# Texas Health and Human Services Commission

## First and Second Level IAM Approval Roles and Responsibilities

Version: 2.2 3/22/2010

<table>
<thead>
<tr>
<th>Project Manager</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>Masood Salami</td>
<td>Hal Crippen</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Approver</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Masood Salami</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations Manager</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Table of Contents

CHANGE LOG ................................................................................................................................. 3

INTRODUCTION ........................................................................................................................................ 4

SCOPE .............................................................................................................................................. 4

ENTERPRISE PORTAL ACCOUNT ........................................................................................................ 4
  REQUEST FOR Portal Account ........................................................................................................... 4
  DESIGNATED Organizational Role .................................................................................................... 5

OPERATIONAL RESPONSIBILITIES .................................................................................................... 5
  ACCOUNT Provisioning ......................................................................................................................... 5
  FIRST AND SECOND LEVEL Approver ............................................................................................... 5

MODIFICATION OF USER ACCOUNTS ............................................................................................. 5
  Application Accounts .......................................................................................................................... 5
  Personal Information .......................................................................................................................... 6

ACCOUNT LIFE CYCLE RULES ....................................................................................................... 6
  Rationale Behind the Rule ...................................................................................................................... 6
  STAGE 1 Event (Dormant Account Warning) ......................................................................................... 6
  STAGE 2 Event (Dormant Account Suspension) ................................................................................... 10
  STAGE 3 Event (Dormant Account De-Provisioning) ........................................................................ 10
  Manual Suspension ............................................................................................................................ 10
  Restoration of Suspended Accounts .................................................................................................. 10

SUSPENSION AND RESTORATION OF A PERSON ........................................................................ 10

EMPLOYEE TRANSFER .................................................................................................................... 11

DEPROVISIONING ............................................................................................................................ 11
  Process ............................................................................................................................................. 12
## Change Log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Description (list of changes, reason for change, &amp; editor’s name)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>9/18/2009</td>
<td>Hal Crippen</td>
<td>Initial draft version</td>
</tr>
</tbody>
</table>
| 0.1.1   | 9/22/2009  | Hal Crippen| Title Change  
Scope of document increased to include all approval authorities                                                              |
| 0.2     | 10/02/2009 | Hal Crippen| Incorporate reviewer comments                                                                                                    |
| 0.3     | 10/6/2009  | Hal Crippen| Incorporate reviewer comments                                                                                                    |
| 1.0     | 10/6/2009  | Hal Crippen| Published to User Guide                                                                                                         |
| 2.0     | 2/12/2010  | Hal Crippen| Incorporated new life cycle rules                                                                                               |
| 2.1     | 2/24/2010  | Hal Crippen| Incorporated new life cycle rules for employee transfer                                                                         |
| 2.1     | 3/22/2010  | Hal Crippen| Modified Inactive Accounts section IAW life cycle rules                                                                       |
First and Second Level IAM Approval Roles and Responsibilities

Introduction

HHS Organizations provide services to HHS clients. In the performance of service delivery the Organization frequently must interact with HHS Applications. To protect the sensitivity of the data involved in these interactions HHS has instituted the Identity and Access Management (IAM) System.

This document provides an overview of the roles and responsibilities of Supervisor and Application Security Administrator positions within the HHS Enterprise IAM System. The following summarizes the roles addressed by this document:

- Supervisor\(^{1}\) aka First Level Approval Authority
  - Access request by user through Portal.
  - User roles assigned and access approved by Supervisor.
  - Request forwarded\(^{2}\) to AA through workflow

- Application Administrator (AA) aka Application Security Administrator aka Second Level Approval Authority
  - Granting of final access approval.
  - In some applications, the AA may modify the User roles.

Scope

This document is limited in scope to those roles and responsibilities of Supervisors and Application Security Administrators performed within the IBM Tivoli Identity Management (ITIM) as part of the IAM. This document does not describe the operational use of the ITIM functions. Rather, the reader is referred to the Identity and Access Management User’s Guide. An online version of the Guide may be found at: [http://architecture.hhsc.state.tx.us/Portal%20Web%20User%20Guide/Home.html](http://architecture.hhsc.state.tx.us/Portal%20Web%20User%20Guide/Home.html)

Enterprise Portal Account

The Enterprise Portal serves as the primary conduit for access to Applications within the IAM system. All users of HHS Applications within the IAM system, regardless of employee type, must have an Enterprise Portal Account. That process is generalized in the following sections.

