (e.g., based on a song, movie, or any phrase).
 - i. To create a passphrase; use letters, numbers, and symbols to represent a phrase only you know. (Example: a phrase such as “This May Be One Way to Remember”, the passphrase might be TmB1w2R or Tmb1W>r-).
 9. BSMH workforce members must change any password assigned to them at first use.
 10. Usernames and Passwords used to gain access to BSMH network, or technology assets must not be used to access non-BSMH systems, services, or websites.
- D. Communications-Email, Voicemail, Instant Messaging, Texting, and Faxing
1. BSMH communication technologies such as email, voicemail, instant messaging, texting, and faxing should be used for business purposes only (except for the limited personal use allowed under internal policy). Workforce members are expected to use BSMH resources in an efficient, effective, ethical, and lawful manner. Approvals

must be obtained prior to using external public services including instant messaging or file sharing (e.g., AOL instant messenger, Yahoo instant messenger, DropBox, Box, Google Drive, etc.).

2. Sending any confidential information (i.e., PHI, PCI, PII, etc.) through email is strongly discouraged. If your job requires you to send any privileged, confidential, or sensitive information to outside parties via email, or fax, you must:
 - a. Ensure that any confidential information in electronic form is encrypted when sent outside the organization. If you have an approved business purpose to send PHI outside the organization through email, you must include the word “Secure” or “SafeMail” in the subject line to encrypt the data.
 - b. BSMH workforce members should not send PII/PHI over facsimile (FAX) unless it cannot be sent over other, more secure channels (e.g., delivery by hand, secure email). When faxing confidential data, ensure that the correct phone number and contact information is being used.
3. All email messages are the property of BSMH, and as such, are not private communications. Email communications may be monitored for training, maintenance, or investigative purposes. Deleting messages or email will not remove them from the database nor protect them from auditing.
4. Never open attachments or follow links provided in email messages from senders you do not recognize. Use extreme caution when opening attachments or following links that originate from outside BSMH, even from senders you know. Links and attachments can be used to perform various malicious functions on workstations (e.g., install viruses, key loggers, remote access software, etc.).
5. Should you receive a suspicious email, report the phishing email immediately, see Appendix A for instructions. If you accidentally clicked on a link that you suspect as being malicious or provided your BSMH login credentials to an unknown source, immediately contact the Bon Secours Mercy Health Service Desk at 1-833-691-4357.
6. Unauthorized use or forging of email header information is prohibited.
7. Sending of “chain letters” or conducting any type of solicitation, unless permitted by law and or BSMH Human Resources policy for any organization not affiliated with BSMH, is prohibited.
8. Voicemail boxes must be protected by a PIN which must never be the same as the last four digits of the telephone number of the voicemail box.
9. Only BSMH approved, encrypted, and authorized messaging applications (e.g., PerfectServe) may be used for texting confidential information. The communicating of patient information via text message or IM is prohibited.

10. Accessing personal email accounts (e.g., Gmail, Yahoo mail, etc.) from a BSMH resource is prohibited and is blocked to protect BSMH assets. Never use a BSMH computer to access personal email accounts (e.g., Yahoo mail, Google Mail, Hotmail, etc.). Personal email account security is not as strong as the level of security from Bon Secours Mercy Health managed security.
11. Using personal email accounts for BSMH business related communications is prohibited.
12. Configuring a BSMH email account to forward messages to an email account outside of the BSMH email system (e.g., Gmail, yahoo mail) is prohibited.
13. Use of Distribution Lists and Global Address Book
 - a. Internal distribution lists (example: Shared Services) must be kept confidential and used for internal purposes only.
 - b. The owner of a distribution list (whether team or individual) is responsible for maintaining appropriate use and removing addresses that are no longer needed.
 - c. Guidelines for sending e-mail to distribution lists:
 - i. Use of distribution lists to send e-mail to a large group should only be used when the message is relevant to all members of the distribution list, and directly relates to carrying out BSMH business.
 - ii. Avoid requesting read receipts when sending mass e-mails.
 - iii. Any file attachments must be related to the message content.
 - iv. The use of “reply to all” should be used sparingly and only if justified by the content of the message.
 - v. 'Recall Message' may be used if information was sent in error to a small list. For large lists, send a short follow-up message to correct the error or contact the messaging team.
 - vi. Emails should take care to not resemble unsolicited or spam e-mails (e.g., poor grammar, misspellings, overly generic).
 - vii. E-mails should be edited carefully for content before being sent for posting. Repeat emails and corrections will be sent on a limited basis.
 - d. Out of office reminders are not to be set to send to recipients external to BSMH.

