Exception Request Job Aid

Table of Contents

1. Purpose .................................................................................................................................................. 2
2. Exception Request Creation .................................................................................................................. 2
3. Workflow Process .................................................................................................................................. 4
1. Purpose

IOT has implemented an automated workflow process in Archer to help facilitate better review of exception requests. Users that are in an Archer Compliance or Archer Security Team group will be able submit requests on behalf of their agency. Each agency will only be able to see their own requests, but all IOT Archer users will be able to see everyone’s.

2. Exception Request Creation

Once logged into Archer (https://grc.iot.in.gov/RSAArcher), click on the down arrow next to the “Regulatory and Corporate Compliance” heading. In the center column there will be a Quick Link for “New Policy Exception Request”.

This will bring up a new record that is very similar the previous IOT Exception Form.
A few new fields have been added to help facilitate the workflow and add additional information.

Submitted By and Agency Approver
The Submitted By field will always auto-populate with the current user. The user will need to manually select an individual from their agency. Unfortunately there is not a way to filter this list based upon the user’s agency. The IOT Security Team can provide the names for a specific agency if needed.

Expiration Date
This field will automatically be set to 6 months from the current date. Exceptions are valid for a maximum of 1 year.

Technical Contacts
These will be any individuals directly responsible for implementing the exception or have in depth knowledge of why it is required. All State employees will be available for selection. Use the “Lookup” link on the right side of the field.

Subject
Please select a short phrase that will help identify the exception.

**EXCEPTION DECLARATION**

Impacted Tier 1 Standards
This field is now required and is the standard that the exception would be violating. Clicking the ellipses at the end of the field will bring up a dialog box with all of the standards. If the standard ID is already known it can be filtered down or simply browse through the list to find the correct one.

Exception Request Attachments
Supporting documentation or any additional required forms can be attached to the record. Click “Add New” on the right side of the field to browse to the desired file. Please note that the file cannot be open otherwise Archer will not be able to upload it.
Once all of the required fields have been completed the record can be saved and will be entered into the workflow process.

3. Workflow Process

Once the record has been saved and entered into workflow it will be in Draft mode. From here the submitter can make any changes or come back to it at a later date before submitting it for review. When ready click on the “Submit for Review” button to move the workflow forward.

EXC-27 Exception Requests

NEW   COPY   SAVE   VIEW   DELETE

Submit For Review

Exception Declaration

About

Your request is currently saved in Draft mode. Once you are

From here it will go to the Agency Authorizer for approval. They will get an email indicating a new record requires their review. The Authorizer will have two options at this point, either “Return to Submitter” or “Approved” and will be required to put in comments regardless of which option they choose. They will also have the ability to make any changes they see fit to the record.

EXC-27 Exception Requests

NEW   COPY   SAVE   VIEW

Return To Submitter   Approved

After the Agency Authorizer has approved the exception the record will move on to the IOT Policy Committee for review and the record will be set to Read-Only from here forward unless returned to the submitter. The Committee is able to return the record back to the submitter (which restarts the process and requires agency approval again), acknowledge the exception (which will allows it to be completed by the appropriate team), or escalate it to the Chief Information Officer. The CIO can then deny it or acknowledge it.

When a final decision has been made the submitter, agency approver, and IOT Risk and Compliance team will be emailed.
The Exception Requests can be viewed by browsing to “Exception Requests” under “Regulatory and Corporate Compliance” and then “Policy Management”.

The stage in the workflow process can be determined by the “Overall Status” of the record.

Exceptions cannot be extended and when they expire a new one will need to be created. The submitter will receive an email 30 days before expiration and another one 7 days before expiration.

If there are any questions, please contact IOTRiskCompliance@iot.IN.gov.