PREMERA	Corporate Cybersecurity Policy

Title	**Email and Other Electronic Communications**
Document ID	**CP.IT.CS.104.v4**
Previous Document ID	CP.IT.SS.007
Current Effective Date	1/18/2024
Original Effective Date	7/5/2001
Replaces	Former name: eMail Use and Management policy
Cross Reference (Related Documents)	Code of Conduct; Computer, Network and Telephone Usage policy (CP.IT.CS.115); Confidentiality of Protected Personal Information policy (CP.CS.PR.5); Cryptography policy (CP.IT.CS.118); Records Management policy (CP.HI.DG.1); Email Security standard (ST.IT.CS.105); Secure Transfer – Fax policy (DP.IT.CS.143); departmental Confidentiality of Protected Personal Information Procedures

Purpose	To specify requirements for the use of email, instant messaging, and other electronic communication mechanisms, in order to: • Ensure that Premera Communication Networks are used responsibly, • Minimize potential liability related to use and retention of email and other electronic communications, and • Protect Premera's computing systems and our members' personal information.
Scope	Applies to PREMERA and its subsidiaries and affiliates ("Premera" or the "Company"), and to all Users who have been granted access to Company email or other text-based or multimedia electronic communication services provided by the Company. This policy does not apply to telephone services, which are covered in the Computer, Network and Telephone Usage policy.
Definitions	**Internet Mail:** A non-Company personal email account, such as a Gmail account, that is accessed via an Internet browser. **Phishing:** A cyberattack method, often carried out by email, instant messages, SMS text messages, or phone calls, in which an attacker uses a legitimate-seeming message to try to trick the recipient into clicking a malicious link or attachment, and/or revealing login credentials or other confidential information. **Premera Communication Network:** Data transmission services that are maintained by the Company to allow communication among the Company's workstations, servers, business partners, and the Internet. **Proprietary Data:** A classification of information that is highly sensitive related to how the Company conducts its business and is seen as an advantage over competition in the market. The inappropriate release of this information may potentially cause severe harm to organizational operations, organizational assets, or individuals.

	Protected Data: A classification of information that is highly sensitive and has been designated by the Company as Protected Personal Information (PPI). The Company is required by law to safeguard this data. The inappropriate release of this information could cause severe harm to individuals and the organization. **Spam:** Unsolicited or undesired bulk electronic messages. **User:** An individual who is granted access to the Company's non-public technology resources, excluding web portals provided for external use.
Policy	**<u>Authorized Use of Company Electronic Communications Services</u>** [005] The Company provides email and other electronic communication services primarily for business purposes. [010] Users may occasionally use these services for personal correspondence, as long as they comply with the Personal Use provisions of the Computer, Network, and Telephone Usage policy. [015] Users are responsible for completing security awareness training, including reviewing this policy. [015.a] The training educates Users about limits on their use of Premera's information and Premera assets associated with information-processing facilities. [020] Users are also responsible for using electronic communications ethically and lawfully. [020.a] Communications must be truthful and accurate. [020.b] Non-business communications that can be traced back to Premera (for example, emails sent from a Company email address) must not appear to make pronouncements or express opinions on behalf of the Company. **<u>Unauthorized Use of Company Electronic Communication Services</u>** **Prohibited Activity** [025] Do not do any of the following: a. Send Spam b. Knowingly spread viruses c. Engage in Phishing (except for Phishing tests performed by or for the Cybersecurity department) d. Set up a Company email account to automatically forward messages to an Internet Mail account e. Set up an Internet Mail account on a Company computing device f. Use a Company email account for communications related to a side business g. Try to evade Premera security measures (for example, to access unapproved websites or to send information to people who are not authorized to access it) h. Engage in any other activity that is prohibited under state or federal laws, Premera policies and standards, or contractual agreements **Inappropriate Content** [030] Do not use Premera Communication Networks to distribute material that is: a. Fraudulent, b. Discriminatory or derogatory to any individual or group, c. Harassing, defamatory, or threatening, d. Obscene, pornographic, or sexually explicit, or that uses profane language (this includes not using obscene or profane words in the names of attachments), or e. Otherwise unlawful or inappropriate.

[035] Do not display or store inappropriate content on Company technology resources.

Political Purposes
[040] Do not use Company technology resources for any political purpose, unless that is part of your specific job responsibilities. Otherwise, your political activities and opinions could be falsely attributed to the Company and could have a serious negative impact.

Transmission of Confidential Information
[045] Premera must never send unencrypted Protected Data or Proprietary Data over end-user messaging technologies or external public services such as email, instant messaging, file sharing, or chat.

[050] Use extreme caution when sending sensitive information electronically. [050.a] This includes Protected Data, Proprietary Data of Premera or its business partners, and employment information. [050.b] Send only the minimum amount of sensitive information necessary for the intended purpose. [050.c] Send or forward messages only to people who have a business need to receive them.

[055] Premera provides a layered approach to secure email capabilities. This ensures that Protected Data and certain types of Proprietary Data are encrypted in transit.