Request for Portal Account

The IAM System provides functionality to all users for self registration of an Enterprise Portal Account. The process followed which leads to self registration is included in the User’s Guide and can be found at: [http://architecture.hhsc.state.tx.us/Portal%20Web%20User%20Guide/PartnerRequestPortalAccess.html](http://architecture.hhsc.state.tx.us/Portal%20Web%20User%20Guide/PartnerRequestPortalAccess.html)

---

1 Supervisor is normally a member of the organizational chain of command with individuals reporting to them. In partner organizations this role may be filled by Administrative personnel outside of the chain of command, i.e. no subordinates reporting to them. For the purposes of this document, no distinction will be made between Supervisor and Partner Supervisor.

2 The normal workflow sequence call for Two Level Approval. Individual Application approval requirements are at the discretion of the Application owner and may vary from the norm on a case by case basis.
Designated Organizational Role

An individual must have the Organizational Role of Supervisor or Application Security Administrator before they can act as a First or Second Level Approval Authority. In the case of HHS Employees the designation is automatically assigned by the system, provided they have been identified as a Supervisor in the AccessHR System. Partner Supervisors are designated by the Partner Organization and may or may not have direct Supervisory responsibility within the Organization. Enterprise Security Management (ESM) personnel assign the Partner Supervisor and Security Administrator Organizational Role. Communication with ESM ensures the Role is assigned to the correct individual.

Operational Responsibilities

Account Provisioning

The first responsibility we’ll examine is the Provisioning of employee accounts. Provisioning an account enables an employee to access that account via the Enterprise Portal.

While the information required to approve a Request for Access varies with the Application, the process of provisioning remains constant. The three step process follows:

- Employee submits a Request for Access to a specific Application. Both First and Second level approvers may Request Access for another individual
- First Level approval to the requested application is given by the Supervisor based upon knowledge of responsibilities of Requestor.
- Second Level approval to the requested application is granted by the HHS Application Security Administrator.

First and Second Level Approver

- For the First Level Approver the steps taken to approve an Access Request will vary with the Application requested. See the User Guide for detailed instruction and reference for the steps.
- The procedural steps taken by the Second Level approver also vary with the application requested and the reader is referred to the User Guide for detailed instruction and reference.

Modification of User Accounts

The IAM System would not be very functional if it did not provide the ability to modify account information. Fortunately, the System does provide that capability. Modification of User Account enables the Approver to maintain the accuracy of User information and should be preformed regularly as needed.

Account modification can be initiated by either the First or Second Level Approver. If the Second Level Approver initiates it, it will go to the First Level Approver for initial approval first. The First Level Approver is notified of the final action in either case.

Application Accounts

Accounts belonging to your subordinates (or members of your organization in the case of Partner Supervisors with no subordinates) only are available and modifiable by the Supervisor, i.e., you can modify Application Account information for Jane if Jane reports to you, but not Dick if Dick reports to someone else. As such, the modification of Application Account information becomes one of your responsibilities.
**Personal Information**

As the Supervisor you have access to the Personal Information of each employee reporting to you (or members of your organization in the case of Partner Supervisors with no subordinates). You are limited to viewing the information only.

However, you do have the ability to modify your own Personal Information as required. See the User Guide for detailed instruction and reference to making changes to your Personal Information.

**Account Life Cycle Rules**

**Rationale Behind the Rule**

Identity and Access Management (IAM) system automates the enterprise security policies as defined by Enterprise Security Management department. If a user has an application account that has been inactive for 80 days a notification will be sent to the user and their supervisor that their access will be suspended after 10 days if the account is not accessed.

Application accounts that have been inactive for 91 days will be automatically suspended. A notification of the suspension will be sent to the user and their supervisor. In the case of partner employees the supervisor notification will go to each of the user in the Partner Supervisor role for that organization. In the case of the SNAPS application the SNAPS Application Administrator role will receive the notification for the account suspension.

