Awareness Standard for Canadian Telecommunications Service Providers (CTSPs)

V1.1 January 20, 2020

Authored by: Canadian Telecommunications Cyber Protection (CTCP) working group

for

Presentation by: Canadian Security Telecommunications Advisory Committee (CSTAC)
Contents

Contents ................................................................................................................................. 2
Revision History ...................................................................................................................... 3
1. Awareness Standards.......................................................................................................... 4
1.1 Policy and Standards Controls .................................................................................. 4
  1.1.1 Policy and Standards Creation Control: .......................................................... 4
  1.1.2 Policy and Standards Maintenance Control: .................................................. 4
1.2 Education and Training ............................................................................................... 4
  1.2.1 Basic Security Awareness Training Controls: ................................................ 4
  1.2.2 Specialized/Role Based Training Controls: ..................................................... 4
  1.2.3 Ongoing Training Controls: ............................................................................... 5
  1.2.4 Records and Metrics Control: ........................................................................... 5
1.3 Internal Security Awareness....................................................................................... 5
  1.3.1 Program Creation Control:................................................................................. 5
  1.3.2 Measuring Program Efficacy Controls:............................................................ 5
1.4 Security Community/Industry Contacts Control: .................................................... 6
1.5 External Security Awareness Controls: .................................................................... 6
Annex B – References............................................................................................................. 7
Revision History

The following table highlights edit changes to the document.

<table>
<thead>
<tr>
<th>Editor</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lori Welland, TELUS</td>
<td>September 13, 2019</td>
<td>Draft started</td>
</tr>
<tr>
<td>Kevin Miller, SaskTel</td>
<td>September 17, 2019</td>
<td>Edits</td>
</tr>
<tr>
<td>Marc Kneppers, TELUS</td>
<td>January 20, 2020</td>
<td>Minor updated based on stakeholder feedback</td>
</tr>
<tr>
<td>Kevin Miller, SaskTel</td>
<td>March 3, 2020</td>
<td>Minor updates to align with standard format</td>
</tr>
</tbody>
</table>

The following table highlights major content or policy changes to the document.

<table>
<thead>
<tr>
<th>Section</th>
<th>Contribution</th>
<th>Date</th>
</tr>
</thead>
</table>
1. Awareness Standards

1.1 Policy and Standards Controls

CTSPs should have the capability to:

The Policy and Standards section of this standard define recommended controls for Awareness. Creating an effective security awareness program is key to securing any organization, large or small. Demystifying security and educating users about their role in protecting your organization helps cultivate a robust first line of defence.

1.1.1 Policy and Standards Creation Control:

CTSPs should have the capability to:

1. Publish corporately documents that detail specific rules and best practices around key security basics (i.e. data classification and management, access control, device management, corporate email use, passwords and acceptable password manager tools etc).

1.1.2 Policy and Standards Maintenance Control:

CTSPs should have the capability to:

1. Conduct a regular review of applicable policies, process documents and standards, updating as necessary.
2. Define review cadence based on organizational needs and/or any applicable audit / compliance requirements.

1.2 Education and Training

1.2.1 Basic Security Awareness Training Controls:

CTSPs should have the capability to:

1. Provide mandatory training as part of new hire process (employees and contractors)
2. As required, educate users on system updates and/or new application roll outs.

1.2.2 Specialized/Role Based Training Controls:

CTSPs should have the capability to:

1. Ensure training is completed before providing access to sensitive data.
2. Ensure training is completed before a user takes on full role responsibilities (i.e. customer facing employee must complete social engineering training before working with customers).

1.2.3 Ongoing Training Controls:
CTSPs should have the capability to:
1. Create and manage ongoing program to regularly educate users.
2. Maintain records of results and increase difficulty of training, change training format, etc. as applicable to ensure continuous learning.
3. Annual training – require users to acknowledge (electronically or in writing), that they have reviewed and understand the organization’s security policies and standards.

1.2.4 Records and Metrics Control:
CTSPs should have the capability to:
1. Maintain records of user training completion to ensure compliance with specified training requirements.
2. Follow up and escalate to management as necessary should users not complete training within specified timeframe.

1.3 Internal Security Awareness

1.3.1 Program Creation Control:
CTSPs should have the capability to:
1. Create program content to engage and educate users using multiple methods of communication, including posters, emails, bulletins, articles, videos, web based and in person training, meetings, events and promotional materials.
2. Provide a single ‘hub’ for employees and contractors to access security awareness information.

1.3.2 Measuring Program Efficacy Controls:
CTSPs should have the capability to:
1. Collect all metrics available (i.e. training completion, article reads, event/promotion participation, etc) to measure impact of awareness program content.
2. Solicit user feedback to both measure program impact and identify groups who may struggle with access to content due to the nature of their role and/or would benefit from more specialized awareness subject matter.
3. At a minimum, conduct annual review of program strategy and metrics, adjusting as necessary to create increased/maximum use engagement.

1.4 Security Community/Industry Contacts Control:
CTSPs should have the capability to:

1. Discuss program development strategies, use groups as a resource to brainstorm solutions to shared/common program challenges.
2. Discuss approaches for educating users about new/emerging threats and/or new approaches to training users about known threats (different tools, platforms, etc)

1.5 External Security Awareness Controls:
CTSPs should have the capability to:

1. Identify potential situations in which your customers and end users can put their security at risk when interacting with your organization
2. Educate customers and end users on how to mitigate the risk and/or avoid potential threats (e.g how to set a strong password and two-factor authentication, how to identify and avoid phishing emails, etc.)
3. Provide a way to be notified of potential security threats and challenges associated with your brand (e.g an inbox for reporting suspected phishing emails).
Annex B – References

These best practices leverage work done by other standards bodies referenced earlier in the document or below:

- International Organization for Standardization (ISO), 27001, [https://www.iso.org/isoiec-27001-information-security.html](https://www.iso.org/isoiec-27001-information-security.html); retrieved Jan 20, 2020
- International Organization for Standardization (ISO), 27002, [https://www.iso.org/standard/54533.html](https://www.iso.org/standard/54533.html); retrieved Jan 20, 2020
- National Institute of Standards and Technology (NIST), CyberSecurity Framework, [https://www.nist.gov/cyberframework](https://www.nist.gov/cyberframework); retrieved Jan 20, 2020
- Payment Card Industry (PCI), Security Standards, [https://www.pcisecuritystandards.org/pci_security/standards_overview](https://www.pcisecuritystandards.org/pci_security/standards_overview); retrieved Jan 20, 2020