E. Computers - Workstations, PCs, Laptops

1. All BSMH workstations, PCs, and laptops are securely set up with password protected screensavers, configured by I&T, which are activated after a specified time limit (e.g., 15 minutes).
2. When leaving your workstation, a workforce member must always lock their computer (Windows Key + “L”, or Ctrl-Alt-Del and “Lock”), even if it is just for getting up to retrieve something at the printer or attending to a patient, even in an emergency.
3. Because information contained on computers is especially vulnerable, special care must be exercised as follows:
 - a. Do not keep data and files anywhere on your computer’s local hard drive (i.e., the local computer’s “Desktop” or C drive). Data and files are to be stored on your personal network drive for backup and protection.
 - b. Be mindful of your surroundings. Shield login screens and other sensitive information from prying eyes. Use a shield/privacy screen in open areas where the public has access and could see confidential data.
4. To protect the integrity of BSMH’s information resources, BSMH computer system configurations must only be changed by authorized BSMH I&T personnel.
5. Workforce members are strongly encouraged to use BSMH issued computer resources (laptops or desktops) to access the BSMH network. Workstations not issued by BSMH must meet BSMH security and technology standards and be approved for use by the I&T department prior to accessing the BSMH network. Required security configurations include, but are not limited to, the following:
 - a. Full disk encryption.
 - b. A host firewall configured to block all but approved inbound connections.
 - c. An approved anti-virus solution, configured to automatically update as new anti-virus signatures become available.
 - d. An approved operating system version, configured to automatically install the latest operating system updates and security patches via the native operating system update service.
6. If a computer has been lost, stolen or used inappropriately, notify the BSMH service desk (833-691-4357 or 833-MY1-HELP) immediately.

F. Software

1. All software installed on a BSMH computer must be licensed and registered to BSMH.

2. Installation or modification to BSMH software or operating system configurations is prohibited. New installations or upgrades on BSMH resources will only be performed by authorized BSMH personnel.
3. All workforce members must honor copyrights and software licenses and follow all federal and state laws.
4. Workforce members must not use personally owned software on BSMH's information resources. This includes purchased and licensed applications, shareware, freeware, and other personally owned software.

G. Protecting Electronic Devices

1. All PCs (Desktops, Laptops) portable computing devices, and mobile devices accessing the BSMH network, systems, or data must be password protected, unless specifically authorized by BSMH I&T.
2. BSMH issued laptops, mobile devices and removable media must be equipped with encryption or other security measures to protect the data contained within such devices.
3. Workforce members are forbidden from changing settings of, disabling, or bypassing virus detection software.
4. Unattended laptops and mobile devices must be secured to decrease the likelihood of loss or theft. Examples of securing a laptop or mobile device include:
 - a. Locking the device(s) in an office, desk drawer, or filing cabinet. If computers are equipped with a locking port, they may be attached to a desk or cabinet using a cable lock system intended for such use.
 - b. When traveling, workforce members must not leave devices unattended. When this is unavoidable, the device should be secured to the best of their ability. This may include securing the device in a room safe, locking the device in an automobile trunk, or securing the device to the interior of an automobile using the provided cable lock system (leaving a device in an automobile is not optimal and should only be done for the minimum time necessary).
 - c. At no time should a device be placed in checked baggage.
 - d. Please refer to AC-ST-1.0.07 Mobile Computing and Teleworking Standard for workforce member responsibilities.
5. When transporting a BSMH laptop outside of a BSMH facility, it must be turned off so that the full disk encryption is at its strongest state. A device that is merely in hibernate or sleep mode is not considered to be fully protected.


6. When using a personal computer to access BSMH networks or systems, it is the responsibility of the workforce member to ensure that the computer meets BSMH corporate computer security standards. This includes keeping the system and all associated software up to date on versions and patches, implementing software firewalls, and installing, running, and keeping up to date a commercial anti-virus software solution.
7. Never save BSMH data on a personal device.
8. The BSMH corporate standard, supported anti-virus software must be installed on all BSMH systems.
9. All BSMH workforce members must follow the recommended processes to prevent virus problems:
 - a. If you are using a portable device, such as a USB device, anti-virus software will scan the files for viruses when you open them. Do not interrupt the scanning.
 - b. Never share CDs, DVDs, USBs, or other disks unless there is a critical business requirement to do so.
 - c. Never download files from unknown or suspicious source on the Internet.
10. For international travel, workforce members must not assume use of BSMH managed devices and must not assume access to BSMH resources.
 - a. BSMH prohibits associates from working outside of the U.S. due to unintended legal, payroll and tax implications. Additionally, the security of our ministry's network and data are at risk when the BSMH network is accessed outside of the U.S.

