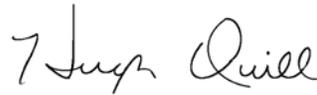


OAKS FINANCIALS SECURITY POLICY

POLICY NUMBER: 800-01	EFFECTIVE DATE: 03/01/2008	APPOINTING AUTHORITY APPROVAL: 
REPLACES POLICY DATED: New Policy	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 “OAKS Agency Financials Security Application” and the “OAKS Central Financials security Application” forms are the vehicles 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.” There are two types of users, Agency Security User and Central Security 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 transfer from one division to another.
2. Delete User from System - when a user terminates employment, transfers within DAS, or transfers to another state agency.
3. Update Existing User – when there is a change in the user’s existing authorized security role(s).

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 by means of a computer account which has an associated user ID and password. 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 OAKS Agency Financials

Security Application or the OAKS Central Financials Security Application and forward the application 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. DETERMINE AGENCY USER'S FINANCIAL ROLE ACCESS

1. An employee's supervisor must analyze and determine the OAKS financial roles required for the employee to perform his/her job duties.
2. A supervisor should refer to the "Agency FIN Role Handbook" or the "Central FIN Role Handbook" for assistance. These handbooks can be downloaded from the Office of Budget Management's (OBM) website:

<http://www.obm.ohio.gov/forms/index.asp>

(Financial Role Handbook is listed under "State Accounting")

3. OAKS/OBM requires that all requests for security role assignments be documented and approved by each agency prior to submission to OBM.
4. The instructions for completing the "OAKS Agency Financials Security Application" form are an attachment to this policy or can be obtained from OBM's website.
5. The "OAKS Agency Financials Security Application" forms should be obtained from OBM's website to ensure the most current version is used:

<http://www.obm.ohio.gov/forms/index.asp>

(the form is listed under "State Accounting")

B. COMPLETING THE SECURITY APPLICATION FORM for OAKS FIN USERS

1. A user's supervisor completes the "OAKS Agency Financials Security Application" or the "OAKS Central financials Security Application" form online and saves it to a file. (Note: Use the excel version only)
2. 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

C. 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 directly to the OAKS FIN Security Team.
2. The division Business Office Manager reviews the security application for completeness and correctness.
3. If the security application is approved, the division's business manager types in the Chief Financial Officer's (CFO) or CFO delegate's name and date of approval in Section 3 of the application form. This action serves as the division's approval of the Security Application.
4. Division Business Manager e-mails the security application to the CFO and CFO Delegates for approval:
 - DAS Chief Financial Officer (CFO) - Quentin Potter
 - DAS CFO Delegate - Anni Efthimiou
 - DAS CFO Delegate - John Yoho

Completed security applications are not to be sent directly to the OAKS FIN Security Team.

5. The security application is reviewed by the CFO and/or CFO Delegates (Authorized Security Agents).
6. If the security application is not approved, the CFO or CFO Delegate returns the application to the division Business Manager for revisions.

D. SUBMISSION OF A USER'S APPLICATION

1. Following departmental approval, the CFO shall e-mail each security application to the OAKS FIN Security Team at: OAKS.FINSecurity@oaks.state.oh.us
2. OAKS FIN Security Team will review, approve and enter the security assignments identified on the user's security application.
3. Upon completion and approval of an application, the OAKS Security Team will notify the agency CFO of approval.

F. NOTIFICATION OF APPROVED APPLICATIONS

1. Response and processing time of OAKS Financial Security applications by the OAKS Financial Security Team will vary based on volume of requests received.

2. Upon completion and approval of an application, the OAKS Security Team will notify the agency CFO of approval.
3. The Agency CFO will notify the division's business manager of the approval.
4. The division's business manager will notify the supervisor and employee of the approval.

G. USER ID and PASSWORD for OAKS FINANCIAL SYSTEM

Upon notification that a user's OAKS FIN access has been established, the user contacts the OAKS Help Desk at oaks.helpdesk@oaks.state.oh.us, at 614-644-6625, or 1-888-OhioOAKS (1-888-644-6625) to receive an initial password.

