

## Talent Hiring System (THS) Request for User Authorization/Change

Date \_\_\_\_\_

Name of person making the request \_\_\_\_\_

Phone number \_\_\_\_\_

User's Employee ID Number	Name of User	User's Email address	Department Number(s) User associated with in THS (number format should match HRMS)	User Level: Approver 1, Approver 2, or Preparer	THS Workflow Emails (yes or no)	New, Addition, Change or Deletion

**The Talent Hiring System access levels are defined as follows:**

**Preparer:** Creates and routes requisition to the Approver 1 level in the department. Entries made by preparer must be approved by a Departmental approver in the system before it will route to HR.

**Approver Level 1:** Ability to create the requisition and/or approve requisitions that have been received from the Preparer. The Approver will route to the next level in the department workflow.

**Approver Level 2:** Ability to create the requisition and/or approve requisitions that have been received from the Preparer or from Approver Level 1. This Approver provides the highest level of approval for a requisition and will directly route to HR.

**Contact Human Resources for Training: School of Medicine (362-7196) Danforth Campus (935-5906)**

The employee ID will be the user's ID and password initially. The user will be prompted to change the password the first time logged on. The password should be kept confidential. Supervisor or Department should contact Security Systems and Procedures (5-5707) if the user transfers to another department within the University or terminates employment with the University.

I acknowledge that I have read and understand the Washington University Computer & Administrative Information Security Policy attached to this form.

Employee Signature \_\_\_\_\_

Date \_\_\_\_\_

Dept Head Signature \_\_\_\_\_

Date \_\_\_\_\_

Human Resources \_\_\_\_\_

Date \_\_\_\_\_

Security Systems & Procedures \_\_\_\_\_

Date \_\_\_\_\_

Please send completed form to your campus Human Resources  
Campus box # 8002, fax 362-2500 for School of Medicine  
Campus box # 1178, fax 935-9780 for Danforth Campus

# **Please, read and retain in your departmental records.**

## **Washington University Computer and Administrative Information Systems Security Policy**

Washington University's Computers and Administrative Information Systems (AIS) may be used only by designated University employees for the University's purposes. Information contained in these computers and systems is highly sensitive and must be treated as such, not only to comply with our legal and ethical responsibilities to protect the privacy of the University's students, alumni, faculty and employees but also to ensure the integrity of University data. Unauthorized use of AIS and unauthorized distribution of any AIS information is strictly prohibited.

All those who use the AIS system must follow these rules:

1. You may use AIS and any information stored in AIS for specifically authorized University purposes only.
2. You may not discuss information obtained from AIS with anyone except other University employees whose University responsibilities require access to that information.
3. You may not disclose information obtained from AIS by telephone, e-mail, mail, or any other means except as specifically authorized.
4. You may not share your password with others or disclose a password to anyone else. You are responsible for the security of your password and for any use of your password.
5. You should log off AIS when you are not using it. You may not allow others to use your workstation while logged on to AIS or leave your station unattended so that others have access to AIS.
6. You must change your password on a periodic basis.
7. You may not modify or alter computer data files or programs except as specifically authorized.
8. You may not place data or programs on University computers unless you are authorized to do so and the University has the right (by law or license) to do so.
9. Needless to say, you may not use the University's computers for any unlawful purpose and may not vandalize or otherwise damage the University's computer system.

Should your affiliation with the University change or terminate, these prohibitions will remain in effect.

Violation of any of these guidelines may result in disciplinary action, including dismissal, and may also result in referral for civil or criminal legal action.

This Policy supplements and does not replace the Washington University Computer Use Policy, located at <http://www.wustl.edu/policies/compolcy.html>. Each employee must review and understand that computer use policy as well as the guide to legal and ethical use of software located at [http://www.wustl.edu/policies/use\\_sw.html](http://www.wustl.edu/policies/use_sw.html). Anyone with access to student records information must also review and understand the Student Records policy, located at <http://AISweb.wustl.edu/Registrar/ferpa.nsf/pages/ferpa>.

If you have any questions about these guidelines, contact Systems and Procedures at 935-5707.