**Stage 1 Event (dormant account warning)**

An employee, contractor, or partner employee has not accessed their account for at least 79 days. An email is sent on the 80th day notifying the individual that the said inactive account(s) will be suspended after 10 days if not accessed. On the same day another email is also sent notifying the employee’s accordingly. The email will list all affected supervisor’s employees and their inactive accounts.
Stage 1 Notifications

To Employees or Contractors

From: HHSC Identity Mgmt Testing
Sent: Friday, March 12, 2010 10:18 AM
To: User’s Name
Subject: Notification of application inactivity
ITIM notification Page 1 of 1
3/12/2010

This is to inform you that the following HHS Enterprise Portal application has not been accessed in the past 79 days; pursuant to the Enterprise Security policy, a user’s access will be suspended if the application has not been accessed within 90 days.

The following HHS Enterprise Portal application is affected:
_ASOIG Account - IEVS ITST (UserId: xxxxxxxxx)

If you have a legitimate business need to keep this access, simply click on this link http://dev.hhsportal.hhs.state.tx.us, login to the Enterprise Portal and access the listed application. If you do not have a legitimate business need to keep this access, please contact your supervisor. If no action is taken the account will be suspended after 10 days.

An email has been sent to your supervisor at the same time that this email was generated. If you have any questions about this email, please contact your supervisor.

If you feel this was done in error or you need to report access issues, please follow your normal problem reporting procedures or contact Identity Management Testing Support at IdentityManageTest@hhsc.state.tx.us or 512-438-2096.

To Employee/Contractor Supervisor

From: HHSC Identity Mgmt Testing
Sent: Friday, March 12, 2010 10:18 AM
To: <supervisor’s name>
Subject: Notification of application inactivity – pending suspension
ITIM notification Page 1 of 1
3/12/2010

This is to inform you that the following HHS Enterprise Portal application has not been accessed in the past 79 days; pursuant to the Enterprise Security policy, a user’s access will be suspended if the application has not been accessed within 90 days.

The following user and HHS Enterprise Portal application are affected:
_Thad Smith (UserId: xxxxxxxxx)_
_ASOIG Account - IEVS ITST

If this user has a legitimate business need to keep this access, they can prevent the account from being suspended by simply accessing the application in the HHS Enterprise Portal (http://dev.hhsportal.hhs.state.tx.us). Otherwise the account will be suspended after 10 days and a notification will be sent.

If the user no longer has a business need for this access, you can suspend their account in the HHS Enterprise Portal ITIM system (http://dev.hhsportal.hhs.state.tx.us/itim). A guide to manually suspending accounts can be found in the “Need Help...?” section of the HHS Enterprise Portal (http://dev.hhsportal.hhs.state.tx.us).

A notification of this issue has been sent to the above user in a separate email.

If you feel this was done in error please follow your normal problem reporting procedures or contact Identity Management Testing Support at IdentityManageTest@hhsc.state.tx.us or 512-438-2096.
To Partner Employee

From: HHSC Identity Mgmt Testing
Sent: Friday, March 12, 2010 10:29 AM
To: <partner's name>
Subject: Notification of application inactivity
ITIM notification Page 1 of 1
3/12/2010

This is to inform you that the following HHS Enterprise Portal application has not been accessed in the past 79 days; pursuant to the Enterprise Security policy, a user's access will be suspended if the application has not been accessed within 90 days. The following HHS Enterprise Portal application is affected:
_CSYL Account (UserID: xxxxx)

If you have a legitimate business need to keep this access simply click on this link http://dev.hhsporal.hhsonstate.tx.us, login to the Enterprise Portal and access the listed application. If you do not have a legitimate business need to keep this access, please contact YOUR organization's designated HHS contact. If no action is taken the account will be suspended after 10 days. An email has been sent to YOUR organization's designated HHS contact at the same time that this email was generated. If you have any questions about this email, please contact them. If you feel this was done in error or you need to report access issues, please follow your normal problem reporting procedures or contact Identity Management Testing Support at IdentityManageTest@hhsc.state.tx.us or 512-438-2096.

To Partner Employee Supervisor

From: HHSC Identity Mgmt Testing
Sent: Friday, March 12, 2010 10:29 AM
To: <supervisor's name>
Subject: Notification of application inactivity – pending suspension
ITIM notification Page 1 of 1
3/12/2010

This is to inform you that the following HHS Enterprise Portal application has not been accessed in the past 79 days; pursuant to the Enterprise Security policy, a user’s access will be suspended if the application has not been accessed within 90 days. The following user and HHS Enterprise Portal application are affected:
<partner's name> (UserID: xxxxxx)
_CSYL Account

If this user has a legitimate business need to keep this access, they can prevent the account from being suspended by simply accessing the application in the HHS Enterprise Portal (http://dev.hhsporal.hhsonstate.tx.us). Otherwise the account will be suspended after 10 days and a notification will be sent.

