**Title** | Email and Other Electronic Communications  
--- | ---  
**Number** | CP.IT.SS.007.v3.4  
**Current Effective Date** | 08/20/18  
**Original Effective Date** | 07/05/01  
**Replaces** | Former name: eMail Use and Management  
**Cross Reference** | Code of Conduct; Confidentiality of Protected Personal Information Policy; Computer, Network and Telephone Usage Policy; Encryption Policy; Records & Information Management Policy; IT Email Security Standard; 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 all Users who have been granted access to Company email or other text-based or multimedia electronic communication services provided by the Company. Does not apply to telephone services, which are covered in the Computer, Network and Telephone Usage policy.  

**Definitions**  
- **“Internet Mail”** means a personal email account that is accessed via an Internet browser. Examples include accounts set up through Yahoo and Google.  
- **“Phishing”** means a cyberattack method 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. Phishing attacks can be carried out using a variety of different types of messages, including emails, instant messages, SMS text messages, and phone calls.  
- **“Premera Communication Networks”** means data transmission services that are maintained by Premera and/or Premera’s managed service providers to allow communication among Premera PCs, servers, business partners, and the Internet.  
- **“Protected Personal Information (PPI)”** is defined in the [Confidentiality of Protected Personal Information policy](#).  
- **“Spam”** means unsolicited or undesired bulk electronic messages.  
- **“Users”** means all individuals granted access to Premera technology resources, including employees, contractors, subcontractors, managed service provider staff, and consultants.
<table>
<thead>
<tr>
<th>Policy</th>
<th>Authorized Use of Company Electronic Communications Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Company provides email and other electronic communication services primarily for business purposes. Users may make occasional or incidental use of these services for personal correspondence, so long as such use is in compliance with the Personal Use provisions of the Computer, Network, and Telephone Usage policy.</td>
<td></td>
</tr>
</tbody>
</table>

Users are responsible for ensuring that their use of electronic communications is ethical and lawful, and the content of communication is truthful and accurate. Users must also take care that non-business communications that can be traced back to Premera (for example, emails sent from a Company email address) do not appear to make pronouncements or express opinions on behalf of the Company.

Users are responsible for completing training, including reviewing this policy, that makes them aware of the existing limits on their use of Premera’s information, and of Premera assets associated with information processing facilities.

| Unauthorized Use of Company Electronic Communication Services |
| Prohibited Activity: The following uses of Premera Communication Networks are strictly prohibited under this policy: |
| • Sending Spam, knowingly spreading viruses, and Phishing (except for Phishing tests performed by or for the Cybersecurity department); |
| • Setting up a Company email account to automatically forward messages to an Internet Mail account; |
| • Using a Company email account for correspondence related to a side business; |
| • Attempting to evade Premera security measures (for example, to access unapproved websites or to provide information to persons who are not authorized to access it); and |
| • Engaging in any other activity that is prohibited under state or federal statute, Premera policies and standards, or contractual agreements. |

| Inappropriate Content: Users are not to use Premera Communication Networks to distribute material that is: |
| • Fraudulent; |
| • Discriminatory or derogatory to any individual or group; |
| • Of a harassing, defamatory, or threatening nature; |
| • Obscene, pornographic, or sexually explicit; or |
| • Otherwise unlawful or inappropriate. |

Users are not to display or store electronic messages or attachments containing these types of materials on Company technology resources.

| Political Purposes: Use of Company technology resources for any political purpose, unless specifically required as part of a User’s job responsibilities, is strictly prohibited. A User’s political activities and opinions could be falsely attributed to the Company and could have a serious negative impact. |

| Transmission of Confidential Information |
| Premera never sends unencrypted sensitive information over end-user messaging technologies such as email, instant messaging, or chat. |

Any electronic transmission of confidential information must be done with extreme caution. This includes PPI, Premera and business partner proprietary information, and employment information. Messages must include only the minimum information.
necessary for the intended purpose, and must be addressed or forwarded only to those individuals who have a need to receive the confidential information.

Premera provides a layered approach to secure email capabilities to ensure encrypted transmission of PPI and other confidential data when such transmission is allowed by corporate policy and departmental processes. Approved uses or disclosures of PPI that are too large for transmission via 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, contact the ETC Mailbox.)

**Between Employees and Campuses:** Confidential information, including PPI, may be transmitted safely within Premera Communications Networks. This includes communications to and from Users who are traveling or telecommuting, as long as the communication is via their Company email address (premera.com, lifewise.com, etc.), Premera’s instant-messaging client, or another form of electronic communication that is controlled by the Company.

**Beyond Company Campuses and Computer Systems:** Because Internet connections outside of the Company are not secure and are susceptible to tampering, additional restrictions apply to the transmission of confidential information outside of the Company:

- Emails containing PPI may be sent to non-Company email addresses only via secured mechanisms that have been formally approved by the Chief Information Security Officer (CISO) or Compliance & Ethics. (See the Key Processes section for information on approved mechanisms.)
- Documents containing PPI may be faxed to authorized recipients as long as senders follow their department or division’s Confidentiality of PPI procedure.
- SMS text messaging, non-Company instant-messaging applications, social media and microblogging services, Internet file-transfer services, and other electronic communication mechanisms that are not controlled by the Company may not be used for the transmission of PPI.

