

**PMWeb
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: _____

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
	Accounting User	View, create and edit access to project setup, budgeting, and cost management modules for the purposes of construction accounting; view only access to BI reporting.
	Administrative Assistant Guest User	View only access to all visible modules and reporting; view, edit, create access to relevant forms and change requests.
	Administrative Assistant User	View access to all visible modules, create and edit access on project setup, cost management and forms for the purpose of project management support; view only access to BI reporting.
	Administrators	Full access to all PMWeb features and functions
	Executive Management	View only access to all visible modules for the purposes of project management and oversight.
	Management	Full control over all visible modules for the purposes of project management oversight and control.
	Project Guest	View only access to all visible modules and reporting; view, edit, create access to relevant forms and change requests.
	Project Managers	View, create and edit access to project setup, cost modules and forms for the purpose of project management; view only access to BI reporting
	Purchasing Team	View, create and edit access to planning modules and forms for the purpose of resource management; full access to procurement module; view only access to Cost Management and BI reporting.
	Superusers	Full control over all visible modules for the purposes of project management and construction accounting; view only access to BI reporting.
	View Only	View only access to planning, cost and reporting modules.

Part C. Department 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 _____

Facilities Dept Signature _____ Date _____

Security Officer
Systems & Procedures _____ Date _____

Please retain a copy for your departmental records.

PMWeb
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.