Please see the following HR documents for details:

- BSMH-HR-STRP_002 Remote Work Policy
- Workplace Routines Frequently Asked Questions
- Remote & Hybrid Associates: Tax Information Frequently Asked Questions (FAQ)

H. Internet Usage

1. BSMH workforce members are expected to use the Internet responsibly and productively. Internet access should be limited to business related activities only. The use of the BSMH network and the Internet is a privilege, not a right, and inappropriate use will result in cancellation of these privileges.

2. All Internet data that is composed, transmitted, and/or received by BSMH's technology assets are considered to be the property of BSMH, and as such, is subject to disclosure for legal reasons.
 3. Avoid using public Wi-Fi locations when possible as your system and data could be hacked. When using a public Wi-Fi hotspot is unavoidable, always enable and use your VPN for all connectivity, whether or not it is BSMH related.
 4. Do not download non-business files.
 5. Use caution when following links on the Internet. Always know where the link goes before following. Links can be verified by hovering your mouse cursor over the link to reveal its true destination. If the web address is different from what is displayed in the text of the link, do not click on the link.
 6. Never use your BSMH ID or password to sign on to any personal Internet websites, including social media. Use a different password for each of your website logins. If a hacker gets your password, they will try to access other sites using it.
 7. While the "Remember Passwords" feature on your browser is convenient, do not use it. If your computer is stolen, the damage could be increased if your passwords are extracted and misused.
 8. Never share personal information online. It could easily be used to hijack your BSMH account, apply for a credit card in your name, or access your bank account.
 9. Look for HTTPS with the padlock ( <https://>) in the web address, indicating a secure website, before you enter any sensitive or personal information onto that website.
 10. BSMH reserves the right to monitor Internet traffic and data that is composed, sent, or received at any time without your consent or knowledge.
- I. Social Media using a Business Account
1. Social media usage and blogging is subject to the terms and restrictions in BSMH-HR-CUL_008 Social Media Policy.
 2. Postings to newsgroups using a BSMH email address is prohibited unless it is business related and you have permission. Posting non-business-related messages to large numbers of newsgroups (newsgroup spam) while using a BSMH email address is prohibited.
 3. Do not post to social media in patient areas or hospital kiosks.
 4. Workforce members may not create social media pages on behalf of BSMH without permission.

5. BSMH reserves the right to monitor, prohibit, restrict, block, suspend, terminate, or discontinue your access to any work-related social media site at any time without notice for any reason at its sole discretion.

J. Mobile Devices

1. Except in limited circumstances, BSMH does not issue mobile devices to workforce members, but follows a Bring Your Own Device (BYOD) program, permitting the use of Personal Mobile Devices for the limited access of BSMH data.
 - a. Workforce members who use personal mobile devices to access BSMH data must adhere to the BSMH-HR-STRP_001 Personal Mobile Device Use Policy.
 - b. Workforce members must agree to have installed on their mobile device the BSMH standard Mobile Device Management (MDM) software suite.
 - c. Workforce members are required to configure their mobile device with a 6-character access PIN to prevent unauthorized access.
 - d. Workforce members must agree to allow the mobile device to be configured for auto-wipe after 10 invalid logon attempts.
 - e. Workforce members must ensure that their mobile device is running a current version of operating system.
 - f. Workforce members must agree to surrender their mobile device to BSMH at the request of I&T Security, Legal Department, Human Resources, or other management personnel for the purpose of analysis or data collection. Failure to follow such a request may result in corrective action up to and including termination.
 - g. Workforce Members using Personal Mobile Devices for approved access to BSMH applications (i.e., Haiku/Canto for Epic, Workday, encrypted text messaging) and who have installed approved apps for this access will receive support from the various application teams via a Compass ticket for issues that arise in the use of those apps. Support for any other installed application or operating system other than those necessary for the approved access of BSMH data are the sole responsibility of the device owner and cannot be provided by BSMH I&T.

K. Unacceptable Use

1. The following activities are considered unacceptable and prohibited, with no exceptions except as permitted by law, and may lead to disciplinary action up to and including termination of employment. In cases of fraud, misuse, or breach of privacy laws, legal action may be taken.

