**Instructions:** State Agencies requesting a Standards Exception should complete this form and submit it to NCDIT for approval through the NC eProcurement Sourcing Tool for active IT solicitations and through the NC eProcurement Contracts Tool for active IT contract amendments or renewals. If this Standards Exception Request is not related to an active IT procurement in the Sourcing Tool or an active IT contract amendment or renewal in the Contracts Tool, State Agencies may email the completed form and supporting documentation to dit.exceptions@nc.gov. NCDIT will enter the request into the Sourcing Tool on the State Agency’s behalf**.** More detailed information about the Standards Exception Request process can be found at the end of this Form.

|  |
| --- |
| **Summary** |
| Description: | Click or tap here to enter text. |
| Standards Exception Category: | [ ]  Hosting[ ]  Other: Click or tap here to enter text. |
| Hosting Location: | [ ]  Vendor[ ]  Agency[ ]  Other: Click or tap here to enter text. |
| Is this an IT Project? | [ ]  Yes [ ]  No |
| If an IT Project, enter IT Project Name as it exactly appears in Touchdown | Click of tap here to enter IT Project name as it exactly appears in Touchdown (if applicable and known). |
| Estimated Cost: | $Click or tap here to enter text. |
| Privacy Threshold Analysis (PTA) Number: | Click or tap here to enter text. |
| **Attachments** |
| Attachment Type:  | [ ]  Click or tap here to enter text.[ ]  Click or tap here to enter text.[ ]  Click or tap here to enter text.[ ]  Click or tap here to enter text. |

|  |
| --- |
| **Business Case** |
| Please provide context for your request by summarizing your related business need.  |
| Click or tap here to enter text. |

[ ]  Check Here is Business Case is Attached

|  |  |
| --- | --- |
| **Exception Category** | **Hosting** |
| Authority: | [NCGS § 143B-1365; Session Law 2016-94, Section 7.9(b)](http://www.ncleg.net/EnactedLegislation/Statutes/PDF/BySection/Chapter_143B/GS_143B-1365.pdf)  |
| Condition: | [ ]  Using an outside contractor would be more cost effective for the State.[ ]  The Department [NCDIT] does not have the technical capabilities required to host the application. [ ]  Valid security requirements preclude the use of the State infrastructure, and a vendor can provide a more secure environment. [ ]  The application is natively or commercially sold and delivered as a cloud-based solution.  |
| **Justification** |
| Our agency has reviewed the applicable authority, identified 1 and only 1 condition applicable to our agency, and demonstrates the following in support of this request.  |
| Click or tap here to enter text. |

[ ]  Check Here is Justification is Attached

|  |  |  |
| --- | --- | --- |
| **Exception Category** | **Other:**  | Click or tap here to enter text. |
| Authority: | Click or tap here to enter text. |
| **Justification** |
| Our agency has reviewed the applicable authority and demonstrates the following in support of this request.  |
| Click or tap here to enter text. |

[ ]  Check Here is Justification is Attached

Listed below is more information around the Standards Exception Request process.

|  |
| --- |
| **Instructions** |
| Form Submission Information * The Standards Exception Request Form B and any supporting documentation should be submitted through the NC eProcurement Sourcing Tool to NCDIT for active IT solicitations and through the NC eProcurement Contracts Tool for active IT contract amendments or renewals. The Sourcing Tool or Contracts Tool will first route the Standards Exception Request Form to the State Agency’s IT Security Liaison for approval. Once the State Agency’s IT Security Liaison has approved the Request in the Sourcing Tool or Contracts Tool, the Request will automatically route the Standards Exception Request Form to NCDIT.
* For Standards Exception Requests that are not associated with an active IT procurement in the Sourcing Tool or an active IT contract amendment or renewal in the Contracts Tool, State Agencies may email the completed Standards Exception Request form and supporting documentation to dit.exceptions@nc.gov. NCDIT will enter the Standards Exception Request into the Sourcing Tool on the State Agency’s behalf for processing.
* State agencies that wish to use the Sourcing Tool to submit a Standards Exception Request that is not associated with an active IT procurement in the Sourcing Tool or an active IT contract amendment or renewal in the Contracts Tool can follow the steps below:
1. Agency user that wants to submit a Standards Exception Request downloads the latest Standards Request Form from the [NCDIT Exceptions website](https://it.nc.gov/documents/exception-resources).
2. Agency user completes the Standards Exception Request Form and provides the completed form and any required supporting documentation to Agency Procurement.
3. Agency Procurement creates a Sourcing Project (not a Sourcing Request) in the Sourcing Tool, and selects Solicitation Vehicle to be IT: Exception Request Only.
4. Agency Procurement attaches the completed Standards Exception Request Form and supporting documentation to the applicable approval task in the Sourcing Project and submits it to NCDIT for approval (it will be sent first to Agency IT Security Liaison for their approval).
5. NCDIT Reviewers review and provide approval decision to submitted Standards Exception Request in Sourcing Tool.
* If State Agencies require any assistance in using the Sourcing Tool or Contracts Tool to submit a Standards Exception Request to NCDIT, they can contact the NC eProcurement Help Desk at 888-211-7440, option 1 or send email to ephelpdesk@its.nc.gov.
* The State Chief Information Officer (SCIO) has statutory authority in planning and managing a framework that collaboratively develops and publishes, information technology standards that guide architecture, design, engineering, procurement, and operational activities.

