# Access Request System
# Approver Guide

## Approving Roles in ARS

Approving roles in the Access Request System (ARS) is simple. Ensuring that just the right people have just the right access requires more thought. Please review all of the materials in the Resources section after following the "How-To" steps, especially the Segregation of Duties and Role Checklist for the roles you approve.

### Step 1: Set Up Shortcuts

Use this shortcut to streamline your work. Add Approve Requests page to My Links in myUFL:

- Log on to myUFL and navigate to Access Request System > Requests > Approve Requests.
- Click Add to My Links in upper right-hand corner (near Sign out). Use the default name or type a new name.
- Click Save, then click on the drop-down for My Links and verify that it is listed.

### Step 2: Receive Email for Roles to Approve

- All members of an Approver Group will receive an email when a DSA submits a role request for a role in the group.
- The requested action – Add, Delete or Update – is included in the email subject line and body text.
- If you do not need to approve delete role requests, you can disregard the delete requests. These will be processed automatically in the nightly batch process. Some approvers need to see these emails so that they may remove the setups associated with the role.

## Step 3: Review Role Request

- Navigate to the Approve Requests page using the myUFL Menu or the shortcut you created.
- Click on Search. Only requests containing roles in your Approver Group will appear in the list.
- Click on a Role Request in list.
- Review the user information listed in the top section of the Role Request.
- Review requester information and comments, if any, located just below the user information box.
- Scroll down to the Requested Roles section near the bottom of page and find the role or roles you approve.
- You can only take action (i.e., approve, deny, update, hold) on roles in your Approver Group.
- Roles that are approved by other Approver Groups, those that have been approved by other approvers in your own group, and those that are approved automatically in the nightly batch process (i.e., pre-approved roles and most delete role requests), will display in the request but you cannot take action.
- Look at the roles listed in the new request, as well as the list of current roles held (scroll up to top of the page), to check for conflicting roles.
- If a user does not yet have any roles in ARS, you will see the following:


## Step 4: Approve Roles for User

- Note the action requested by the DSA– Add, Delete or Update. The update action only applies to non-PeopleSoft roles that require an Authority Area.
- For your role(s) only, select the appropriate Approver Action from the drop-down box.
- Add an Approver Comment if you **deny** (e.g., "This is a core user role given only to UF Travel Office staff.") or **hold** the role request (e.g., "Waiting on confirmation from Controller that this request is appropriate."). **A hold is a short-term action—it should be used for hours, not days.**
- Note: Approvers do not need to verify that users have taken the required course for a role. The DSA is can no longer request a role until the user has completed the required training course.
- Click Save and then click Approve Request in the myUFL Menu. This will return you to the Approve Request page with all the search fields cleared. Repeat Steps 3-4 until all roles are approved.

- User should have the role the next day. The DSA is instructed to follow up with Bridges Security if this does not happen.

- **Important:** If you cannot take action on a role request within one (1) day, remember to use the Approver Action of "Hold" and fill in the Approver Comments section with the reason for the delay. This will circumvent unnecessary phone calls or emails from DSAs and Bridges Security inquiring why the request has not been completed. **A user cannot have any new roles requested by their DSA until all roles are approved and implemented.**

# Resources for Approvers

There are several tools and resources available to assist you as an approver of security roles. Some of these materials were produced before or during the 2004 implementation. Please provide feedback on these resources and we will revise them in timely manner.

## Reports for Approvers and DSAs

There are several reports in myUFL > Enterprise Reporting > Access Reporting > Application Access. Approvers should use the *Role Authorization by Role Name* report to verify who has a particular role or roles. It is especially useful for making sure only the appropriate individuals have sensitive roles, or for checking for users who have conflicting roles. You must have the UF_ER_PA_APPLICATION_ACCESS and UF_ER_USER roles to access these reports.

## Security Roles

Bridges Security Web page: www.bridges.ufl.edu/security.

This is a good starting point if you are looking for something and not sure where to find it. Includes links to all of the items listed below, and more. This guide and list of approvers will be added to this Web site soon.

