

**COMPLIANCE MODULE/COMPLIANCE MANAGEMENT SYSTEM
SECURITY AUTHORIZATION/REQUEST FOR DELETION**

Return completed forms to Systems and Procedures, Campus Box 1110, or fax to 935-8619.

Part A. Requester Information

Name: _____ Job Title: _____

Employee ID: _____ Phone Number: _____ Box: _____

Dept Name: _____ Dept. No: _____

Do you currently have an FIS password? No Yes

Please select reason for request: New Change Addition Deletion

Part B. Functional Access

Put a check mark in the "Need" column to designate the functions that you require in the performance of your job.

Need	Role Description	Access Description
	Inquiry	This role allows the user to view compliance and training requirements for an individual, by department/division, and by grant proposal.
	*Compliance Non WU Appointee Entry	This role allows the user to enter a Non WU Appointee for the purpose of completing education or compliance requirements, for example Human Subjects Education (CITI)
	*Compliance Non WU Appointee Update	This role allows the user Non WU Appointee Entry plus the ability to update/edit the name fields. <i>(Reserved for Compliance/Central Offices only)</i>
	*Non WU Appointee Requirements Move	This role allows the user to move compliance and training requirements from a Non-WU Appointee to a WU Appointee. <i>(Reserved for Compliance/ Central Offices only)</i>
	*Compliance Financial Disclosure Statement	This role allows the user access to the "View FDS Details" tab on both the View Requirements for an Individual and Proposal pages. <i>(Reserved for the Office of Sponsored Research Services only.)</i>
	*Compliance User	This role allows the user to attach a Compliance Category to an individual and also record the date a Compliance Requirement has been met. <i>(Reserved for Compliance/Central Offices only)</i>
	*Compliance Administration	This role allows the user to maintain most of the tables within the Module. Access to create and link Requirements and Compliance Categories, various maintenance pages, including the creation and maintenance of the Compliance Profile questions, and access to the Non-WU Appointee Match page. <i>(Reserved for the Office of Vice Chancellor for Research only.)</i>

*(*Requires Research Ethics & Compliance Office signature.)*

Part C. Departmental Approval

I certify that the above named individual requires the specified access to the requested system as stated on this Security Authorization form, and that such access is appropriate in the conduct of their job responsibilities.

Dept. Head Signature _____ Date _____

**Research Ethics & Compliance Office* _____ Date _____

Security Officer, Systems & Procedures _____ Date _____

Please retain a copy for your departmental records.

**RESEARCH ADMINISTRATION SYSTEM (RAS)
SECURITY AUTHORIZATION/REQUEST FOR DELETION**

EMPLID _____

Part D. Requester Security and Privacy Statement

I certify that my position at Washington University requires access to the requested system as stated on this Security Authorization form. I acknowledge that my access is strictly for business use and any non-business use may be subject to disciplinary action. I further acknowledge that I have read and will comply with the following University policies:

- Information Security Policy, located at <http://www.wustl.edu/policies/infosecurity.html>,
- Computer Use Policy, located at <http://www.wustl.edu/policies/compolicy.html>,
- Guide to Legal and Ethical Use of Software, located at http://www.wustl.edu/policies/use_sw.html,
- Student Records Policy, located at <http://aisweb.wustl.edu/registrar/ferpa.nsf/pages/ferpa>.

To ensure the privacy and security of University data, I will:

- Access, distribute and share all University data only as needed to conduct campus business as required by my job.
- Respect the confidentiality and privacy of individuals whose data I access.
- Observe any ethical restrictions that apply to data to which I have access.
- Immediately report to my supervisor any and all security breaches.
- Comply with all department and campus IT and business process security policies and procedures, including proper and timely destruction of documents and/or files containing sensitive data.
- Protect and secure data on portable devices; e.g., laptops, thumb drives, CDs.
- Change my password on a periodic basis, as required.
- Contact the appropriate personnel to have my access revoked upon transfer to another department within the University or termination of my employment with the University.

I will not:

- Discuss verbally or distribute in electronic or printed form University data except as needed to conduct University business as required by my position.
- Knowingly falsely identify myself.
- Gain or attempt to gain unauthorized access to University data or computing systems.
- Share my user ID(s) and password(s) with anyone nor use anyone else's user ID(s) or password(s) without departmental review.
- Leave my workstation unattended or unsecured while logged-in to critical functions or sensitive information.
- Use or allow other persons to use University data or software for personal gain
- Make unauthorized copies of University data or software.
- Engage in any activity that could compromise the security or confidentiality of University information services.
- Place data or programs on University computers which are not required for my job function. All data and programs must be ones for which the University has the right for use by law or license.

I have read and agree to comply with the terms and conditions stated above. I further understand that a breach of this agreement may be grounds for immediate dismissal and may also result in referral for civil or criminal legal action. Should my affiliation with the University change or terminate, these prohibitions remain in effect.

Requester Signature _____ Date _____

If you have questions about any of these terms and conditions, contact your school, department, or unit system manager, or call Systems and Procedures at 314-935-5707.

Please retain a copy for your departmental records.