# Access Review – Segregation of Duties (SoD) Procedure for Asset Owners

**Purpose:**  Certify users with access to develop source code Do Not also have HPA access or access to deploy source code to the production application, database or operating system.

**Scope:**  All Critical, Sox, FISMA, Internet Facing applications

**Procedure:**

Provide SoD Evidence

Notification - You will receive an email from the Access Review Workflow.

You must attach several documents to the Access Review workflow. Collect the documents here and when you have them all complied, attach them to the workflow and submit.

In the last quarter, have any changes been made in your development or deployment process?

|  |  |
| --- | --- |
| **Changes to Development process**  (None **or** describe the change and provide the approval ticket number, and updated user lists ) | **Changes to Deployment process**  (None **or** describe the change and provide the approval ticket number, and updated user lists) |
| Response: | Response: |

**Provide evidence of all Changes introduced into production for your application during the past quarter**: (If possible a report or screen shot from ServiceNow with details of all changes)

|  |  |
| --- | --- |
| **Your Evidence** | **Sample Evidence Files** |
|  | OR  OR |

**Provide Name & SSO of users with Developer access. Include all with access to Source Code Developer tools**: (Screenshot of the Open GE list and confirmation that only specific users have access to development. Please provide the open GE project name and ID if applicable)

|  |  |
| --- | --- |
| **Your Evidence** | **Sample Evidence Files** |
|  | OR  OR  OR |

**Provide Name & SSO of all users with Deployment access. Include all with access to Source Code Deployer tools**: (Screenshot from the WebOPs portal showing Portal Project ID and a confirmation that only specific users have access to deployment of changes.)

|  |  |
| --- | --- |
| **Your Evidence** | **Sample Evidence Files** |
|  | OR PPM Extract |

**If you are performing an HPA access review for this quarter, you may have already submitted these files.**

**Provide a list of all production server Highly Privileged Account owners. Include anyone with elevated level of access to production servers.**  (Requires a list or a contact name with contact information.)

|  |  |
| --- | --- |
| **Your Evidence** | **Sample Evidence Files** |
|  | For most applications Anna McCord’s Team (Go IT) can provide the details. If possible, please provide an explicit list or team who handles it |

**Provide Name & SSO of all application System Administrators**: (Screenshot or written confirmation)

|  |  |
| --- | --- |
| **Your Evidence** | **Sample Evidence Files** |
|  |  |

**Provide a list of all Project Database Administrators. Include anyone with access to change master data. Identify each database**: (Requires a list or a contact name with contact information. )

|  |  |
| --- | --- |
| **Your Evidence** | **Sample Evidence Files** |
|  | For most applications Anna McCord’s Team (Go IT) can provide the details. If possible, please provide an explicit list or team who handles it |

**Provide a list of all Operation Database Administrators. Include anyone with complete edit database privileges. Identify each database**: (Requires a list or a contact name with contact information. )

|  |  |
| --- | --- |
| **Your Evidence** | **Sample Evidence Files** |
|  | For most applications Anna McCord’s Team (Go IT) can provide the details. If possible, please provide an explicit list or team who handles it |

Remediate Conflicts

**When the Access Review workflow is returned to you, a Conflict Report will be attached** identifying the Segregation of Duties conflicts identified for your asset – if any.

**Remediate all conflicts.**

If you are not able to remediate a conflict, submit an [Aviation IT Risk Acceptance and Security Exception](http://supportcentral.ge.com/ProcessMaps/form_new_request.asp?prod_id=63877&form_id=525743&node_id=1691113&map_id=&reference_id=&reference_type=) workflow request and mitigate if possible.

**Submit Access Review Workflow**

After addressing all conflicts, attach proof of remediation or Security Exception documentation and resubmit the Access Review Workflow.

## HPA Definitions

**Application HPAs**

**HPAs** have an elevated level of access:

* Can perform System-level administrative functions:
  + Can override application controls,
  + Can modify or promote code
  + Can change configurable parameters in production,
  + Can manage/monitor the application
* Account creation or management privileges or password management privileges.
* Account administration - can change master data

**Database HPAs**

**HPAs** have an elevated level of access:

* Can perform System-level administrative functions
* Can manage/monitor accounts/privileges/passwords
* Can alter schemas

**OS / Domain HPAs**

**HPAs** have an elevated level of access:

* Can perform System-level administrative functions
* Can create, modify, delete users
* Can modify permissions
* Can modify systems