- a. Engaging in activity that is illegal under any local, state, federal, or international law.
- b. Using BSMH devices or BSMH accounts to perpetrate any form of fraud, and/or software, film, or music piracy.
- c. Using BSMH devices for political lobbying.
- d. Supplying information about, or lists of, BSMH workforce members to parties outside of BSMH.
- e. Sharing or supplying access to your BSMH account or encouraging another workforce member to share or supply their account.
- f. Compiling subsets of BSMH data for personal use, whether in written or electronic form.
- g. Using BSMH resources for non-work-related purposes or performing acts that waste BSMH's systems resources or monopolize resources (e.g., playing games, engaging in online chat groups, uploading or downloading large files, or accessing streaming audio and/or video files (e.g., March Madness streaming)).
- h. Downloading, installing, viewing, storing, transferring, posting, or sending obscene, profane, libelous, pornographic, abusive, slanderous, defamatory, harassing, vulgar, hateful, discriminatory, threatening, illegal, inappropriate, and/or offensive materials or messages. If a workforce member has knowledge of the transmission of inappropriate materials or messages, the workforce member is obligated to report it immediately to BSMH Corporate Responsibility via the BSMH Ethics Hotline.
- i. Creating or distributing offensive comments or jokes that include but are not limited to race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practices, political beliefs, or national origin.
- j. Using a BSMH device to actively engage in acquiring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- k. Vandalism, including but not limited to intentionally uploading or creating computer viruses, or introduction of malicious programs (i.e., viruses, Trojan horse programs, worms, email bombs) into BSMH's network or technology assets.
- l. Utilizing security or hacking software, tools, or techniques on the BSMH network to capture or modify information without proper authorization (e.g., packet capture, port scanning, ping floods, packet spoofing, denial of service, forged routing information for malicious purposes).

- m. Unauthorized copying of copyrighted material, sharing trade secrets, patents, or other intellectual property owned by BSMH.
- n. Tampering with or unauthorized destruction of information.
- o. “Hacking” or gaining unauthorized access to other computers or computer systems or trying to gain such unauthorized access.

VI. Authority/Enforcement

The BSMH Chief Information Officer (CIO) shall have authority to interpret and apply this standard. This Standard may be changed or amended at any time, if it has been through a formal review and approval process. The Chief Information Security Officer (CISO) shall provide notice of any such modifications or amendments and will post the current version on the internal BSMH network where all employees may access it.

Non-compliance with this procedure by BSMH I&T employees and systems users without proper approval (see next section) is a serious matter. Depending on severity of violations and applicable legal statutes, consequences could result in removal of access rights and special system privileges, removal of system access, or, for BSMH I&T employees, disciplinary action to include potential termination of employment. In cases of fraud, misuse, or breach of privacy laws, legal action may be taken.

VII. Exceptions

Any deviation or exception from this policy may be appropriate in non-standard circumstances and should be justified in written form and must be approved by the CIO & CISO (or designee).

VIII. Definitions

Underlined words identify terms that are defined in MP-ST-0.0.01 Information Security Governance Manual Attachment 1.

IX. Attachments

Appendix A - Reporting a Cybersecurity Phishing email in Microsoft Office 365

X. Related Policies, Standards & References

- AC-PO-1.0 Access Control Policy
- AC-ST-1.0.02 Authorized Access to Technology Assets Standard
- AC-ST-1.0.07-R1.0 Mobile Computing and Teleworking Standard
- CS-ST-9.0.07 Media Handling Standard
- BSMH-HR-STRP_001 Personal Mobile Device Use Policy (Human Resources Knowledge document)

- BSMH-HR-STRP_002 Remote Work Policy (Human Resources Knowledge document)
- BSMH Work Routines_Associate_FAQ (Human Resources Knowledge document)
- BSMH-HR-CUL_008 BSMH Social Media Policy (Human Resources Knowledge document)
- BSMH-HR-CUL_014 Corrective Action Policy (Human Resources Knowledge document)
- Sanctions Policy (BSMH System-wide Policies - HIPAA Policies Folder)
- HITRUST CSF v11.1

