# Vendor Access Policy

## Overview

Vendors play an important role in the support of hardware, software, management, and operations for [LEP]. Setting appropriate limits and controls on what can be seen, copied, modified, and controlled by vendors reduces the risk of exposure, breach, liability, loss of trust, and embarrassment to [LEP].  
  
2. Purpose

This policy establishes vendor access procedures that address information resources and support services, vendor responsibilities, and protection of [LEP] information.

## Scope

This policy applies to all [LEP] staff who interact, utilize, or manage vendor contractors who used [LEP] information resources.

## Policy

### GENERAL

Vendors and contracted employees shall comply with all applicable [LEP] policies, procedures, and agreements including but not limited to policies in the following areas:

* Safety
* Privacy
* Security
* Auditing
* Software Licensing
* Acceptable Use

### **[Insert Appropriate Role] AND [LEP] RESPONSIBILITIES**

The [Insert Appropriate Role] shall implement and maintain a consolidated list of vendors with access to [LEP] information resources. This list, as well as vendor agreements and contracts, shall specify:

* Resources that the vendor accesses
* Security measures vendor will take to protect [LEP] data
* Acceptable methods for the return, destruction, or disposal of [LEP] information under vendor control at the end of the contract
* Vendor assurance that information collected and stored during the term of the contract shall only be used for the purposes of the business/contract agreement
* Information acquired by the vendor during the course of contract execution cannot be used for any other purposes other than those specified in the contract and shall not be divulged to others
* [Insert Appropriate Role] shall post and maintain on its website a list of the School Service Contract Providers that [LEP] contracts with and a copy of each contract

C. VENDOR RESPONSIBILITIES [LEP] shall provide a point of contact for the vendor as part of its normal operating procedure. The point of contact will work with the vendor to make certain they are in compliance with [LEP] policies. Vendors shall comply with the following procedures as part of their [LEP] working relationship:

* **Contractor Lists** - Each vendor must provide a list of all staff working on the contract. The list must be updated and provided to [LEP] as staff changes on a monthly basis.
* **ID and Security Clearances** - Vendors shall acquire [LEP] security badges/key cards that shall be displayed at all times while on [LEP] premises. The badge shall be returned promptly when the contract employee leaves the [LEP].
* **Security Clearances** - Contractors with access to [LEP] Confidential Information or Personally Identifiable Information (PII) must be cleared to handle that information.
* **Incident Reporting** – Contractors shall report all security incidents directly to the [Insert Appropriate Role] or designee. If vendor management is involved in a security incident or breach, the responsibilities details, and possible penalties must be specified in the contract.
* **Change Management** - Vendor personnel must follow all applicable [LEP] change control processes and procedures.
* **Remote Access** – Remote vendor access must be uniquely identifiable and password management must comply with [LEP] password standards. [LEP] reserves the right to determine applicable virtual private network and encryption technologies used to access their systems and network.
* **Contractor Termination** - Upon departure of a contractor from [LEP] for any reason, the vendor shall ensure that all sensitive information is collected and returned to [LEP] or destroyed within a timeframe determined in the original contract terms.
* **Keycard and Security Access** - Upon termination of contract or at the request of [LEP], the vendor shall surrender all identification badges, access cards, equipment and supplies owned by the [LEP] immediately. Equipment and/or supplies retained by the vendor must be documented by authorized by the [Insert Appropriate Role] or their designee.
* **Auditing and Compliance** - Vendors are required to comply with all [LEP] auditing requirements. All software used by the vendor in providing service to [LEP] must be properly inventoried and licensed.
* **Disclosure of Sub-Contractors** - Third party agreements that directly, or indirectly, impact [LEP] information resources are required to include explicit coverage of all relevant security requirements. This includes agreements involving processing, accessing, communicating, hosting or managing the organization's information assets or adding or terminating services or products to existing information. Asset agreements provisions shall include security and integrity controls for data exchanged to prevent improper disclosure, alteration, or destruction.

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the [LEP] internal procedures. Controls are provided in detailed policies around individual component processes.

## Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

## Distribution

This policy is to be distributed to all [LEP] staff responsible for vendor contractor management.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 10/16/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |