OKLAHOMA
Office of Management
& Enterprise Services

Site to Site VPN Encryption Standard

Introduction

Data exchanged over the internet without encryption is vulnerable to security breach. To ensure the confidentiality of conversations with remote partners along with the integrity of the exchanged data, OMES Cyber Command, in cooperation with the OMES network team, must define which operational virtual private network security parameters are acceptable.

Purpose

This document establishes both the minimum and preferred configuration standards for IPsec VPN communications.

Definitions

IPsec – Internet Protocol Security is a widely used network layer security control for protecting communications. IPsec is a framework of open standards for ensuring private communications over Internet Protocol networks.

IKE – Internet Key Exchange is an IPsec-based tunneling protocol that provides a secure VPN communication channel between peer VPN devices.

Standard

The preferred and minimum IKE phase 1 and phase 2 security parameters are defined as follows:

Preferred:

IKE (Phase 1)	
IKE Mode	Main
IKE Version	V2
Encryption Algorithm	AES-256-CBC
Authentication Algorithm	SHA-384
Key Exchange	Group 19
Lifetime (seconds)	28800
Authentication Method	PSK (Minimum 64 Characters)

IKE (Phase 2)	
Protocol	ESP
Encryption Algorithm	AES-256-CBC
Authentication Algorithm	HMAC-SHA-256
Lifetime (seconds)	3600
PFS Key Group	Group 19

Minimum:

IKE (Phase 1)	
IKE Mode	Main
IKE Version	V1
Encryption Algorithm	AES-128-CBC
Authentication Algorithm	SHA-256
Key Exchange	Group 14
Lifetime (seconds)	28800
Authentication Method	PSK (Minimum 64 Characters)

IKE (Phase 2)	
Protocol	ESP
Encryption Algorithm	AES-128-CBC
Authentication Algorithm	HMAC-SHA-256
Lifetime (seconds)	3600
PFS Key Group	Group 14

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 08/29/2022	**Review cycle:** Annual
Last revised: 08/29/2022	**Last reviewed:** 08/08/2023
Approved by: Joe McIntosh, Chief Information Officer	