External Data hosting Standard Statement

Purpose:

Externally hosted data needs to be protected according to the sensitivity of the information that is transmitted and stored. There are specific controls that are required by law (or required under other circumstances) that must be met to a high degree of certainty in order to consider that the data is properly protected.

Policy:

To require the review of the data classification and protections needed for any data that may be "hosted" at a site that is not fully and directly controlled by the State of Nebraska. To identify potential risks to that information so that the Agency can properly evaluate the risk of the potential hosting of that data. To acknowledge the residual "hosting" risk by formally submitting a classification/risk acceptance evaluation.

Exclusions to this policy:

All data that is considered public information.
All data that is hosted by a State entity and under direct State control.
All data that is hosted with a Federal government entity.

Procedure:

Identify what data elements will be involved with the potential hosting arrangement
Classify the data involved
Determine how the data will be utilized and transmitted during the hosting life-cycle
Review of Standards needed to conform to data protection requirements
Review best practices on the protection of the data
Review the contract language for appropriate data protection language requirements
Identify the residual risk to the data
Submit an evaluation of the risk to the hosted data with acknowledgement of the residual risk

External Data Hosting Guidelines

Best-Practices:

NIST Standards
Data Classification Toolkit: Link
Cloud Security Alliance Matrix/Info: Link
Confidential Data Handling Blueprint: Link

Policy requirements:

8-102 Data Security Standard - Requirement to classify data and to designate a data owner.
Identify risk to information based on classification and use.
Document and acknowledge risk acceptance.

Recommended controls:

SAS70 (T1 or T2)/SSAE16
ISO 27000 Series
FISMA: Link
HIPAA: Link

Related NITC policy requirements:

8-101 Information Security Policy
- Page 7 sharing non-public data

8-201 Information Technology Disaster Recovery Plan Standard
- Business Impact Analysis required, Resumption plans required
- BIA requires Identifying risk and classifying data

8-301 Password Standard
- State systems are required to follow – is it a State system?

8-302 Identity and Access Management Standard for State Government Agencies
- All new web apps that utilize logins need to conform.

8-303 Remote Access Standard
- Agency is required to ensure secure remote access

Resource Document:
8-RD-01 Security Officer Instruction Guide [Word Version]
- Chapter 3 – Business Impact Analysis walk-through

Nebraska Statutes:
87-801 Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006

RFP issues to be addressed:

Application security, remediation requirements and audits
Data Protection contractual language
Breach/Incident notification circumstances and requirements
Indemnification language
Use of data
Investigative issues
Termination of contract
After contract issues