

OAKS FINANCIALS SECURITY POLICY

POLICY NUMBER: 800-01	EFFECTIVE DATE: 06/07/2012	APPOINTING AUTHORITY APPROVAL: 
REPLACES POLICY DATED: 03/01/2008	AUTHORITY:	

I. PURPOSE

The Department of Administrative Services (DAS) employees requiring access to the DAS Financial System in OAKS, must have the appropriate security role(s) assigned and proper approval obtained. The procedure for obtaining this approval is established by this policy. The "FIN Security Request Form – DAS Created" Excel file located in the Fiscal Services Reference Room folder is the form used to request approval and establish proper role access.

II. POLICY

A. FINANCIAL SECURITY APPLICATION REQUESTS

DAS employees who are assigned user role(s) in the OAKS Financial (FIN) System must have divisional and departmental approval of these assigned role(s) in order to access and perform their duties in OAKS FIN. An employee who accesses OAKS to perform job duties is known as an "OAKS user." Approval must be obtained for all FIN users based on the following categories:

1. New User – when a user applies for OAKS access the first time. A "new user" is also defined as a user who has been previously deleted from the OAKS FIN system due to a HCM Position Action being processed.
2. Update Existing User – when there is a change in the user's existing authorized security role(s).
3. Delete User from System – whenever a PA is processed in HCM, an OAKS FIN user will lose FIN access. If that FIN access needs to be deleted before the PA is processed than a FIN Security Request form is needed.

Only those DAS employees who have valid business reasons for accessing OAKS FIN will be granted access. Access privileges are determined by a person's job duties. OAKS FIN access is granted via an update to the OAKS Financials module security table which is accessible through the MyOhio webpage. A user's OAKS FIN access is to be used only for the specific business purposes associated with the user's job duties.

B. SUBMISSION of SECURITY APPLICATION FORM

It is the responsibility of the OAKS FIN user's supervisor to determine the role(s) the user will be assigned. The supervisor will complete the 'FIN Security Request Form – DAS Created' and forward the form to the Division's Business Office Manager.

C. BI-ANNUAL REVIEW OF USERS' SECURITY ROLES

A bi-annual review of all users' security roles will be conducted by all supervisors having employees who use OAKS FIN to perform their job duties. The intent of this review is to raise awareness among the supervisors as to the security access assigned to each employee and to ensure that users have the correct and appropriate roles to perform their jobs in OAKS.

III. PROCEDURE

A. COMPLETING THE SECURITY APPLICATION FORM for OAKS FIN USERS

1. An employee's supervisor must analyze and determine the OAKS financial roles required for the employee to perform his/her job duties. For assistance, the supervisor may view the OAKS FIN Security handbook by running the OAKS FIN query 'OH_ROLE_HANDBOOK' or by contacting the DAS Security Administrator or Designee.
2. A user's supervisor completes the "FIN Security Request Form – DAS Created" located in the Fiscal Services Reference Room folder.
3. A user's supervisor completes the following sections of the security application:
 - Section 1 - Employee/User Information
 - Section 2 - Supervisor Requesting Access for End User
 - Section 4 - Data Access
 - Section 5 - Role Access

B. APPROVAL WORKFLOW for SECURITY APPLICATIONS

1. A user's supervisor e-mails the completed security application to the division's Business Office Manager.
 - Completed security applications are not to be sent to the OAKS FIN Security Team.
2. The division Business Office Manager reviews the security application for completeness and correctness.
3. Division Business Manager e-mails the security application to the CFO and CFO Delegates for approval. The email serves as the divisional approval of the FIN Security Request.

- DAS Chief Financial Officer (CFO) - Jennifer Leymaster
 - DAS CFO Delegate - Anni Efthimiou
 - DAS CFO Delegate - John Yoho
4. The security application is reviewed by the CFO and/or CFO Delegates (Authorized Security Agents).
 5. If the security application is not approved, the CFO or CFO Delegate returns the application to the division Business Manager for revisions.
 6. If the security application is approved, the CFO or CFO Delegate enters the security application into the On-Line Security Request.
 7. Some on-line security applications will require OBM approval and the system will notify the CFO or CFO Delegate as such at the time of submission.
 8. The CFO or CFO Delegate will notify the division's Business Manager that the security application has been approved or requires OBM approval.
 9. If the security application required OBM approval, the CFO or CFO Delegate will wait for OBM's reply.
 10. The CFO or CFO Delegate will notify the division's Business Manager of OBM's reply.
 11. The division Business Manager will notify the supervisor and employee of the approval

IV. MAINTENANCE

A. STORAGE OF SUBMITTED SECURITY APPLICATION FORMS

1. Electronic DAS FIN Security Requests will be maintained by the DAS Office of Finance. DAS users' applications are electronically cataloged by Division/UserName/Date.