**Access to Premera Email When Not on a Premera Campus**
Many applications for remotely accessing email, such as Outlook Anywhere, do not meet Premera’s security requirements. When not on a Premera campus, Users may access their Premera email only via applications approved by IT Infrastructure for this purpose, such as Outlook Web Access and the email client included with the Company’s mobile device management (MDM) software. Employees with computers configured for remote access may access their email through Microsoft Outlook, just as they would when on campus.

Remote access via any of these methods requires approval from management and IT. Users may also be required to install or use specific software or hardware if they want remote access.

**Attorney-Client Communications**
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.”

An attorney-client privileged communication must not be forwarded to anyone, within or outside the Company, without the permission of a Premera attorney. If such permission is given, the Premera attorney must be copied on the forwarded email unless he or she instructs otherwise.
**Ownership and Expectations of Privacy**

All materials and messages created, stored, sent, or received on Company technology resources are the records and property of the Company. This includes messages sent from or stored in the secure MDM container on a synced mobile device.

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

If Users wish to keep specific information personal or private, they should not use Company technology resources to store or transmit that information.

**Malicious Software and Phishing**

Company software scans incoming email for known viruses, links to malicious websites, and messages that appear to be spam or Phishing attempts. However, this technology cannot identify all potential threats. In order to further protect Premera from malicious software and Phishing attempts, Users:

- Must not open attachments or click links in a questionable or suspicious email;
- Must not open an email or attachment once warned not to do so by Cybersecurity, other Information Technology staff, or a Company communication;
- Must 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; and
- Must not attempt to repair or eradicate a suspected virus except under specific instructions from IT Service Desk, Client Technology Services, or Cybersecurity personnel.

Users must be cautious about opening attachments or clicking on links even within electronic communications that appear to be legitimate. (It is always possible that a sender’s account has been compromised, or that they have unknowingly forwarded a malicious link or attachment.) Users must 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.)*

If a User experiences symptoms indicative of malicious software, such as a sharp increase in pop-up advertisements or a sudden slowing of computer response times for local actions such as opening a file from the hard disk, the User must immediately report these symptoms to the IT Service Desk.

**Protecting Against Spam**

IT is accountable for implementing centrally-managed anti-Spam technologies at information system entry/exit points that:

- Are configured to receive frequent updates; and
- Evaluate messages sent to Premera email addresses before they reach the User’s inbox.

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.
<table>
<thead>
<tr>
<th>Suspicious email messages should be reported through existing Phishing message submission channels. (See <em>Key Processes.</em>)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Violations of Policy</strong></td>
</tr>
<tr>
<td><strong>Exception Process</strong></td>
</tr>
</tbody>
</table>
| **Controls** | The Cybersecurity and IT Infrastructure departments enforce this policy through monitoring of user accounts, including but not limited to: monitoring system logs; reading email sent and received through Premera; reading instant messages; and collecting statistical data such as message counts, file sizes, and logon times.  
IT users technology that scans outgoing communications for the presence of PPI and other confidential information, and can block such messages or force them to be encrypted in transit.  
Mobile device management (MDM) software is used to ensure that only authorized devices can be synced to Company email accounts. |
| **Contact** | Any questions regarding the contents of this policy or its application should be directed to the Chief Information Security Officer. |
| **Approval Dates** | 08/20/18; 09/06/17; 07/06/16; 06/02/15; 05/29/14; 09/13/13; 09/18/12; 10/18/11; 11/1/10; 07/23/09; 06/19/07; 10/20/05; 04/16/03; 09/2001 (Version History) |
### Key Processes

**Secure Email**
Premera has several approved mechanisms for secure email. You must use secure email when sending emails containing PPI, Company confidential information, or other sensitive information to recipients outside the Premera companies.

**Partner Connections**
Premera has secure communication links with certain business partners, customers and other companies. Emails sent between Premera companies and these partners is always sent securely.

For a list of these secure connections, see the Secure TLS/VPN Partner Connections page on the Cybersecurity iHub site: [http://ihub/depts/security/Pages/Secure-Partner-Connections.aspx](http://ihub/depts/security/Pages/Secure-Partner-Connections.aspx). To request secure communication links with additional business partners, contact the IT Service Desk.

**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 is securely from the MDM email client (on synced mobile devices):

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 iHub site: [http://ihub/depts/security/Pages/Secure-Email-Guides.aspx](http://ihub/depts/security/Pages/Secure-Email-Guides.aspx)

**Email Management**
Size restrictions have been implemented for all email boxes. If your mailbox reaches 90% of the maximum limit, you’ll receive an automatic notification. If you reach the maximum limit, you won’t be able to send any electronic messages until you delete some emails.

Each User is responsible for managing their email in accordance with this policy and with the **Records & Information Management Policy**. See the Records Management team’s **Email Best Practices** document for guidance. Information Technology is not responsible for any data loss.

Refer to the ServiceNow Knowledge topic “Best Practices for Computer Use” for general guidance on creating and managing emails.

**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 you receive such an email on your smartphone, you can report it to Cybersecurity by forwarding it to phish@premera.com.

Cybersecurity will examine the email, and will let you know if it turns out that the email is legitimate and not a security threat.

**Reporting Unauthorized Usage**
If you notice unauthorized use of electronic communications, report it immediately to your supervisor, Human Resources, or Compliance & Ethics.