Responsible Office: Office of the Controller
Date First Effective: 6/1/2000
Revision Date: 6/30/2013

Financial Systems Access

Policy Statement

This policy establishes under what circumstances individuals can access University-wide financial systems. Access to these systems will be granted only where there are valid business reasons. All financial-systems access requests must originate from tub-appointed Authorized Requestors, and all requests are granted by administrative personnel within Financial Systems Solutions (FSS).

All data and information stored on Harvard's financial applications is considered confidential and must be handled in accordance with the University's Enterprise Information Security Policy.

Reason for Policy

Certain Harvard employees and other individuals connected to the University must have access to the University's financial systems to allow the University to operate efficiently and to enable local units to process University payments and other financial transactions in accordance with risk-control requirements like separation of duties. This policy is necessary to minimize the risks associated with granting access to Harvard's financial systems.

Who Must Comply

All Harvard University schools, tubs, local units, Affiliate Institutions, Allied Institutions and University-wide Initiatives must comply.

Procedures

1. **Identify business need for new or changes to existing systems access**. Access to Harvard financial systems is only granted where required by a University business need. Where required by a valid business need, the University permits financial systems access of varying levels to the following four types of financial- systems users:

    A. Harvard employees

    B. Temporary Harvard employees (including students with jobs)
        a. Harvard temporary employees (including students) may be granted access to certain Harvard financial systems in limited situations.
        b. These individuals are generally **not** allowed access to the PCard settlement system.

    C. Affiliated hospital employees
        a. Affiliated hospital employees may be granted access to Harvard's financial systems in limited situations. See the Appendix A of this policy for more information.
        b. Non-Harvard Medical School tubs should note that HMS has done extensive work in the area of establishing procedures for granting systems access to its affiliates. HMS has developed standard forms and agreements that must be signed by the affiliated hospital employees prior to granting financial-systems access. These forms might serve as a model for other tubs with non-Harvard employees requiring financial-systems access.

    D. Consultants and agency employees
        a. Consultants and agency employees may be granted access to Harvard's financial systems in limited situations. These situations are expected to be rare given risks associated with security, maintenance, and monitoring of such activity.
        b. These individuals are not allowed access to the PCard settlement system.

2. **Ensure user has a valid HUID**. All users of Harvard's financial systems must have a valid University-issued identification number (HUID), which may be a permanent-employee ID or a temporary ID.

3. **Send request documenting business need to tub Authorized Requestor (AR).**
   A. All access requests must originate from Authorized Requestors, established in each of the tubs. Refer to the "Responsibilities and Contacts" and "Definitions" sections of this policy for more information.
   B. Certain types of access (e.g., University-wide access, access to other tubs' data) require additional approvals.
   C. See Appendix B for detailed instructions on how to request, change or terminate access for different types of users.

4. **Validate user access annually.** Each year, Authorized Requestors must review the list of users and their associated access for appropriateness, making changes where needed. Authorized Requestors must sign off on final lists for their respective areas.

Responsibilities and Contacts

Financial deans or equivalent tub financial officers are responsible for ensuring that local units abide by this policy. Tubs are responsible for appointing Authorized Requestors, and for ensuring that local financial-systems users are adequately trained, have appropriate systems security privileges, and are aware of and compliant with the University's Enterprise Information Security Policy. In particular, tubs granting access to non-employees (i.e., students, post-docs or third-party employees) must ensure that the access granted to such individuals is necessary to assist Harvard employees in performing administrative tasks. Tubs must periodically review local users who have been granted system access, and change, grant, or delete access as appropriate.

Authorized Requestors are responsible for requesting financial-systems access for a certain group of individuals within a tub or for individuals across an entire tub, depending on local tub policies and procedures. Authorized Requestors must determine the minimum level of system access necessary for each designated user to perform his or her required job duties. Authorized Requestors must send all requests directly to Financial Systems Solutions (FSS) using established practices, and must maintain documentation to support those requests.

Financial Systems Solutions (FSS) is responsible for responding to tub Authorized Requestor requests for financial-systems access, and for regularly monitoring active financial-systems users for appropriateness of system access, using employee-termination data and other information. ***Contact: http://vpf-web.harvard.edu/fss/ or 617-496-2001***

Definitions

Affiliated Hospital Employee: An individual who performs Harvard business but who is paid by one of the affiliated Harvard hospitals. The affiliated hospital employee (or "affiliate") must have a special ID number issued by Harvard University Identification and Data (HUID) Services for the purpose of logging into the financial systems. Note: Harvard affiliate institutions other than affiliated hospitals, whose workers are not Harvard employees, may apply this policy to their own employees. Affiliate institutions in this situation should follow the guidelines related to affiliated-hospital employees when applying this policy.

Agency Employee: Worker hired on a short-term basis from an employment agency; must have a special ID number issued by Harvard University ID Services for the purpose of logging into the financial systems.