B. BI-ANNUAL REVIEW OF USERS' SECURITY ROLES

1. A bi-annual review of all users' security roles is to be conducted by all supervisors having employees that use OAKS FIN to perform their job duties. The intent of this review is to raise awareness among the supervisors as to the security access assigned to each employee and to ensure that users have the correct and appropriate roles to perform their jobs in OAKS.
2. The timing of the bi-annual reviews will be determined by OBM. Supervisors will be provided with instructions, along with important data security reminders to share with their users.
3. Should a user's security need to be modified, a supervisor shall submit an FIN Security Request form following the instructions within this policy to add, change or delete roles, as appropriate.

IV. INQUIRIES

Direct inquires about this policy to:

Finance Service Assurance and Policy Manager
DAS Office of Finance
30 E. Broad Street, 40th Floor
Columbus, OH 43215
Telephone: 614.644.1724
FAX: 614-728.2541

V. REVISION HISTORY

Date	Description of Change
03/01/2008	Original Policy Effective
5/14/2012	Revised to reflect updates in OAKS processes and procedures

OAKS AGENCY FINANCIALS SECURITY APPLICATION INSTRUCTIONS

Section 1 – Employee/User Information

Employee name – Identify the employee using the same name associated with the Employee ID.

OAKS Employee ID – Enter the 8 digit ID assigned in the user in OAKS HCM system

User Setup

New User – Check this box when employee applies for OAKS access the 1st time or if an employee has previously been deleted from the system.

Update existing User – Check this box for any and all changes except New or Deleting a user.

Delete user from System – Check this box when a user's access should be removed from the system. For this action, you need only complete Sections 1, 2 and 3. Also remember, if a PA is processed in HCM, the user's FIN access will be deleted at that time.

Section 2 – Supervisor Requesting Access for End User

Name – Name of user's supervisor.

Phone Number – Supervisor's work phone number.

Section 3 – Authorized Agent Signature

Name of Agent – This is the agent who is authorized by the requesting agency/bureau/dept to approve OAKS security system access requests

Date - Enter, month day, year i.e. June 6, 2007 or 06/06/07

Section 4 – Data Access

Add Business Units – List the Business Units (DAS, PAY, PRT, or Statewide) to which the user should have access in addition the Primary/Default Business Unit. Do not place the Primary/Default Business Unit on this line.

Default Business Units – List the Primary /Default Business Unit (DAS, PAY, or PRT) to which the user should have access. Only enter this Business Unit for the initial application or when the default Business Unit changes

Section 5 – Role Access

Add (Role) – Check the role which should be added to the user's system access. Also enter additional information for those roles where indicated as required.

Delete (Role) – Check the role which should be removed from the user's system access. You do not need to enter additional information for a role when deleting it.

Change (Role) – This box should be marked only when there are changes to the additional information portion of a role that is already assigned to the user.

Accounts Payable Roles

Provided below is a description of the additional information that is required for some of the roles in Accounts Payable.

AP Origin - Enter the Origins to be used when routing information through workflow. When assigning multiple roles, each of which has origins, the same origin must be shown for each role.

Voucher Processor (various types) and Maintainer:

- ***Origin (required)***: This origin will save on the voucher when this user enters a new voucher. The origin will dictate the approval path for that voucher. It will route to Voucher Approvers authorized to approve this origin. A Voucher Processor can only be assigned one Origin.

Voucher Approver 1-3

- ***Origin(s) Authorized to Approve (required)***: Vouchers with this origin provided in the previous field will route to this Voucher Approver.. A Voucher Approver can be assigned multiple Origins.

Note: A user may be a Voucher Approver 1 for one set of origins and a Voucher Approver 2 for a different set of origins. A user may be a Voucher Processor for one Origin and a Voucher Approver for another Origin.

Accounts Receivable Roles

Does not require any additional information, please check the appropriate action needed.

Asset Management Roles

Does not require any additional information, please check the appropriate action needed.

Billing Roles

Does not require any additional information, please check the appropriate action needed.

General Ledger (GL) Roles

Does not require any additional information, please check the appropriate action needed.
A GL Agency Processor cannot also be a GL Agency Approver.

Purchasing Roles

Provided below is a description of the additional information that is required for some of the roles in Purchasing.

- ***Requisitioner***: Gives the OAKS FIN user the ability to enter requisitions; however, the user must enter a Requestor for workflow purposes. That Requestor can be the employee or another Requestor.

