**Instructions:** State Agencies requesting a Security 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 Security 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 this 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 Security Exception Request process can be found at the end of this Form.

|  |
| --- |
| **Basic Information** |
| Request Title: | Click or tap here to enter text. |
| Date: | Click or tap here to enter text. |
| Agency: | Click or tap here to enter text. |
| Division: | Click or tap here to enter text. |
| **Contacts** |
|  | Name | Email Address |
| Business Owner: | Click or tap here to enter text. | Click or tap here to enter text. |
| CISO/Security: | Click or tap here to enter text. | Click or tap here to enter text. |
| Project Manager: | Click or tap here to enter text. | Click or tap here to enter text. |
| Director: | Click or tap here to enter text. | Click or tap here to enter text. |
| Agency CIO: | Click or tap here to enter text.  | Click or tap here to enter text. |
| **Summary** |
| 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). |
| Privacy Threshold Analysis (PTA) Number: | Click or tap here to enter text. |
| **Reason for Request** |
| Reason: | [ ]  Patch Management – (SI-2: Flaw Remediation)[ ]  Software – (SA-3: System Development Life Cycle / SA-8: Security Engineering Principles)[ ]  Hardware – (SA-3: System Development Life Cycle / SA-8: Security Engineering Principles)[ ]  Password – (IA-5: Authenticator Management)[ ]  Service/Group Account – (AC-2: Account Management)[ ]  Other: Click or tap here to enter text. |
| **Attachments** |
| Attachment Type:  | [ ]  Click or tap here to enter text.[ ]  Click or tap here to enter text. |

|  |
| --- |
| **Business Case** |
| Please explain why the waiver is needed (details of the deficiency). Please include the following if applicable: Operation System Details, Version Information, and/or Length of Waiver Requested.  |
| Click or tap here to enter text. |

[ ]  Check Here is Business Case is Attached

|  |
| --- |
| **Mitigation Approach** |
| Please explain how you are mitigating the risk. Please include the following items, if applicable:* Network Controls (e.g., vlans, non-routable IPs)
* Other access control measures in place
* Current compliance state (e.g., based on recent scan)
* System Hardening
* Monitoring ability (how do you ensure the controls in place remain unchanged)
 |
| Click or tap here to enter text.  |

[ ]  Check Here is Mitigation Approach is Attached

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

|  |
| --- |
| **Information** |
| Form Submission Instructions * The Security Exception Request Form C and any supporting documentation should be submitted to NCDIT through the NC eProcurement Sourcing Tool 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 Security 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 Security Exception Request Form to NCDIT.
* For Security 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 Security Exception Request form and supporting documentation to dit.exceptions@nc.gov. NCDIT will enter the Security 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 Security 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:
* Agency user that wants to submit a Security Exception Request downloads the latest Security Exception Request Form from the [NCDIT Exceptions website](https://it.nc.gov/documents/exception-resources).
* Agency user completes the Security Exception Request Form and provides the completed form and any required supporting documentation to Agency Procurement.
* Agency Procurement creates a Sourcing Project (not a Sourcing Request) in the Sourcing Tool, and selects Solicitation Vehicle to be IT: Exception Request Only.
* Agency Procurement attaches the completed Security 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).
* NCDIT Reviewers review and provide approval decision to submitted Security Exception Request in Sourcing Tool.
* Agencies should review and ensure that all required security policies are in place to protect sensitive data; refer to the Statewide Information Security Manual.
* Pursuant to NCGS § 143B-1377, agencies must complete the necessary security, risk, and/or data classification assessment for each request. Agencies should use the Privacy Threshold Analysis form to assist with this effort.
* Your agency may have a procurement for a business solution that includes services handling sensitive or confidential data (e.g., PII, HIPAA, FERPA). Use the Privacy Threshold Analysis (PTA)form to assess the types of data and potential risks involved. PTAs are not required for Security Exception Requests (Form C).
* The agency Chief Information Security Officer (CISO) or their designee should include a statement of review and/or compliance consistent with agency and state standards with each exception submitted.
* **Information Security Incidents** (e.g., intrusion, hacking, information disclosure, denial of service, exploitation, cyber-attack) are not exceptions and should be reported at: <https://it.nc.gov/cybersecurity-situation-report>.

Privacy Threshold Analysis (PTA) * The Privacy Threshold Analysis form is available to assist agencies in assessing system and application privacy implications.

Industry Certification Report * In some cases, pursuant to NCGS § 143B-1378, agencies will need to provide an industry certification report and in particular, for cloud-based hosting or application solutions.
* Agencies will need to contact their vendor, obtain, and provide a copy of its most recent third party audit. Examples include SOC 2 Type 2, SSAE 18, ISO 27001, or FedRAMP certification reports.

Questions* If State Agencies require any assistance in using the Sourcing Tool or Contracts Tool to submit a Security 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.
* For all other questions, State Agencies can email the NCDIT Enterprise Security and Risk Management Office (ESRMO) at security@its.nc.gov.
 |