Hosting * NCGS § 143B-1365[[1]](#footnote-1) requires State agencies to use the State infrastructure to host their projects, services, data, and applications pursuant to current guiding authorities/laws.
* Agencies seeking an exception must demonstrate justification in one of the following areas:
* Using an outside contractor would be more cost-effective for the State.
* The Department does not have the technical capabilities required to host the application.
* Valid security requirements preclude the use of the State infrastructure, and a vendor can provide a more secure environment.

NCID* The State Chief Information Officer (SCIO) strives to simplify electronic transactions with North Carolina State Government. The SCIO is required to ensure this happens in a secure manner. This is accomplished through authentication of users and controlled access to applications and services.
* To achieve this, the SCIO requires all inter-agency and external facing solutions/applications that create content use the State’s Identity and Access Management solution (“NCID”).
* More information on the NCID service can be found at: https://it.nc.gov/ncid/ and <https://it.nc.gov/services/nc-identity-management-ncid>.
* NCID is used to integrate with numerous systems to synergize the end-user experience by providing authentication/authorization to State applications and solutions. All solutions requiring NCID authentication must externalize identity and access management and support the following protocols:
	+ Security Assertion Markup Language (SAMLv2)
	+ Lightweight Directory Access Protocol (LDAP)
	+ WebServices(SOAP/WSDL)
* As existing solutions are upgraded or replaced, they will be required to support the above protocols.
* A formal exception is required to use a solution other than NCID. The agency must provide just cause for the exception to be approved.

Guidelines For Writing Your Business CaseThe following guidelines may be helpful when writing your business case. * Regulatory Authority:
	+ Is there state, Federal, or other regulations driving your business need?
	+ What alternatives were explored to attempt compliance?
* Costs:
	+ Attach list of services, equipment, or items to be purchased.
* Risks:
	+ Describe associate risks, risk that may be introduced, why the risk is tolerable.
	+ Describe interfaces and technical environment that will exist with the exception.
	+ How will risk management be evaluated?
* Data Classification:
	+ Use the Privacy Threshold Analysis form to describe the types of data (e.g., PII, HIPAA, FERPA) being managed, processed, how stored, or transmitted, directly and indirectly, involved and where hosted.
* Impact:
	+ What users and customers are impacted by this exception?
	+ What are the implications if this exception is not approved?
* Compensating Controls:
	+ What controls will be put in place to mitigate risk to acceptable levels, when?
	+ Identify security methodology to manage data and access to include logical security via application, system, database, or other means, as well as physical security of hardware and other related infrastructure.
	+ Exceptions that create significant risks without compensating controls will not be approved or acknowledged without requiring further agency action.
* Mitigation:
	+ Mitigation must equal or exceed those of the exception.
	+ Address both initial and ongoing implementation. Include information on hardware, software, infrastructure, training and procedural documentation, administrative and support personnel, consultants and vendors, disaster recovery, back-up, business continuity, and monitoring.
* Exception Strategy:
	+ Detail how the above controls will be maintained and reviewed by your agency.
	+ List responsible parties for maintenance and review.
	+ Outline the agency timeframe for coming into compliance.
* Describe any additional information relevant to understanding this exception.
 |

1. *NCGS § 143B-1365. Data Centers.*

*(a) The State CIO shall create an inventory of data center operations in the executive branch and shall develop and implement a detailed, written plan for consolidation of agency data centers in the most efficient manner possible. By May 1, 2016, the State CIO shall present a report on the data center consolidation plan to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division. (b) State agencies shall use the State infrastructure to host their projects, services, data, and applications. The State Chief Information Officer may grant an exception if the State agency can demonstrate any of the following: (1) Using an outside contractor would be more cost- effective for the State. (2) The Department does not have the technical capabilities required to host the application. (3) Valid security requirements preclude the use of State infrastructure, and a vendor can provide a more secure environment. (2015-241,s.7A.2(b).)*  [↑](#footnote-ref-1)