Remote Administration Software

Standard ID
IOT-CS-TEC-002

Published Date
8/9/2017

Effective Date
9/1/2017

Last Updated
7/21/2017

Next Review Date
7/21/2018

Policy
06.0 Access Control (PR.AC)
  06.3 PR.AC-3
    06.3.1 Remote Access

Purpose
To control the tools used to remotely administer systems, reducing the amount of unknown software. Further, the limited number of tools will reduce the amount of potential vulnerabilities.

Scope
IOT Supported Entities

Statement
All remote access tools used to communicate between assets and other systems must comply with the following requirements:

Remote Access Tools provide a mechanism to connect between client and server. Proper configuration is important for secure usage of these tools, therefore mandatory configuration procedures are provided for each of the approved tools. The approved software list is subject to change based on determination from the Indiana Office of Technology (IOT).

Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the data encryption policy (IOT-CS-SEC-003).

All antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way. All remote access tools must be purchased through the standard procurement process, and the information technology group must approve the purchase.
The approved software with approved protocols is listed in the chart below:

<table>
<thead>
<tr>
<th>Tool</th>
<th>RDP</th>
<th>SSH</th>
<th>X11</th>
<th>License Needed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Remote Desktop</td>
<td>X</td>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Royal TS</td>
<td>X</td>
<td>X</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Remote Desktop Manager</td>
<td>X</td>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Mobaxterm</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Yes</td>
</tr>
<tr>
<td>Putty</td>
<td></td>
<td>X</td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

For use of an approved tool for remote access, a Helpdesk ticket will need to be entered with manager approval and billing information, if a software license is required. The software will then be pushed out by Microsoft System Center Configuration Manager (SCCM) for desktops.

**Roles**
All Personnel
Information Asset Owners/System Owners

**Responsibilities**
All personnel and Information Asset Owners/System Owners shall be aware of the tools available for remote administration and must remove any unauthorized software that deviates from the published Standard.

**Management Commitment**
Management shall ensure that all remote administration software is authorized for their respective agency.

**Coordination Among Organizational Entities**
Agencies shall coordinate with IOT for use of remote administration software.

**Compliance**
All remote administration software found on State machines that are not approved are subject to removal.

**Exceptions**
Exceptions will be handled on a case-by-case basis through the State CISO and COO.

**Associated Links**
Software Licensing Request