The Bridges Web site is broken down into services, and approvers may find it easier to navigate to their particular area (e.g., purchasing, payroll, travel) and then look under the Additional Resources section for role-related documents.

PeopleSoft Role Definitions: www.bridges.ufl.edu/security/roles.html (easiest access via myUFL > ARS)

Should include a list of all requestable roles in ARS, except reporting roles. Please let Bridges Security know if you find any end or core user roles that are missing or inaccurate. Organized by type of role (basic, end, core, Bridges roles), then by module.

Enterprise Reporting Role Definitions: www.bridges.ufl.edu/security (link in first paragraph)

Reporting roles are maintained in Excel spreadsheets and not incorporated into the Bridges Roles Web page.

Legacy (Non-PeopleSoft) Role Definitions: www.bridges.ufl.edu/security (link in first paragraph)

Non-PeopleSoft roles are maintained in Excel spreadsheets and not incorporated into the Bridges Roles Web page.

Role Checklists: www.bridges.ufl.edu/security (Additional Resources for DSAs)

These are resources provided to DSAs to help them determine which roles to request for a user, identifies conflicting roles, warns them of a password policy of P4 or higher, etc.

List of Department Security Administrators: www.bridges.ufl.edu/security/DSA.pdf (access via myUFL > My Account > My Roles)

The list of persons who have the UF_SEC_REQUESTOR role (commonly referred to as a DSA) is typically updated every week or two. Organized in DeptID order and includes the UF Business Email address of every DSA.

## Internal Controls

Segregation of Duties: www.bridges.ufl.edu/security/duties.shtml

Includes an overview of internal controls and segregation of duties. Specific conflicting roles identified for: Accounts Receivable and Billing, Human Resources Management System, Encumbered Purchases, Unencumbered Purchases, PCard, Sponsored Research, and Travel and Expense.

Office of Audit and Compliance Review: http://oacr.ufl.edu/Internal_Control.htm

Includes an overview of internal controls and segregation of duties. Specific conflicting roles identified for: Accounts Receivable and Billing, Human Resources Management System, Encumbered Purchases, Unencumbered Purchases, PCard, Sponsored Research, and Travel and Expense.

## IT and Security Policies

GatorLink Password Management Policy: http://www.it.ufl.edu/policies/passwords.html

The GatorLink username and password is the University standard username and password for authentication for all new information systems. This policy describes the various password policy levels and their relationship to user security roles in myUFL.

UF Information Technology Security Regulations: www.it.ufl.edu/policies/security

Unauthorized access, breach of confidentiality, loss of integrity, disruption of availability, and other risks threaten UF IT resources. UF IT security policies are aimed at reducing exposure to threats, thereby minimizing risk in order to protect UF IT resources. This page contains a link to policies listed below that are particularly relevant to you as an approver and core user.

UF IT Data Security Standard: http://www.it.ufl.edu/policies/security/uf-it-sec-data.html

All data at UF is classified for confidentiality, integrity and availability. This site provides useful examples of the three data classifications at UF: unrestricted, sensitive, restricted.

US Privacy & Data Security: www.nacubo.org/x1594.xml

NACUBO has a useful site that lists reports and news files related to privacy and data security laws and their impact on higher ed institutions. It has a specific site dedicated to the Gramm-Leach-Bliley Act (www.nacubo.org/x2152.xml). Per NACUBO, "…the GLB Act requires financial institutions [including those who participate in financial activities, …like the Federal Perkins Loans] to take steps to ensure the security and confidentiality of customer records such as names, addresses, phone numbers, bank and credit card account numbers, income and credit histories, and Social Security numbers."

UF Acceptable Use Policy: http://www.it.ufl.edu/policies/aupolicy.html

This policy applies to all users of university computing resources, whether affiliated with the university or not, and to all uses of those resources, whether on campus or from remote locations.

# Questions?

Please do not hesitate to contact Bridges Security if you have any questions, problems, or corrections to any of the Bridges documents or Web pages listed above.

Email: Bridges-Security@admin.ufl.edu
Phone: 273-1019
Mailing Address: PO Box 113359