If the user no longer has a business need for this access, you can suspend their account in the HHS Enterprise Portal ITIM system (http://dev.hhsporal.hhsonstate.tx.us/itim). A guide to manually suspending accounts can be found in the “Need Help…?” section of the HHS Enterprise Portal (http://dev.hhsporal.hhsonstate.tx.us).

A notification of this issue has been sent to the above user in a separate email.

If you feel this was done in error please follow your normal problem reporting procedures or contact Identity Management Testing Support at IdentityManageTest@hhsc.state.tx.us or 512-438-2096.
To TDA Employee

From: HHSC Identity Mgt Testing  
Sent: Friday, March 12, 2010 10:22 AM  
To: <user's name>  
Subject: Notification of application inactivity  
ITIM notification Page 1 of 1  
3/12/2010  
This is to inform you that the following HHS Enterprise Portal application has not been accessed in the past 79 days, pursuant to the Enterprise Security policy, a user's access will be suspended if the application has not been accessed within 90 days.  
The following HHS Enterprise Portal application is affected:  
SNAPS Account - Internal (User Id: xxxxx)  
If you have a legitimate business need to keep this access simply click on this link http://dev.hhsporal.hhs.state.tx.us, login to the Enterprise Portal and access the listed application. If you do not have a legitimate business need to keep this access, please contact the Texas Department of Agriculture at 888-839-5437.  
An email has been sent to The Texas Department of Agriculture at the same time that this email was generated. If you have any questions about this email, please contact the Texas Department of Agriculture at 888-839-5437.

To TDA Employee Supervisor

From: HHSC Identity Mgt Testing  
Sent: Friday, March 12, 2010 11:00 AM  
To: <supervisor's name>  
Subject: FW Notification of application inactivity - pending suspension  
ITIM notification Page 1 of 1  
3/12/2010  
From: IdentityMgmtTest@hhsc.state.tx.us [mailto:IdentityMgmtTest@hhsc.state.tx.us]  
Sent: Friday, March 12, 2010 10:22 AM  
Subject: Notification of application inactivity - pending suspension  
This is to inform you that the following HHS Enterprise Portal application has not been accessed in the past 79 days, pursuant to the Enterprise Security policy, a user's access will be suspended if the application has not been accessed within 90 days.  
The following user and HHS Enterprise Portal application are affected:  
<User's name> (User Id: xxxxx)  
SNAPS Account - Internal  
If this user has a legitimate business need to keep this access, they can prevent the account from being suspended by simply accessing the application in the HHS Enterprise Portal (http://dev.hhsporal.hhs.state.tx.us). Otherwise the account will be suspended after 10 days and a notification will be sent.  
If the user no longer has a business need for this access, you can suspend their account in the HHS Enterprise Portal ITIM system (http://dev.hhsporal.hhs.state.tx.us/itim). A guide to manually suspending accounts can be found in the ‘Need Help…?’ section of the HHS Enterprise Portal (http://dev.hhsporal.hhs.state.tx.us).  
A notification of this issue has been sent to the above user in a separate email.  
If you feel this was done in error please follow your normal problem reporting procedures or contact Identity Management Testing Support at IdentityMgmtTest@hhsc.state.tx.us or 512-438-2096.
Stage 2 Event (dormant account suspension)
The individual’s accounts were suspended on the 91st day because the individual did not access the accounts. An email is sent on the 91st day to the individual stating that the said accounts have been suspended. The email contains instructions to refer the individual to the supervisor for assistance.

Stage 3 Event (dormant account de-provisioning)
The employee’s accounts were deprovisioned on the 121st day because the supervisor did not restore the suspended accounts.
No notification is sent.

Manual Suspension
Account suspension refers to the process of disabling an account without fully removing the account from the IAM system.

Supervisors and Partner Supervisors are authorized to suspend accounts for any user that reports directly to them or the partner organization in the case of partner employees. Similarly, Application Administrators are authorized to suspend accounts for the application(s) they are an administrator for. Regional Security Officers are also permitted to suspend accounts for the application(s) they are an administrator the application(s) they are an administrator for. Enterprise security administrators will be authorized to suspend application or enterprise accounts for any user.

