



P7100: NETWORK ARCHITECTURE POLICY

DOCUMENT NUMBER:	P7100
EFFECTIVE DATE:	OCTOBER 11, 2016
REVISION:	1.1

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (ADOA), the Agency shall establish a coordinated plan and program for information technology (IT) implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statutes (A.R.S.)§ 18-104.

2. PURPOSE

The purpose of this policy is to define the State of Arizona's strategy for providing a unified network for voice, video and data serving all budget units (BU) in accordance with ARS §41-712.

3. SCOPE

This policy shall apply to all state BUs.

4. EXCEPTIONS

4.1 PSPs may be expanded or exceptions may be taken by following the Statewide Policy Exception Procedure.

4.1.1 With regards to existing IT products and services, BU subject matter experts (SMEs) should inquire with the vendor and the state or agency procurement office to ascertain if the contract provides for additional products or services to attain compliance with PSPs prior to submitting a request for an exception in accordance with the Statewide Policy Exception Procedure.

4.1.2 With regards to procurement of new IT products and services, prior to selecting and procuring information technology products and services, Agency SMEs shall comply with Statewide IT PSPs when specifying, scoping, and evaluating solutions to meet current and planned requirements.

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall be ultimately responsible for the correct and thorough completion of Statewide IT PSPs throughout all state BUs.

- 5.2** State Chief Networking Officer (CNO) shall:
- 5.2.1** Be responsible for the development and implementation of statewide networking strategic plan with the exclusion of agency dedicated and managed Data Centers and/or independent propriety networks, i.e. ACIJS network;
 - 5.2.2** Be responsible for complying with all federal, state, and local statutes, regulations, policies and standards;
 - 5.2.3** Identify all stakeholders, be responsible for documenting requirements and setting minimum service level agreements (SLAs);
 - 5.2.4** Be responsible for monitoring network performance and stakeholder satisfaction levels;
 - 5.2.5** Be responsible for implementing appropriate corrective action when required; and
 - 5.2.6** Be responsible for selecting and managing third-party service providers.
- 5.3** BU Administrator shall:
- 5.3.1** Be responsible for providing requirements and feedback timely; and
 - 5.3.2** Complying with all terms of service.

6. STATEWIDE POLICY

- 6.1** In accordance with ARS §41-712, the Telecommunication Program Office also known as Enterprise Infrastructure and Communications (EIC) shall provide voice, video and data networks supporting all State BUs.
- 6.2** EIC shall establish and manage steering and oversight committees for voice, video and network composed of key stakeholders. The committees shall review all plans, budgets and investments and will monitor performance and dissemination of information.
- 6.3** EIC shall manage the day-to-day operations of the network and monitor performance against documented service level agreements.
- 6.4** EIC shall develop a pricing model and pass all costs along to State BUs based on usage.
- 6.5** EIC shall select and manage third-party service providers in accordance with state procurement rules.
- 6.6** EIC shall design and implement the voice, video and data network that comply with the state network standards.
- 6.7** EIC shall develop capacity forecasts and monitor usage to ensure adequate resources are available to stakeholders.
- 6.8** EIC shall ensure that network redundancy for critical services is part of the Enterprise Network Architecture and implemented with automatic, timely failover features as specified within the scope of the AZNet contract for core systems; budget units can opt for redundancy at remote locations subject to terms and conditions of the AZNet contract.

- 6.9** EIC shall ensure that all security and privacy policies, standards and procedures are implemented, including by the BUs.
- 6.10** EIC shall ensure that all network equipment and software is current with all appropriate patches and upgrades installed at all times.
- 6.11** EIC shall ensure that all wireless networks have appropriate controls, including restricted access and encryption if necessary to protect confidential data.
- 6.12** EIC shall ensure that remote access is provided using virtual private network (VPN).
- 6.13** EIC shall ensure that configuration change management is enforced and that all changes are tested prior to promotion to production and monitored to verify proper performance.
- 6.14** EIC shall develop, document, and test a disaster recovery and business continuity plan for all critical services.
- 6.15** EIC shall provide 24X7 incident management for stakeholders and monitor response times.
- 6.16** EIC shall develop and document the infrastructure and cabling requirements that meet the statewide network standards.

7. DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms located on the ADOA-ASET website.

8. REFERENCES

- 8.1** Arizona Revised Statutes (A.R.S.) § 18-104.
- 8.2** Arizona Revised Statutes (A.R.S.) § 41-712.

9. ATTACHMENTS

None

10. REVISION HISTORY

Date	Change	Revision	Signature
7/20/2015	Initial version	1.0	
10/11/2016	Updated all the Security Statutes	1.1	Morgan Reed, State CIO and Deputy Director