- **Requestor:** This role is for workflow purposes only. It drives the approval workflow on a requisition and does not grant access to the system. This role may be set up as a dummy user. Agencies that route workflow based on commodity or dollar value may want to create dummy Requestors for purchases such as IT, office supplies, purchases above \$25,000, etc. If you're using a dummy user, you must use the following naming convention: REQ_<3 letter agency code>_<use of Requestor> and enter this as the OAKS Employee ID. Ex: REQ_DPS_IT or REQ_DPS_OVER25K. Please limit to 30 alphanumeric characters. If setting up a dummy user, enter "Requestor" as both the first and last name. A dummy user will NOT be able to have roles other than the Requestor. A Requestor can NEVER be a Level 4 Agency Approver.
- **Requestor's EmplID (optional):** The Requestor entered in this field will always default when the Requisitioner is entering a requisition. This is for default purposes only; the Requisitioner can change the Requestor during entry. Using this default is useful only if you foresee a Requisitioner entering the same Requestor often or if the Requisitioner and Requestor are one and the same.
- **Next Level Approver (required):** This field is used to drive PO workflow only and should list the employee ID of the first user who the requisition should route to when that Requestor is entered on the requisition. The user entered on this supervisor field should be a Level 1, 2, 3, or 4 Agency Approver.
- **Ship to Location (optional):** This field will default as the Ship To location on the requisition when this Requestor is used. The Ship To location can be updated before the PO is sent to the vendor at the time of entry or during PO approval.
- **Telephone (optional):** This field will display on the PO sent to the vendor as a contact number.
- **Department (optional):** This is one of the five required ChartFields needed to save the requisition. This field can be modified during requisition entry and PO approval. This field should be defaulted when an Agency's Requisitioner may not know about accounting information and it's expected that one of the Requisition Approvers will enter the correct accounting information.
- **Fund (optional):** This is one of the five required ChartFields needed to save the requisition. This field can be modified during requisition entry and PO approval. This field should be defaulted when an Agency's Requisitioner may not know about accounting information and it's expected that one of the Requisition Approvers will enter the correct accounting information.
- **ALI - Appropriation Line Item (optional):** This is one of the five required ChartFields needed to save the requisition. This field can be modified during requisition entry and PO approval. This field should be defaulted when an Agency's Requisitioner may not know about accounting information and it's expected that one of the Requisition Approvers will enter the correct accounting information.
- **Account (optional):** This is one of the five required ChartFields needed to save the requisition. This field can be modified during requisition entry and PO approval. This field should be defaulted when an Agency's Requisitioner may not know about accounting information and it's expected that one of the Requisition Approvers will enter the correct accounting information. Defaulting an account will almost always guarantee that you will need to update this field during requisition entry/approval.
- **Program (optional):** This is one of the five required ChartFields needed to save the requisition. This field can be modified during requisition entry and PO approval. This field should be defaulted when an Agency's Requisitioner may not know about accounting information and it's expected that one of the Requisition Approvers will enter the correct accounting information.
- **A PO Requestor must have a Next Level Approver**

Level 1-3 Agency PO Approvers

- **Next Level Approver (required):** This field is used to drive PO workflow only and should list the employee ID of the user to whom the requisition should route after the current user approves the requisition. The user entered on this supervisor field should have a higher level than the Requisition Approver for which the supervisor is being entered. Ex: A Level 2 Approver must have a supervisor with a Level 3 or Level 4 role. If this user is meant to be an alternate approver (see documentation on

setting up alternates in PO Workflow presentation) and not part of the every-day PO Approval workflow, please enter “alternate” in this field.

- Agency Requisition Approvers for levels 1, 2, and 3 may be set up as dummy users – where the username and password can be shared by a group of users. This allows agencies with central purchasing groups to have requisitions routed to a group without being limited to an individual. If using a dummy user, you must use the following naming convention GRP_<3 letter agency code>_<group identifier> and enter this as the OAKS Employee ID field. Ex: GRP_DMH_CentralPurchasing. Please limit to 30 alphanumeric characters. Also, please enter “group” as both the first and last name.
- A user can only be one level of Agency PO Approver
- A user cannot be a PO Requestor and an Agency Level 4 Approver
- A user cannot be a PO Approver within a path that they are also a PO Requestor
- A user cannot be a PO Ad-Hoc Reviewer and a PO Ad-Hoc Approver
- Anytime a PO Approver is deleted, the Next Level Approver for every Requestor or lower level PO Approver that workflows to that PO Approver must also be changed.

Reporting

Does not require any additional information, please check the appropriate action needed.

- A user needs at least one role in a module to have Reporting access to the data in the role. For example, a user with Reporting role can create a query/report for an Open Purchase Order report but unless that user also has at least one Purchasing role the query/report will be empty.

Central Level Accounts Payable

Does not require any additional information, please check the appropriate action needed.

Central Level Accounts Receivable

Does not require any additional information, please check the appropriate action needed.

Central Level Asset Management

Does not require any additional information, please check the appropriate action needed.

Central Level Purchasing

Does not require any additional information, please check the appropriate action needed.

Central Level Reporting

Does not require any additional information, please check the appropriate action needed.

Central Level System Administration

Does not require any additional information, please check the appropriate action needed.

Central Level Strategic Sourcing

An Event Buyer must have a Next Level Approver