When an application account is manually suspended by anyone other than the user’s supervisor a notification will be sent to the user’s supervisor that the account will be automatically de-provisioned after 90 days.

Restoration of Suspended Accounts
Supervisors are authorized to restore any application or enterprise account for the contractors or employees assigned to them. Similarly, Partner Supervisors are authorized to restore any application or enterprise account for the employees assigned to their partner organization. If supervisor restores an account that was manually suspended by an Enterprise Security Administrator, Regional Security Officer or Application Administrator, the restoration will not be scheduled. Instead, a request for approval will be generated and assigned to that administrator role for approval.

Application Administrators are allowed to restore accounts for the applications they administer and Enterprise Accounts as long as the owner of that account is active. If the account was manually suspended by an Enterprise Security Administrator, or a Regional Security Officer a request for approval will be generated and assigned to that administrator role for approval.

Regional Security Officers are authorized to attempt to restore the application(s) they administrate the application(s) they are an administrator for. If the account was manually suspended by an Enterprise Security Administrator a request for approval will be generated and assigned to that administrator role for approval.

Enterprise Security Administrators are authorized to restore any active user’s account without the need for authorization regardless of the administrator role who initially suspended the account.

For application accounts, a notification will be sent to the user and their supervisor when the account is successfully restored.

Suspension and Restoration of a Person
By suspending a person you essentially deny their access to the Enterprise Portal. There are many scenarios under which this suspension is required. Regardless of reason, a Supervisor, Partner Supervisor, Application
Security Administrator, or a Regional Security Officer are allowed to perform the Suspension and/or Restoration of a Person. The processes for the Suspension and Restoration of a Person are included in the User’s Guide and can be found at: http://architecture.hhsc.state.tx.us/Portal%20Web%20User%20Guide/PartnerRequestPortalAccess.html

Employee Transfer

If an employee is transferred to a different HHS agency any application accounts they have been granted will be automatically deprovisioned. A notification of the accounts being de-provisioned will be sent to the employee’s previous supervisor.

If an employee is transferred to a different business unit and department and they are assigned a new supervisor any application accounts they have been granted will be automatically deprovisioned. A notification of the accounts being de-provisioned will be sent to the employee and the new supervisor.

If an employee is transferred to a different business unit and department, but keep the old supervisor, any application accounts they have been granted will be automatically suspended with a suspended by field set to “ACCESSHR” and the reason for suspension set to “TRANSFER”. A notification of the accounts being suspended will be sent to the employee and the supervisor.

If an employee is transferred to a different department and they are assigned a new supervisor any application accounts they have been granted will be automatically suspended with a suspended by field set to “ACCESSHR” and the reason for suspension set to “TRANSFER”. A notification of the accounts being suspended will be sent to the employee and the new supervisor.

Any other changes to the employee including being transferred to a different department within the same business unit will not trigger any actions being taken on the application accounts they have been granted.

If the employee is a Supervisor of any contractors and the employee is being automatically transferred to a different agency or business unit and department, any contractors that are assigned to the Supervisor will automatically have that Supervisor relationship removed. This will also occur if the employee’s position number is being changed.

Deprovisioning

Deprovisioning or removal of an individual's access is a simple matter; however the reasons for de-provisioning an account can be serious. Regardless of the reason, an account within a First or Second Level Approvers own Area of Responsibility (Application)/Organization can be deprovisioned with the following process.
**Process**

**Step 1**
After searching for and finding the employee in question, (See User Guide for instructions on Search), select the **Manage Account** action option as shown in the circle at right.

**Step 2**
Select the Application account to be deprovisioned as shown in the circle at right.
To select the item, place a **Check Mark (✓)** in the shown check box by mouse clicking inside the check box.
Step 3
Select the **De-Provision** button as shown in the circle at right.

Step 4
The de-provisioning action is scheduled to occur immediately by default as shown in circle #1 at right. If you wish the action to take place on a different date adjust the four list boxes as needed.

Once satisfied with the effective date, select the **Submit** button as shown in circle #2 at right.
Step 5

The Account Management page reappears. At first glance the account just deprovisioned appears present. To verify that the actions you’ve taken have led to the desired result select the Refresh button as shown in the circle at right.

Step 6

The Account Management page reappears minus the deprovisioned account. The subject employee now will not be allowed to Access the Application,