Vendor Management Standard for Canadian Telecommunications Service Providers (CTSPs)

V1.1 Jan 15, 2020

Authored by: Canadian Telecommunications Cyber Protection (CTCP) working group for Presentation by: Canadian Security Telecommunications Advisory Committee (CSTAC)
Vendor Management Standards for Canadian Telecommunications Service Providers (CTSPs)

Contents

Revision History.................................................................................................................................................. 3

1. Vendor Management Standards.................................................................................................................... 4
   1.1 Equipment Supply Chain ............................................................................................................................ 4
   1.2 Vendor Security Management.................................................................................................................... 4
Vendor Management Standards for Canadian Telecommunications Service Providers (CTSPs)

# 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>CTCP Architecture Team</td>
<td>June 1, 2019</td>
<td>Updated content</td>
</tr>
<tr>
<td>Kevin Miller, SaskTel</td>
<td>Sept 17, 2019</td>
<td>Draft started</td>
</tr>
<tr>
<td>Marc Kneppers, TELUS</td>
<td>Jan 15, 2020</td>
<td>Minor updated based on stakeholder feedback</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>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1. Vendor Management Standards

1.1 Equipment Supply Chain
The CTSPs should have the capability to:

1. Select or define security standards for procurement of systems, devices, and software.
2. Identify and enforce hardening requirements for suppliers.
3. Ensure that relevant security standards are included in purchase agreements, Requests for Proposals (RFPs), and contracts.
4. Require third parties to test and verify all equipment, systems, and software in accordance with well-known best practices (e.g. Common Criteria). Depending on criticality of the system, assurance level required will vary.
5. Avoid doing business with vendors who do not meet security standards unless the vendors are willing to address the issues or mitigating controls can be introduced.
6. Define procedures to ensure that vendors are following the standards defined by the CTSP.
7. Support a compliance verification program to ensure that vendors are following the standards defined by the CTSP and are have a product lifecycle that includes the regular maintenance and update of the product.

1.2 Vendor Security Management
CTSPs should have the capability to:

1. Limit vendor access to only those systems for which vendors provide support.
2. Demonstrate that the practices of their vendors do not impact or degrade the security level of CTSPs’ infrastructures.
3. Monitor and audit vendor activity to ensure the integrity and security of their networks.
4. Ensure that security hardening requirements are included in Service Level Agreement (SLA) clauses with third party providers.