Security and Business Continuity

Vendor Management Policy and Procedures

Section 1 – Introduction

1.1 Overview

In accordance with the mandated security requirements which were adopted and approved by management, LEAP Agency (“LEAP”) has established a formal Vendor Management policy and supporting procedures. This policy is to be implemented immediately along with all relevant and applicable procedures. Additionally, this policy is to be evaluated on a(n) annual basis for ensuring its adequacy and relevancy regarding LEAP's needs and goals.

1.2 Purpose

The purpose of this policy is to provide LEAP with a documented and formalized Vendor Management process that is to be adhered to and utilized throughout the organization at all times. Compliance with the stated policy and supporting procedures helps ensure the safety and security of LEAP system resources.

Increased use of outsourcing to various third-parties has created a need for monitoring such entities for baseline compliance measures with regards to LEAP's minimally accepted standards for security. Specifically, all outsourced processes, procedures, and practices relevant to LEAP's business are to be monitored on a regular basis, which includes undertaking various measures on all third-parties providing critical services. The subsequent policies and procedures relating to vendor management initiatives for LEAP strive to ensure the overall confidentiality, integrity and availability of the organization's network and its resources.

1.3 Purpose

This policy applies to all parties operating within the company’s network environment or utilizing Information Resources. It covers the data networks, LAN servers, and personal computers (stand-alone or network-enabled), located at company offices and company production related locations. These systems are under the jurisdiction and/or ownership of the company or subsidiaries, and any personal computers, laptops, mobile device, and/or servers authorized to access the company’s data networks. No third-party agent is exempt from this policy.

Section 2 – Vendor Management Policy

LEAP is to ensure that the vendor management policy adheres to the following conditions, for the purpose of complying with the mandated organizational security requirements:

2.1 Custodian

The acting Agency Principal for LEAP shall serve as the custodian of the Vendor Management Process and is charged with ensuring that due diligence and adherence to the Vendor Management policy is followed for all vendor evaluations.

2.2 Classifications of Vendor Risk

During the vendor selection process, the custodian will assess the risks associated with the vendor inadequacy (e.g. quality of services, delivery schedules, warranty assurances, user support, etc.). Prior to determining the risk, the custodian will consider the criticality of the services and apply a ranking according to the following criteria:

(3) High Risk

Services in this category include those considered “mission critical” to the organization's operation. The organization would not be able to operate at an adequate capacity without the availability of such services.

(2) Medium Risk

Services in this category include those of significance to business operations, but not considered “mission critical” to business impact.

(1) Low Risk

Services in this category include those of minor impact to the organization's operations or for whom the organization would have an acceptable vendor readily available, or an alternative means to process. Such services would be considered to have a nominal business impact, and would not be considered as “mission critical”.

2.3 Risk Management

Risk management is the process of identifying, measuring, monitoring and managing associated risk. Risk exists whether LEAP performs work internally or outsources to accepted third-party organizations.

The Vendor Management custodian will consider some or all of the following factors in evaluating the quantity of risk at the inception of an outsourcing decision. The degree to which these factors will be

considered depends on the risk rating of the function(s) provided by the vendor.

2.3.1 Risks Pertaining to the Function(s) Outsourced

- Sensitivity of data accessed, protected, or controlled by the vendor
- Volume of transactions
- Criticality to LEAP's business operations

2.3.2 Risks Pertaining to the Vendor

- Strength of the vendors financial condition
- Ability to maintain business continuity
- Ability to provide accurate, relevant, and timely information systems and services
- Experience with the function(s) outsourced
- Reliance on subcontractors or subsequent third-party vendors to provide outsourced function(s)
- Location of vendor, especially if vendor is foreign based
- Redundancy and reliability of communication with key vendor assets and personnel

2.3.3 Risks Pertaining to the Technology Used by the Vendor

- Architecture
- Location (both Processing and Data Storage)
- Dependence on third-parties
- Reliability
- Security
- Scalability

2.4 Vendor Procurement

Vendor Procurement will follow the appropriate purchasing policies determined by the nature of services required.

2.5 Vendor Contracts

When contracts are required between LEAP and a vendor candidate, the contract will be developed in accordance with the appropriate contract approval procedures and purchasing policies.

All vendor contracts must be reviewed to ensure the following criteria are properly met:

2.5.1 Scope of Work/Services Provided

Ensure that the contract accurately reflects the full scope of services and/or products expected.

2.5.1 Ownership (Work Product, Intellectual Property, and Associated Data)

Ensure vendor terms around ownership are consistent with expectations for products and/or services to be provided and do not represent compliance risk.

2.5.2 Indemnification/Limitation of Liability

Ensure vendor terms do not conflict with negotiated and/or represented Guarantees and/or Warranties.

Section 3 – Enforcement

Non-compliance with this policy and/or its resulting procedures may be cause for disciplinary action up to and including termination. Depending on the circumstances, federal or state law may permit civil or criminal litigation and/or restitution, fines, and/or penalties for action that would violate this policy.

Section 4 – Responsibility

1. All agents operating on behalf of LEAP are responsible for following this policy.
2. Anyone observing what appears to be a breach of security, violation of this policy, violation of state or federal law, theft, damage, or any action that might place company resources at risk must immediately report the incident to an appropriate-level supervisor, manager, or the IT Security Team.