1. **Purpose**

Unauthorized software can introduce unmanaged, vulnerable software into the State environment, which can be used by attackers to exploit hosts and further compromise them. There can also be legal issues with the installation of unauthorized software, such as violations of licensing agreements. This standard provides the requirements for installing and maintaining software, to ensure a well-controlled desktop environment.

This job aid will walk through the steps required to complete an authorization and detail the workflow process that occurs after it is submitted.

2. **Software Portal**

1. Navigate to https://grc.iot.in.gov
   a. All Security Coordinators should have access at this time. However, there is not an automated way to add new coordinators. If you are a Security Coordinator and find that you do not have access, please open a ticket to get added to the Software Portal in Archer.
2. Begin by expanding the Navigation Menu. Next, click on “Regulatory and Corporate Compliance” then “Software Portal.”
3. The top of the Software Portal will display the text of the standard for those that may not be familiar with it. It will then be followed by the IOT Whitelist and Blacklist.
   a. Items on the whitelist do not require an authorization and can be requested by a security coordinator with only a helpdesk ticket.
   b. Items on the whitelist are patched and maintained by IOT.
   c. Items on the blacklist will not be installed on state machines.
      i. Reasons for blacklisting include, but not limited to: severe vulnerabilities, violation of license agreement, not appropriate for state machines (games, streaming, etc)

4. Next will be quick links to create a new authorization, link to report of the requests that the current user has created, and a link to a report of all the software that has been reviewed by IOT so far. To the right will be a report of all the requests for your agency.
   a. If an item has already been approved for your agency, another request is not needed unless it is for a different version. (ex. Version 7.9 has been approved, but you’re requesting version 9.0)

5. At the bottom of the portal will be a graph with all of the reviewed software broken out by category. This will enable the agency to select items that are already being used in the state rather than trying to research something new to meet their needs.
3. **Software Authorization Instructions**

1. Begin by clicking on the “New Software Authorization Request” link on the Quick Links section of the Software Portal.

2. Fill out the Agency, Software Owner, Alternate Owner, and Software Approval Group fields. The Submitter field will always default to the user creating the record and the Submit Date will always default to the current date.
   a. The Owner fields will allow the creator to search for other employees.
   b. Select your agency’s group in the Software Approval Group field. This field is used as part of the workflow process and all members of that group will receive an email notification that a new request has been submitted.

3. Next the requested software will be selected from the existing list or a new record will need to be created.

   a. If the software has already been reviewed by IOT Security for another agency click the “Lookup” link to select it from a list. After selecting the needed software, skip to **Step 11** in this guide.

   b. If this is software that has not yet been reviewed, click on the “Add New” link.
4. When adding new software complete the Application Name and Manufacturer, Version, Application Type, and Description fields.
   a. If the software does not have version numbers, please use “N/A”
   b. If there isn’t an appropriate application type, please select “Other” and type what it should be. IOT Security will periodically review the responses and add new types as needed.
   c. The description should be about what the software is used for and not how your agency will be using it. Please be as detailed as possible so that other agencies will be able to view it and determine if the software could work for them. IOT Security will deny requests for incomplete or lacking descriptions.

5. Next, complete the licensing information.
   a. If “Free” is selected, you will need to select whether it is a trial version and if the license agreement allows government use.
      i. Please review the license agreement carefully. Many manufacturers classify governments the same as enterprises and do not allow the use of free copies in those environments. This is one of the main reasons software requests get denied by IOT.

6. Please select if the software is capable of storing Personally Identifiable Information (PII).
   a. “Yes” should be selected if the software can store it even if your agency may not specifically be using that feature.
   b. If “Yes” is selected you will be required to select if the data is encrypted and the categories of data that could be stored.
7. Next, disclose if there are any known exploits with the software, if a security exception is required, and the vendor’s patching schedule.
   a. If “Yes” is selected for exploits or requires an exception, you will be required to enter additional information.

<table>
<thead>
<tr>
<th>SECURITY INFORMATION</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Are there any known vulnerabilities or exploits?</td>
<td>Yes</td>
<td>Exploits/Vulnerabilities:</td>
<td></td>
</tr>
<tr>
<td>Does this application require other security exceptions (e.g., older Java or browser versions)?</td>
<td>Yes</td>
<td>Reason that an Exception is Required:</td>
<td></td>
</tr>
<tr>
<td>What frequency is the software regularly patched/maintained by the vendor?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

8. The following section contains technical information regarding authentication to the software, how it is accessible, if it requires a separate database, and if there is a server component to it.
   a. If there is a server component there will be an additional question if it needs to be hosted in the Protected Zone (PZ).

<table>
<thead>
<tr>
<th>ADDITIONAL TECHNICAL INFORMATION</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Types</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is this application accessible from outside of the same network (e.g., over a VPN)?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does this application need to be installed on a server?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

9. Finally complete the compatibility fields (Operating System and Browser) and if there are additional instructions or documentation.

