

**Technical Panel
of the
Nebraska Information Technology Commission**

Standards and Guidelines

**Draft Document
30-Day Comment Period**

NITC 3-101 (Cloud Computing Standard)

Notes:

1. The following document is a draft document under review by the Technical Panel of the Nebraska Information Technology Commission (“NITC”).
2. If you have comments on this document, you may submit them by email to rick.becker@nebraska.gov, or call 402-471-7984 for more information on submitting comments.
3. The comment period for this document ends on July 25, 2016.
4. The Technical Panel will consider this document and any comments received at a public meeting following the comment period, currently scheduled for August 9, 2016. Information about this meeting will be posted on the NITC website at http://nitc.nebraska.gov/technical_panel/meetings/index.html.

**State of Nebraska
Nebraska Information Technology Commission
Standards and Guidelines**

NITC 3-101 (Cloud Computing Standard)

A PROPOSED NEW STANDARD relating to cloud computing:

1. STANDARD

The Office of the Chief Information Officer (“OCIO”) delivers IT solutions in a standards-based, technologically sound and secure environment. In alignment with the State’s strategic direction for IT and to leverage the State’s substantial investment in private cloud computing services, state agencies needing cloud computing services shall use the private cloud computing services provided by the OCIO (“State Cloud”) unless an exception is granted as provided herein.

If the State Cloud does not fully address an agency’s business needs and the agency is considering a vendor provided cloud computing alternative, the agency shall submit a *Cloud Computing – Statement of Intent* (form attached hereto as “Attachment A”) to the OCIO that outlines the requirements, costs and risks prior to proceeding with the initiative.

The agency’s *Cloud Computing - Statement of Intent* shall be submitted to the OCIO during the planning/requirements gathering process of any project potentially utilizing a vendor provided cloud computing solution. Upon receiving the *Cloud Computing – Statement of Intent*, the OCIO will schedule a meeting with the agency to discuss the request.

After reviewing the request, the OCIO may approve the exception; approve the exception with conditions; or deny the exception.

All purchase requests for cloud services shall be submitted using the IT procurement review process as outlined in NITC 1-204.

2. INQUIRIES AND SUBMISSION

Direct inquiries and the submission of the *Cloud Computing – Statement of Intent* to:
OCIO.ITPurchase@nebraska.gov

3. DEFINITIONS

This document uses the National Institute of Standards and Technology (NIST) definition of cloud computing and corresponding service models:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Service Models:

- **Cloud Software as a Service (SaaS).** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- **Cloud Platform as a Service (PaaS).** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
- **Cloud Infrastructure as a Service (IaaS).** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

4. REQUIREMENTS AND CONSIDERATIONS

Requirements and considerations in this section are presented in summary form to illustrate key functional, technical and operational differences between each cloud offering and are meant to be representative as opposed to complete.

Legend: ✓ Preferred Solution, △ Subject to Review, ⊘ Not Acceptable

| Requirement Area | Key Considerations | State Cloud | Hybrid Offering | Public Cloud |
|---|---|-------------|-----------------|--------------|
| <i>Infrastructure Suitability</i> | | | | |
| Security and Privacy | <ul style="list-style-type: none"> Maintenance of Highly Restricted, Confidential, Managed Access Public and Public data (NITC 8-101) Resiliency to unauthorized access via unique encryption keys Data will never be co-mingled with that of other organizations. | ✓ | △ | ⊘ |
| Technical Performance | <ul style="list-style-type: none"> High CPU, Memory, Bandwidth or I/O Requirements Predictable workloads | ✓ | ✓ | △ |
| Availability & Service Levels | <ul style="list-style-type: none"> 24x365 availability, 99.95%+ uptime Fault tolerance, redundancy | ✓ | △ | ⊘ |
| Customization | <ul style="list-style-type: none"> Standards enforcement (OS, DBMS, Security, System Image) Tailored to Application / Agency technical requirements within standards | ✓ | △ | ⊘ |
| Cost Savings Impact Areas | <ul style="list-style-type: none"> Operational Cost of Ownership Ongoing TCO reduction, Cost avoidance | ✓ | ✓ | ✓ |
| Driver of Statewide Consolidation | <ul style="list-style-type: none"> Reduction in systems, software and application counts, operational complexity Simplification of integration, workflows and labor requirements | ✓ | ✓ | ✓ |
| Migration Profile | <ul style="list-style-type: none"> Ease of migration from current solution platform to cloud based offering Technical migration complexity profile | △ | △ | △ |
| Integration (Process & Technical) | <ul style="list-style-type: none"> Cross system workflow support and data exchange Mixture of sensitive and non-sensitive data Adherence to State integration standards | ✓ | △ | ⊘ |
| <i>IT Application Profile Suitability</i> | | | | |
| Websites and Public Interaction (Informational) | <ul style="list-style-type: none"> Presentation of State / Agency presence to public / businesses Distribution of non-sensitive data | ✓ | ✓ | ✓ |
| Transactional Websites | <ul style="list-style-type: none"> Collection of non-sensitive transactional data Collection of low-risk fees/revenue or other information | ✓ | ✓ | △ |
| Workgroup Enablement | <ul style="list-style-type: none"> Storage of routine forms, data, knowledge management and other workgroup enablement data / functions | ✓ | ✓ | ✓ |
| Business Process Enablement | <ul style="list-style-type: none"> Integrated processes within a single application or application suite Processing of transactional data non-critical to the State or public safety, revenue collection | ✓ | △ | △ |
| End User Computing | <ul style="list-style-type: none"> Agency specific and non-critical applications Simple integration and reporting Routine Agency functions (non-sensitive data) | ✓ | ✓ | ✓ |