To log in, do the following:

1. Launch the internet browser and open the OAKS Financial website at FIN.ohio.gov.
2. Enter the ePay (or HCM) UserID and the initial password provided by the OAKS Help Desk.
3. Respond to OAKS FIN prompt to change password.

Note: Employees find it helpful to reset their FIN and ePay/HCM passwords at the same time which allows for both passwords to expire at the same time. The ePay or HCM password can be reset by logging into either ePay.ohio.gov or HCM.ohio.gov (if HCM access is authorized) to change the password.

4. To change the password, click "Change My Password" on the main menu bar.
5. The OAKS FIN password requirements include alpha and numeric characters and a special character:
 - Password length must be at least 8 characters and contain:
 - At least one uppercase or lowercase letter (A – Z or a - z)
 - At least one digit (0 - 9)
 - At least one special character (! " # \$ % & () " * + - , / : ; < = > ? _ .)Examples: Pittsburgh#1, LoneValley?2, \$Lottery12
 - A user's last 10 passwords cannot be re-used.
 - Maximum life of a password is 90 days.
6. In case of a lock-out (after three attempts), contact the OAKS Help Desk at oaks.helpdesk@oaks.ohio.state.oh.us, at 614-644-6625, at 1-888-Ohio-OAKS or follow the instructions in the OAKS Password Reset job aid found at http://oakspmo.ohio.gov/oaks/training/FIN_Job_Aids/FINcontent/FINJA065_Password_Reset.doc

H. SECURING OAKS SECURITY CREDENTIALS AND DATA

DAS OAKS FIN users are responsible for maintaining the security of their unique OAKS FIN access and data. Responsibilities include:

1. Protection of UserID and password: A user must keep his/her UserID and password in a safe location such as a purse or wallet. Do not list the FIN web address with user's UserID and password. A UserID is not to be shared and the password is not to be divulged to others.
2. Securing work station computer: A user must secure his/her OAKS FIN account by properly locking or logging off the computer when leaving the work area.
3. Securing electronic reports: A user must store electronic reports on a DAS or Office of Information Technology (OIT) network server.
4. Protect hardcopy reports containing sensitive data: A user must take precaution at his/her workstation to limit access to hardcopy reports containing sensitive financial data. Where possible, identify and omit sensitive fields from printed reports.
5. Sensitive data includes an individual or company's name, only when in combination or linked to one of the following fields:
 - Social security number;
 - Taxpayer identification number;
 - Driver's license number or state identification card number;
 - Medical information;
 - Information that can be used to access financial resources (such as bank account number, credit or debit card number, EFT numbers, etc.); or
 - Other personal information required by law to be maintained in a secure manner.

I. REVOCATION OF ACCESS TO THE OAKS FINANCIAL SYSTEM

1. When a user no longer works for a division, it is the responsibility of the user's supervisor to request that the User's OAKS FIN account be deleted. At the latest, this request must be completed by the date of termination or transfer. An "OAKS Agency Financials Security Application" form must be submitted to revoke a user's access. This form is available at:

<http://www.obm.ohio.gov/forms/index.asp>
(the form is listed under "State Accounting")

2. If a user transfers to another DAS or OIT division, the hiring supervisor must request that a new OAKS FIN account and security role(s) be established according to the employee's new job duties.

IV. MAINTENANCE

A. STORAGE OF SUBMITTED SECURITY APPLICATION FORMS

1. Electronic DAS Financials Security Applications will be maintained by the DAS Office of Finance. DAS users' applications are electronically cataloged by Division/UserName/Date.
2. Following DAS' submission of the security applications to the OAKS FIN Security Team, the applications are saved to a maintenance file housed on a DAS secure network by the CFO or CFO Delegate.