[060] Approved uses or disclosures of Protected Data that are too large to send over secure email must be handled through the Electronic Transmission Center or another channel approved by Cybersecurity. (*See the Key Processes section for information on secure email. For assistance with large transmissions, open a request with the Electronic Transmission Center*.)

Between Employees and Campuses
[060] Protected Data and Proprietary Data may be transmitted safely within Premera Communications Networks.

[065] This includes communications to and from Users who are traveling or telecommuting, as long as the communication is through one of the following:

a. Their Company email address (premera.com, lifewise.com, etc.)
b. A Premera-managed instant-messaging client
c. Another form of electronic communication that is controlled by the Company

Beyond Company Campuses and Computer Systems
[070] Because Internet connections outside of the Company are not secure and are susceptible to tampering, additional restrictions apply to sending sensitive information outside of the Company.

[075] Send emails containing Protected Data or Proprietary Data to non-Company email addresses only over secured mechanisms that have been formally approved by the Chief Information Security Officer (CISO) or Compliance and Ethics. (*See the Key Processes section for information on approved mechanisms.*)

[080] Fax documents containing Protected Data to authorized recipients only if there is not a more secure channel available for transmitting the information. *(See the IT Secure Transfer – Fax policy for more information.)*

[085] Do not use any of the following to send Protected Data or Proprietary Data to recipients outside the Company:

a. Short Message Service (SMS) text messaging
b. Instant-messaging applications that are not controlled by the Company
c. Social media and microblogging services
d. Internet file-transfer services
e. Other electronic communication mechanisms that are not controlled by the Company

Access to Premera Email When Not on a Premera Campus

[090] When not on a Premera campus, access your Company email only through applications approved by Platform Engineering for this purpose. These include Outlook Web Access using multifactor authentication, and the email client included with the Company's mobile device management (MDM) software. [090.a] On a Premera computer, you may remotely access your email through Microsoft Outlook, just as you would on campus.

[095] The Company may require Users to install or use specific software or hardware for remote access.

Attorney-Client Communications

[100] Communications with in-house or outside counsel that contain legal advice, whether on paper or electronic, must include this warning header in the subject line: "ATTORNEY-CLIENT PRIVILEGED."

[105] Do not forward an attorney-client privileged communication to anyone, within or outside the Company, unless a Premera attorney gives you permission. [105.a] If you have such permission, copy the Premera attorney on the forwarded email unless they tell you not to.

Ownership and Expectations of Privacy

[110] All materials and messages created, stored, sent, or received on Company technology resources are the records and property of the Company. [110.a] This includes messages sent from or stored in the secure MDM container on a mobile device that has access to Company applications and data.

[115] The Company reserves the right to review all such electronic communications and to disclose this information to its representatives or other third parties. [115.a] By using Company technology resources, Users consent to routine and non-routine monitoring and disclosure, at any time and without prior notice.

[120] If you want to keep specific information personal or private, do not use Company technology resources to store or transmit it.

Malicious Software and Phishing

[125] Premera uses security software that scans incoming email for known viruses, links to malicious websites, and messages that appear to be Spam or Phishing attempts. However, this software cannot identify all potential threats.

[130] To further protect Premera from malicious software and Phishing attempts:

a. Do not open attachments or click links in a questionable or suspicious email.

b. Do not open an email or attachment if you've been warned not to do so by Cybersecurity, other Information Technology (IT) staff, or a Company communication.
c. Do not open, transmit, upload, or execute any computer-readable material or email that is of an unknown or suspicious nature, or from an unknown or questionable sender.
d. Do not try to repair or remove a suspected virus unless specifically instructed to by the IT Service Desk, TechHub, Client Technology Services, or Cybersecurity.

[135] Be cautious about opening attachments or clicking on links even within communications that appear to be legitimate. (It is always possible that a sender's account has been compromised, or that they unknowingly forwarded a malicious link or attachment.) [135.a] Report as suspicious any email with an unexpected and unusual attachment. (Examples: The attachment has an odd title, a double filename extension such as .doc.exe, or a non-standard file type). *(See the Key Processes section for information on how to report a suspicious email.)*

[140] If you experience symptoms that may indicate a malicious software infection, immediately report these symptoms to the IT Service Desk. Symptoms of a malware infection may include, but are not limited to, a sharp increase in the number of pop-up advertisements or a sudden slowdown in computer response time.

Phishing Tests

[145] Cybersecurity routinely performs Phishing tests to gauge whether Users understand how a malicious link or attachment may appear. The goal of these tests is to educate Users and keep them aware of the types of suspicious emails they may receive.

[150] Users should anticipate the follow-up actions described in the table below if they fail to recognize a Phishing test and inappropriately:

- Click a link,
- Open an attachment, or
- Provide their username and password.