XI. Version Control

Version	Date	Description	Prepared By
1.0	8/3/2020	Standard created and approved	Bob Rogers, Lou Ann Gerard, Tom Kulas, Heather Rinsky, Kara Mueller
2.0	11/15/2021	Annual review, updated verbiage. Added updates C-8-a, C-8-c-ii, C-8-c-iv, C-9-d-(all), D-2-a. Added D-13 Distribution List and Global Address Book. IX added Authorized Access to Information Systems, Corrective Action Policy, Sanctions Policy. Added Appendix A.	Lara Hayes, Desiree Chumbler, Kara Mueller, Lou Ann Gerard, Mike Gomez, Tracy Griffin
3.0	9/14/2022	Annual review. Updated References. Updated Table of Contents. Added updates C-10, G-4-d, G-9. Updated wording for consistency across documentation.	Lara Hayes, Kara Mueller
3.1	9/22/2023	Annual Review. Systemwide template updates. Outline format updates. Added Intended Audience section. Added G-9-a&b.	Lara Hayes, Kara Mueller, Tracy Griffin
4.0	12/6/2023	Updated References. Updated Section I Social Media using a Business Account. Added G-7. Updated, A-4 & 6, B-3, G-10, K-1.	Lara Hayes, Tracy Griffin, Todd Sarver

Appendix A

KB0021316 - Report Phishing (Suspicious) Microsoft Outlook 365 Email to CybersecurityIntroduction

Bon Secours Mercy Health is committed to making information technology resources more easily accessible for our workforce members. This extends to providing a mechanism to report suspicious phishing emails.

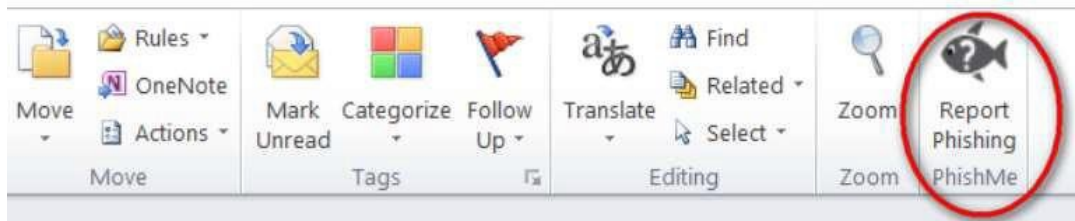
To ensure suspicious emails are being reported, BSMH has implemented a feature in your Microsoft Office 365 email account that will support a one-click reporting option. Once you have reported the email, BSMH Cybersecurity will immediately be notified and initiate an investigation.

NOTE: This feature will also work with the mobile Outlook app.

Instructions

If you receive a suspicious email, perform the steps below to report this to the Cybersecurity team.

From the Microsoft Outlook 365 task bar, click **Report Phishing** as shown in the following illustration.



Complete the fields and submit the request.

E-Mails that **should be reported** with the Report Phishing button:

- External e-mails pretending to be from a BSMH entity
- E-mails asking for sensitive information from unknown or unconfirmed senders
- E-mails with suspicious attachments or links

E-mails that **should not be reported** with the Report Phishing button:

- Marketing e-mails (use the unsubscribe instead)
- Legitimate BSMH communications

This policy/procedure/guideline does not establish a standard of clinical care or practice or standard of non-clinical practice to be followed in every case. The policy/procedure/guideline should guide actions with the understanding that departures may be required at times.

Sites revised 07/08/2022 - Bon Secours Mercy Health adopts the above policy, procedure, policy & procedure, guideline, manual / reference guide / instructions, or principle / standard / guidance document for all Bon Secours Mercy Health entities including, but not limited to, facilities doing business as Mercy Health – St. Vincent Medical Center, Mercy Health – St. Charles Hospital, Mercy Health – St. Anne Hospital, Mercy Health – Tiffin Hospital, Mercy Health – Willard Hospital, Mercy Health – Defiance Hospital, Mercy Health Allen Hospital LLC, Mercy Health - Lorain Hospital, Mercy Health St. Elizabeth Youngstown Hospital, Mercy Health St. Joseph Warren Hospital, Mercy Health - St. Elizabeth Boardman Hospital, Mercy Health - St. Rita's Medical Center, Mercy Health – Springfield Regional Medical Center, Mercy Health - Urbana Hospital, Mercy Health - Anderson Hospital, Mercy Health - Clermont Hospital, Mercy Health – Fairfield Hospital, Mercy Health - West Hospital, The Jewish Hospital – Mercy Health, Mercy Health - Lourdes Hospital LLC, Mercy Health – Marcum and Wallace Hospital, Chesapeake Hospital Corporation DBA Rappahannock General, Maryview Hospital, Bon Secours Richmond Community, Bon Secours Memorial Regional Medical Center, Bon Secours – St. Mary's Hospital, Bon Secours St. Francis Health System, Bon Secours St. Francis Medical Center, Bon Secours Mary Immaculate Hospital, Bon Secours - Southside Medical Center, Bon Secours Mercy Health Franklin, LLC, and Southern Virginia Medical Center