B. UPDATING of AUTHORIZED APPROVAL AGENTS

1. The OAKS Program Management Office requires that each agency establish and maintain a list of authorized approvers. These authorized approval agents receive applications from the divisions' business managers, review and approve the applications for appropriateness and forward to the OAKS Security Team for processing.
2. DAS approval agents shall be employed by the DAS Office of Finance. By default, the primary approver shall be the department's Chief Financial Officer. Alternate approvers shall be assigned by the CFO and shall assist in reviewing and approving the applications, as determined by the CFO.
3. Notification of updated assignments for the authorized approval agents shall be managed by the department's CFO

C. 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. These bi-annual reviews are to be conducted during the spring and fall ASAP Awareness Weeks. 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 Agency Financials Security Application form following the instructions within this policy to add, change or delete roles, as appropriate.

IV. INQUIRIES

Direct inquires about this policy to:

Business 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

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

Agency Name – Enter full name of the agency. Do not use abbreviations.

Phone Number – Enter employee's work phone number.

Employee Email Address – Enter the business email address.

Please note: You will also need to use this area for the following request:

If creating dummy Requestors for purchases:

You must use the following naming convention: REQ_<3 letter agency code>_<use of Requestor> and enter this as the OAKS Employee ID (EmplID). Ex: REQ_DPS_IT or REQ_DPS_OVER25K.

Please limit to 30 alphanumeric characters and do not use character: &

If creating a share User ID's for Agency Requisition Approvers levels 1, 2, and 3.

You must use the following naming convention GRP_<3 letter agency code>_<group identifier> and enter this as the OAKS Employee ID (EmplID). Ex: GRP_DMH_CentralPurchasing.

Please limit to 30 alphanumeric characters and do not use character: &

Please provide an email address for workflow routing.

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.

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

Name of Agent – Printed name of signing agent

Section 4 – Data Access

Add Business Units – List the Business Units 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.

Remove Business Units – List the Business Units from which current data access should be removed. Do not place the Primary/Default Business Unit on this line.

Default Business Units – List the Primary /Default Business Units 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.

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.

Example – To change the AP Origin of the role Agency Voucher Maintainer that is already assigned to the user, then mark the Change box and list the new AP Origin value on the form.

**Special Note:* To remove additional information that is noted as 'optional' on the form, and for those cases where there is *no replacement* value, please write "Remove current value" on the appropriate line of the form.

Accounts Payable Roles

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.

Business Unit – Enter the Business Units associated with this role, This Business Unit must have also been entered in Section 4 – Data Access previously or with this change application.

Access to all Expense Reports within agency Business Unit: This field should be set to “Y” if this user should have access to view/edit all expense reports within their Business Unit, “N” if they should only view/edit the reports he/she has entered

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.

Voucher Approver 1-3

- **Business Unit(s) Authorized to Approve (required):** Vouchers within this Business Unit and with the origin provided in the next field will route to this Voucher Approver. If entering multiple, please delimit with a comma.
- **Origin(s) Authorized to Approve (required):** Vouchers with this origin and the Business Unit provided in the previous field will route to this Voucher Approver. If entering multiple, please delimit with a comma.

Note: A user may be a Voucher Approver 1 for one set of Business Units/origins and a Voucher Approver 2 for a different set of Business Units/origins.

Travel Expense Processor:

- **AP Origin (optional):** This origin will default onto the travel expense report when this user is entering that transaction. This user has the option of changing the origin during entry.
- **Access to all Expense Reports within agency Business Unit? (Required):** This field should be set to “Y” if this user should have access to view/edit all expense reports within their Business Unit, “N” if they should only view/edit the reports he/she has entered.

Accounts Receivable 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.

Purchasing Roles

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

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.

Requisitioner

- **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.
- **Supervisor** (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.

Level 1-3 Agency Requisition Approvers

- **Approver's Supervisor** (required): This field is used to drive PO workflow only and should list the employee ID of the user who the requisition should route to 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.

Reporting

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