

# ISO/IEC 27033-7:2023-11 (E)

## Information technology - Network security - Part 7: Guidelines for network virtualization security

---

<b>Contents</b>		<b>Page</b>
	<b>Foreword</b> .....	<b>iv</b>
	<b>Introduction</b> .....	<b>v</b>
<b>1</b>	<b>Scope</b> .....	<b>1</b>
<b>2</b>	<b>Normative references</b> .....	<b>1</b>
<b>3</b>	<b>Terms and definitions</b> .....	<b>1</b>
<b>4</b>	<b>Abbreviated terms</b> .....	<b>2</b>
<b>5</b>	<b>Overview</b> .....	<b>4</b>
	5.1 General.....	4
	5.2 Description of network virtualization.....	4
	5.3 Security model.....	4
	5.3.1 Model of network virtualization security.....	4
	5.3.2 Network virtualization components.....	6
<b>6</b>	<b>Security threats</b> .....	<b>6</b>
<b>7</b>	<b>Security recommendations</b> .....	<b>7</b>
	7.1 General.....	7
	7.2 Confidentiality.....	7
	7.3 Integrity.....	8
	7.4 Availability.....	8
	7.5 Authentication.....	8
	7.6 Access control.....	8
	7.7 Non-repudiation.....	9
<b>8</b>	<b>Security controls</b> .....	<b>9</b>
	8.1 General.....	9
	8.2 Virtual network infrastructure security.....	10
	8.3 Virtual network function security.....	10
	8.4 Virtual network management security.....	11
	8.4.1 SDN controller security.....	11
	8.4.2 NFV orchestrator security.....	12
<b>9</b>	<b>Design techniques and considerations</b> .....	<b>12</b>
	9.1 Overview.....	12
	9.2 Integrity protection of platform.....	13
	9.3 Hardening for network virtualization.....	13
	9.4 API authentication and authorization.....	13
	9.5 Software defined security for virtual network.....	13
	<b>Annex A (informative) Use cases of network virtualization</b> .....	<b>15</b>
	<b>Annex B (informative) Detailed security threat description of network virtualization</b> .....	<b>18</b>
	<b>Bibliography</b> .....	<b>22</b>