Number of failed Phishing tests within a rolling 12-month period	**Follow-up actions**
First offense	• Manager notified • User must complete an assigned computer-based training
Second offense	• Manager notified • User must complete an assigned computer-based training • User may be required to complete additional training modules
Third offense	• Manager notified • User must complete an assigned computer-based training • User may be required to complete additional training modules • Written warning
Fourth offense	• Further discipline, up to termination

	[155] Assigned training must be completed within 30 days of being assigned. [160] Based on the circumstances, and regardless of the number of Phishing-test failures within the rolling 12-month period, any given Phishing-test failure by a User may be grounds for corrective action, up to and including termination of employment, in consultation with Human Resources. **Spam** [165] IT is accountable for implementing centrally managed anti-Spam technologies that: a. Operate at information system entry/exit points; b. Are configured to receive frequent updates; c. Evaluate messages sent to Premera email addresses before they reach the User's inbox, and act on unsolicited messages transported by email, email attachments, web access, or other common means, or inserted through the exploitation of information system vulnerabilities; and d. Are updated when new releases are made available, in accordance with the Company's configuration management policy and procedures. Anti-Spam technology is imperfect, and some Spam will reach Users' inboxes. Users must be cautious about opening email attachments and clicking links in emails, as explained above.
Violations of Policy	Violations of this policy may be grounds for corrective action, up to and including termination of employment.
Exception Process	Exceptions to this policy require an approved IT Exception. See the Exceptions page on the IT Governance SharePoint site for more information.
Laws, Regulations & Standards	HIPAA Security 45 CFR 164.312(e)(1) Technical Safeguards, "Transmission Security" HITRUST Common Security Framework 07.c "Acceptable Use of Assets"; 09.j "Controls Against Malicious Code"; 09.s "Information Exchange Policies and Procedures"; 09.v "Electronic Messaging"
Compliance Enforcement Controls	The Cybersecurity and Platform Engineering departments enforce this policy by monitoring User accounts. This monitoring includes but is not limited to: • Monitoring system logs • Reading emails and instant messages sent and received through Premera • Collecting statistical data such as message counts, file sizes, and logon times The Cybersecurity department uses simulated Phishing campaigns to test Users' ability to identify Phishing emails. Cybersecurity notifies management when Users fail these tests. IT uses data loss prevention technology that scans outgoing communications for Protected Data and certain types of Proprietary Data. This technology can block some messages or force them to be encrypted in transit. The Company uses mobile device management (MDM) software to ensure that only authorized devices can sync to Company email accounts.

	Premera ensures that communication protection requirements, including the security of exchanges of information, are the subject of policy development and compliance audits consistent with relevant legislation.
Contact	Any questions regarding the contents of this policy or its application should be directed to the Chief Information Security Officer.
Approval Dates	7/5/2001; November 2001; 4/16/2003; 10/20/2005; 6/19/2007; 7/23/2009; 11/1/2010; 10/18/2011; 9/18/2012; 9/13/2013; 5/29/2014; 6/2/2015; 7/6/2016; 9/6/2017; 8/20/2018; 8/1/2019; 8/25/2020; 7/22/2021; 4/5/2022; 2/20/2023; 1/18/2024 (Version History)

Key Processes	**Secure Email** Premera has several approved mechanisms for secure email. As stated above, you must use secure email when sending emails that contain Protected Data (PPI) or Proprietary Data to recipients outside the Premera companies. **Partner Connections** Premera has secure communication links with certain business partners, customers, and other organizations. Emails sent between Premera companies and these partners are always sent securely. For a list of these secure connections, see the Secure Partner Connections page on the Cybersecurity SharePoint site. This page also has instructions on how to request secure communication links with additional business partners. **Proofpoint Secure Email** You can use Proofpoint secure email to send email securely to any outside party. To do this in Outlook: 1. Before sending the message, open its **Properties** dialog box. (Click the **File** tab of the ribbon, click **Info**, and then click **Properties**.) 2. In the **Sensitivity** drop-down list, click **Confidential**, and then click **Close**. To send an email securely from the MDM email client (on a synced mobile device): 1. Include the words **SECURE MESSAGING** in the subject line of the email. For more information about Proofpoint, see the Secure Email Guides page on the Cybersecurity SharePoint site. **Email Management** Premera has size restrictions on all email boxes. If your mailbox nears the maximum size, you'll receive an automatic notification. If you reach the maximum size, you won't be able to send any new emails until you delete some old ones. Each User is responsible for managing their email in accordance with this policy and with the Records Management policy. Information Technology is not responsible for any data loss.

	Reporting Phishing Attempts If you receive an email that you think might be a Phishing attempt, click the **Report Phishing** button to delete the email and report it to Cybersecurity. The **Report Phishing** button is located on the **Home** tab of the Outlook ribbon. If your email application doesn't have a **Report Phishing** button, forward the email to phish@premera.com to report it to Cybersecurity. Cybersecurity will examine the email, and will let you know if it is legitimate and not a security threat. **Reporting Unauthorized Usage** If you notice unauthorized use of electronic communications, report it immediately to your supervisor, Employee Experience, or Regulatory Compliance and Ethics.