<table>
<thead>
<tr>
<th>TSC Category</th>
<th>Operations and User Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSC</td>
<td>Access Control Management</td>
</tr>
<tr>
<td>TSC Description</td>
<td>Manage access control to ensure authorised access in accordance with the organisation's policies</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TSC Proficiency Description</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
<th>Level 6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EPW-OUS-2016-1.1</td>
<td>EPW-OUS-3016-1.1</td>
<td>EPW-OUS-4016-1.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Apply access control policies by following the access limitation and responsibilities granted</td>
<td>Develop access control policies in alignment with the organisation's policies and cybersecurity advisories</td>
<td>Develop organisational access control frameworks to determine granting and revocation of user access control rights</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Knowledge**

- Access enforcement methods
- Remote access methods
- Wired and/or wireless authentication methods
- Least privilege principles
- Account management principles
- Access control technologies
- Troubleshooting tools and techniques
- Access control methods
- Wired and/or wireless access restrictions
- Authorisation methods
- Types of access control systems
- Access control rogue connection audit techniques
- Wireless access restrictions
- Access control risk mitigation techniques
- System interfacing
- Investigative techniques
- Root cause analysis techniques
- Host network access control mechanisms
- Organisational access control needs
- Financial costs for access control changes
- Laws and regulations related to cybersecurity
- Stakeholder communication channels
- Best practices and industry trends for access control
- Policy-based and risk adaptive access controls
## Abilities

- Perform troubleshooting for verified users with access control issues
- Grant users access control rights according to defined frameworks and best practices
- Manage access control lists
- Translate access control policies into feasible solutions based on existing system architectures
- Solve system interfacing issues or problems
- Perform audits on access control systems to identify rogue connections
- Analyse and recommend mitigative measures to reduce access control breaches
- Design group policies and access control lists to ensure compatibility with organisational standards and needs
- Develop organisational access control frameworks in compliance to laws and regulations
- Define access control policies
- Determine communication plans with relevant stakeholders on access control breaches
- Develop access control audit frameworks
- Set frameworks to determine granting and revocation of user access control rights
- Assess adequacy of access controls based on principles of least privilege and need-to-know
- Evaluate and adopt new access control technologies

## Range of Application

Range of application includes, but is not limited to:

- Gas Systems Operations
- Transmission and Distribution
- Automated systems
  - Smart grids
  - Smart homes
  - Substation designs