

Office of Information Technology Policy

Security: Data in Transit

Policy:

All sensitive data that are removed from the state premises must be encrypted consistent with IT STD 1-13 *Encryption*. This includes both data on agency approved portable storage devices (notebook PCs, USB drives, mini/micro solid state disks, CDs, DVDs, diskettes, PDAs, tapes etc.) and data being transferred through network protocols (ssh, https, sftp, etc).

Sensitive data includes: sensitive, proprietary and other data not subject to the Louisiana Public Records Act (LA. RS 44:1 et seq.).

Scope:

All entities under the authority of the Office of Information Technology, pursuant to the provisions of R.S. 39:15.1, et seq., must comply with this policy.

Responsibilities:

- Agencies must document a business case to support employees or contractors taking sensitive data off state premises.
- Agencies must make reasonable assurances that only agency approved storage devices will be used if employees or contractors are allowed to take sensitive data off state premises.
- Agencies must make reasonable assurances that employees subject to this policy are aware of the proper techniques regarding use of encryption on the devices and protocols referenced above.
- Agencies must make reasonable assurances that contractors utilize encryption consistent with IT STD 1-13 when taking sensitive data off state premises.
- Agencies must provide OIT with an electronic copy of their deployment plan relative to becoming compliant with this policy.

Related Policies, Standards, Guidelines:

IT STD 1-13 *Encryption*

Owner:

OIT Security Office

Effective Date:

July 27, 2009