# State of Oklahoma Third-Party Risk Management Policy

## Introduction

OMES Information Services Division ("ISD") is committed to preventing incidents that may impact the confidentiality, integrity, and availability of information assets through third-party risk management for the State of Oklahoma ("State"). Third-party risk management is a critical component of the OMES ISD information security program which helps ensure that any risk to confidentiality, integrity, and availability is identified, analyzed, and maintained at acceptable levels.

State policy requires the performance of routine assessments to identify risk and ensure appropriate controls. Security assessments allow alignment of information security with business objectives and regulatory requirements. Identifying information security risk and control requirements from the onset is essential, and far less costly than retrofitting or addressing the impact of a security incident. Furthermore, these assessments allow management to prioritize and focus on areas that pose the greatest impact to critical and sensitive information assets; providing the foundation for informed decision-making regarding information security.

OMES ISD takes into account vulnerabilities, threat sources, and security controls that are planned or in place. These inputs are used to determine the resulting level of risk posed to information, systems, processes, and individuals that support business functions. While third-party risk management and related assessment activities can take many forms (e.g., formal risk assessment, audits, security reviews, configuration analysis, vulnerability scanning and testing), all are aimed at the same goal - identifying and acting on risk to improve overall security posture. It should be noted that an entity can never completely eliminate risk but can take steps to manage risk.

As per OMES ISD policy, any supplier that is accessing, processing, transmitting or storing State of Oklahoma data must be appropriately managed for risk and undergo risk assessments as part of its life cycle.

## Purpose

The purpose of this document is to ensure OMES ISD performs third-party assessments for suppliers who are accessing, processing, transmitting or storing data in compliance with OMES ISD security policies, standards, and procedures. Details regarding OMES ISD security policies, standards, and procedures can be found in the State of Oklahoma Information security Policy, Information Security Policy, Procedures, Guidelines document.

**Definitions**

Third Party – Any Contractor, service provider, consultant or any other individual and/or organization external to state government providing services or behalf of, for, or as an agent of state government.

**General Use**

1. Security Categorization
    i. The State Agency shall categorize data as confidential by system owners, including protected health information (PHI) and personally identifiable information (PII), in accordance with applicable federal and state laws, directives, policies, and regulations, standards, and guidance.
2. Risk Assessment
    i. OMES ISD shall conduct a third-party security assessment. The assessment should address the likelihood and magnitude of harm should there be unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores or transmits.
    ii. OMES ISD shall document risk assessment results in annual risk assessment.
    iii. OMES ISD shall review risk assessment results annually.
    iv. OMES ISD shall disseminate risk assessment results to stakeholder.
    v. OMES ISD shall update the third-party security assessment annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.
3. Vendor Management
    i. All third parties who are given access to State information, information systems, or information assets belonging to the State must complete a security assessment. The purpose of the assessment is for the State of Oklahoma to identify and manage the risk stemming from the business partnership.
    ii. A supplier is required to complete an assessment if accessing, processing, storing or transmitting State data. The assessment is not restricted to a specific service or solution; this assessment is for the vendor to be assessed from a security standpoint. The tools, platforms, and procedures should have no bearing on the enterprise security controls of the supplier.

**Authority**

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Agencies requesting exceptions shall provide such requests to the CISO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the Agency, initiatives, actions and a time-frame for achieving the minimum compliance level with

the policies set forth herein. The CISO shall review such requests; confer with the requesting Agency.

**References**

1. National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Risk Assessment (RA), NIST SP 800-12, NIST SP 800-30, NIST SP 800-39, NIST SP 800-40, NIST SP 800-70, NIST SP 800-100, and NIST SP 800-115; NIST Federal Information Processing Standards (FIPS) 199
2. State of Oklahoma Hosting Agreement