<table>
<thead>
<tr>
<th>COMPARABILITY</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Compatibility</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any dependencies on other software or other software?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Browser Compatibility</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

10. The final step is click “Save and Close”. This will take you back to the authorization form.
   a. Please review your responses carefully before saving. Once it is saved the record is locked and only the IOT Security Team can make changes.
      i. If changes do need to be made, email #IOT Security Team.

11. Once the software has been selected or a new record completed fill out the justification on why the software is needed and how it will be used by the agency.
   a. Justifications such as “needed for job” or other vague statements will not be accepted and the record will be returned to the submitter for editing.
   b. If the requested version is not the most recent available from the manufacturer IOT Security requires justification on why this specific version is required.

Add New Record Software

NEW COPY SAVE SAVE AND CLOSE VIEW DELETE

11. Once the software has been selected or a new record completed fill out the justification on why the software is needed and how it will be used by the agency.
   a. Justifications such as “needed for job” or other vague statements will not be accepted and the record will be returned to the submitter for editing.
   b. If the requested version is not the most recent available from the manufacturer IOT Security requires justification on why this specific version is required.

Please describe why this application is needed and how it will be used by your agency.

<table>
<thead>
<tr>
<th>Justification</th>
<th></th>
</tr>
</thead>
</table>

Is this the most current version offered at the time? | Yes | Justification for older software version: | |
12. Some applications have the option to enable automatic updates during the packaging process.
   a. If “Yes” is selected, IOT will not be responsible if the update breaks or otherwise affects the use of the application

<table>
<thead>
<tr>
<th>Enable Automatic Updates?</th>
<th>Yes</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>(IOT is not responsible for automatic software patches that “break” or otherwise hinder use of the software.)</em></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   b. If “No” or “Not Sure” is selected, the agency (Software Owners) is responsible for notifying IOT when a patch or upgrade is required. The agency will be accountable for any risk that unpatched or older software may introduce to the environment.

<table>
<thead>
<tr>
<th>Enable Automatic Updates?</th>
<th>No</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>(If automatic updates are not configured or not possible, the agency is responsible for notifying IOT when a patch or upgrade is required. The agency is accountable for any risk that unpatched or older software may introduce to their environment.)</em></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

13. Next is if the application will house any PII. The question on the previous form was if the software could potentially house any at all. This question, and the follow ups, is asking if your agency specifically will be using it for PII and how it will be used.
   a. If “Yes” is selected, please specify how your agency is using the data, the number of individuals affected, and the specific categories your agency will be using.

   | Will this software house any Personally Identifiable Information (e.g., name, address, SSN, etc.)? | Yes | Edit |
   | Number of Affected Individuals |  |  |
   | Categories of Affected Individuals |  |  |

14. If a security exception is required, only users that are members of the agency’s compliance team, security team, or agency authorizer will be able to link or create a policy exception. Linking to an exception is not required at this step, but an exception must be approved before IOT Security will approve the software.

15. Next is completing the licensing information for the software.
   a. If it is licensed and licenses do not need to be purchased, please either put in the license key or where it can be found.

<table>
<thead>
<tr>
<th>License Model</th>
<th>Licensed</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do licenses need to be purchased?</td>
<td>No</td>
<td>Edit</td>
</tr>
</tbody>
</table>

   b. If it is licensed and licenses need to be purchased, please put in how many will be needed.

   | Do licenses need to be purchased? | Yes | Edit |
   | Number of Licenses Needed |  |  |
16. Finally, fill out the installation information.
   a. The installation location should be a website address, CD/DVD, or a network path.
      i. The network path should be the full path with server name. IOT may not know what an agency’s S: or other drive is.
   b. The devices will be the initial list of PC and user names.
      i. If the software needs to be added to devices after the software has been approved only a helpdesk ticket will be required.

17. Once you are finished, click the “Save” button at the top left. This enrolls the record in the workflow and puts it in Draft mode so that you can come back to the record later if needed.

Add New Record  Software Authorization

18. When everything is ready to be reviewed by your agency approvers click the “Submit” button and it will progress through the workflow to the next stage.

4. Workflow Process

   1. Once the “Submit” button has been clicked a notification will go out to everyone in the Software Authorizers group.
      a. The individual that reviews the request will need to select their name and add any comments. If approved, simply typing “Approved” will be accepted.
b. Authorizers will have the option to Approve, Deny, or send the request back for changes.

1326706  Software Authorization

2. If the request is approved it will then go to the IOT Security Team for review.
   a. The IOT Security Team will have the option to Approve, Deny, or Return to Submitter.
   b. They will also have the option to send back to the authorizers if it is determined that a policy exception will be required.

3. Once the request is approved a notification will go out to the submitter, authorizer, and a vFire ticket will automatically be generated and assigned to the Software Distribution Team.