LTSD Vendor Access Procedure

1.0 Overview

The purpose of this policy is to define procedures for allowing vendors access to Information Technology (IT) resources, such as data servers, network systems, or computer systems within the LTSD network domain. As a general principle, this access will only be granted as required,will be extremely restrictive, and will be monitored carefully. This procedure applies to all vendors, including intermediate units, performing network and server management, including but not limited to computers, servers, routers, hubs, firewalls, switches, and the interconnecting cables.

2.0 Purpose

This procedure is designed to ensure data integrity on all district owned servers from vendors with whom the district has contracted to provide a service involving IT resources. This will include hardware, software, and network vendors.

3.0 Scope

Vendors must comply with all applicable LTSD procedures, including, but not limited to:

- *District approved Acceptable Use Policy*
- Security Policies
- Privacy Policies

Any vendor access granted to IT resources will be provided the least security privilege required to accomplish a task. Generally, a vendor will not be given system administrator privileges or their equivalent.

Vendor access to IT resources will be granted for a defined and short duration, usually the length of time required to address a specific support incident. This duration will initially be set at 2 hours unless specified. On completion of the task, access will be disabled. Vendors requiring regular access must provide a security PIN, to ensure identity, prior to the granting of network access. The PIN will be provided to the vendor or vendor's agent.

If vendor is given access to an account that is shared among IT staff, the password for the account may be changed after the vendor completes the work depending on Scope and length of access.

Prior to granting vendor access for software installations and/or upgrades, the process will be reviewed by the appropriate IT system administrator. After a vendor has installed or upgraded a product, the responsible IT system administrator will review the system to ensure that it is functioning properly.

To the extent possible, the activities of a vendor will be monitored by IT personnel.

4.0 Responsibility

Violations of any provisions of this policy will be dealt with in the same manner as violations of other district policies. This can include:

- Permanent loss of computer user privileges;
- Denial of future access to IT resources;
- Disciplinary action in accordance with the appropriate procedures; and/or
- Legal action.

Some violations of this policy also may constitute a state, local, or federal criminal offense.