| | | | | |
|---------------------------------------|--|---|---|---|
| Cross-Agency Systems | <ul style="list-style-type: none"> ▪ Agency specific critical applications ▪ Complex integration and reporting ▪ Routine Agency functions (sensitive data) | ✓ | ⊘ | ⊘ |
| DR – Non Critical Systems / Data | <ul style="list-style-type: none"> ▪ Data replication of non-sensitive systems and data ▪ Archive and reference data management | ✓ | ✓ | ⚠ |
| State ERP (E1) | <ul style="list-style-type: none"> ▪ Operational Uptime and Performance ▪ Highly complex business rules and integration ▪ Maintenance of Sensitive Data | ✓ | ⊘ | ⊘ |
| Highly Integrated Operational Systems | <ul style="list-style-type: none"> ▪ Complex integration and workflows, potentially spanning many systems and work groups ▪ High operational uptime and performance requirements ▪ Maintain personal or confidential data | ✓ | ⊘ | ⊘ |
| State Critical Systems | <ul style="list-style-type: none"> ▪ Systems that directly influence the State’s ability to perform Public Safety, Citizen Services, Revenue Collection and/or Critical Employee Services | ✓ | ⊘ | ⊘ |

Attachment A - Cloud Computing Guidelines – Statement of Intent Submission Form

| | | |
|-------------------------|---------------------------|------------------------------------|
| Date of Request: | Requesting Agency: | Contact Person & Title: |
| | | |

| | | |
|----------------------|-----------------|------------------------|
| Phone Number: | Address: | E-mail Address: |
| | | |



Business rationale for selecting an alternative cloud computing solution (*Provide **specific business and / or technical reason(s)** why the agency/functional unit cannot use an existing State Cloud solution.*):

Proposed cloud computing service model (*e.g., Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS)*):

Deployment strategy (*e.g., hybrid, private or public cloud*):

Description of the maturity of the technologies involved (*Has successfully implemented in other government environment. If NE is the first customer for this technology, it is not mature*):

Estimated agency startup and ongoing maintenance costs of the proposed solution:

If a particular vendor is already under consideration, financial ability to perform the contract *(Can provide documentation showing other customers of same size using solution. Can provide documentation showing they have passed required federal audits):*

| |
|--|
| |
|--|

Exit strategy/plan in the event that the agency is not satisfied with the cloud-based solution or the vendor is not able to provide the service:

| |
|--|
| |
|--|

Identification of the type of data that will be included in the proposed solution, including any sensitive data or personally identifiable information (Refer to <http://nitc.ne.gov/standards/8-101.html> for guidance on data types.):

| |
|--|
| |
|--|

Detail where and how state data will be stored, accessed, tested, maintained or backed-up:

| |
|--|
| |
|--|

Description of the agency's security policies and, if known, vendor security practices that are in place or will be implemented to safeguard the State of Nebraska's information assets from unauthorized disclosure, modification or destruction and to address the basic security elements of confidentiality, integrity and availability:

| |
|--|
| |
|--|

Identification of the proposed business continuity and disaster recovery plan that will be used to ensure the timely restoration, relocation or replacement of resources in the case of a disaster or other business interruption:

Explanation of incident response procedures in the event of a security breach, including the loss or theft of devices and media:

Approach to handling record retention, public record and e-discovery requirements in the proposed cloud computing solution:

Agency plans for providing help desk support for the proposed cloud-based solution:

| |
|---|
| High-level planning, design, development, implementation and maintenance timeline for the effort: |
| |

Requesting Agency Approval

| | |
|-------------------------------------|-------|
| Agency Director Approval Signature: | |
| | Date: |

For OCIO Management Use Only

| |
|---|
| State Chief Information Officer (or his/her designee) Approval: |
| Approve <input type="checkbox"/> Approve with Conditions <input type="checkbox"/> Disapprove <input type="checkbox"/> |
| Conditions or Reason for Disapproval: |

| |
|--|
| State Chief Information Officer (or his/her designee) Signature: |
| Date: |

Please submit the completed form to: **OCIO.ITPurchase@nebraska.gov**