Authorized Requestor: Tub financial dean or designee responsible for determining user security access in their tub. Financial Systems Solutions (FSS) will not accept any user security request unless it originates from an Authorized Requestor.

Consultant: An independent contractor or individual representing a firm providing services for Harvard; must have a special ID number issued by Harvard University ID Services for the purpose of logging into the financial systems.

Harvard Employee: An individual with an active job record or appointment in Harvard's PeopleSoft (PS) Human Resources Management System (HRMS) and a valid Harvard University ID number, including Less than Half Time employees (LHT). Employees generally receive some form of benefits such as pension, medical, dental, vacation, sick days, etc.

Harvard University ID Number (HUID #): A unique eight-digit identification number generated by Harvard's PeopleSoft (PS) Human Resources Management System (HRMS) or the HIRES system. Most degree students also have identification numbers issued by HUID services.

Temporary Harvard Employee: An individual with a job record in Harvard's PeopleSoft (PS) Human Resources Management System (HRMS) and a valid Harvard University ID number. This definition includes Harvard and non-Harvard students with jobs. This group generally does not receive employee benefits. Payroll is driven by hours submitted each week.

University-wide Financial Systems: For purposes of this policy, University-wide financial systems include the Oracle E-Business Suite, the Grants Management Application Suite (GMAS) and the Harvard University Budgeting System (HUBS). Note that PeopleSoft is a Human Resources system; contact HR for information on PeopleSoft access.

Related Resources

Harvard Enterprise Information Security Policy (HEISP) http://security.harvard.edu/enterprise-security-policy
Procurement and Reimbursement Systems: http://vpf-web.harvard.edu/ofs/policies/documents/procu_reimb_syste.pdf
Stewardship Responsibility: http://vpf-web.harvard.edu/ofs/policies/documents/stewa_respo.pdf

Revision History

6/30/2013: Updated format

Appendices

Appendix A: Access to Harvard's Financial Systems Policy Grid
Appendix B: Detailed Instructions for Granting Systems Access
Appendix C: HUBS User Security Form

Appendix A:
Access to Oracle E-Business Suite Matrix

Note: Tubs may have policies that are more restrictive than those outlined below.

Last revised 3/31/2013		User/Employee Type			
		Harvard (including LHT)	Temporary Harvard	Affiliated Hospital	Consultant/ Agency
		HUID#	HUID#	Special ID#	Special ID#
Activity Type	System Access	Univ Policy Allow Access?	Univ Policy Allow Access?	Univ Policy Allow Access?	Univ Policy Allow Access?
RECEIVE $$	AR-Non Collections	Yes	Yes	Yes*	Yes
RECEIVE $$	AR- Collections	Yes	No	Yes*	No
SPEND $$	HCOM/Web Reimbursement Preparer	Yes	Yes	Yes*	Yes
SPEND $$	HCOM/Web Reimbursement Approver	Yes	No	Yes*	No
SPEND $$	Corp Card Holder	Yes	No	No	No
SPEND $$	Pcard Holder ***	Yes	No	Yes*	No
SPEND $$	AP Feeds	Yes	No	No	No
MOVE $$	Pcard Settlement	Yes	No	Yes*	No
MOVE $$	GL Manual Journals, including ADI	Yes	Yes	Yes*	Yes
REPORT $$	Ad Hoc	Yes	Yes	Yes*	Yes
REPORT $$	CREW	Yes	Yes	Yes*	Yes

*Yes, with Special Affiliate Agreement (using his or her own Special ID#, depending on specific financial systems application.

** Eligibility restrictions apply; see the Harvard Travel Service website for more information: http://www.travel.harvard.edu/cgi-bin/travel/policies_procedures.php

*** Certain graduate and undergraduate students may be eligbile to receive a Pcard. Contact your Pcard local administrator for details.

REQUESTING ACCESS			
User Category	**Oracle and CREW**	**HUBS**	**GMAS**
Harvard Employee	• Tub AR submits request via the Oracle user security request online form to FSS Client Services. • FSS reviews the request and grants systems access accordingly. • If the request requires additional approvals (i.e. University wide access), FSS will process the request upon receipt of approval.	• ARs submit a completed HUBS user security form via email to hubssecurity@harvard.edu. • See HUBS user security form in Appendix C	• GMAS ARs submit requests in body of an email to gmassecurity@camail.harvard.edu and include the following details: o Schools who own their standing teams submit the following: ▪ User name ▪ HUID ▪ Action required (either set GMAS user flag to Yes or No) o Schools who do not own their standing teams submit the following: ▪ User name ▪ HUID ▪ Action required (either set GMAS user flag to Yes or No) ▪ Standing team to which user needs to be added/removed
Temporary Harvard Employee (including students with jobs)	• Tub AR submits request via the Oracle user security request online form to FSS Client Services. • **The Form must specify the temporary employee's expected termination date**. • FSS reviews the request and grants systems access accordingly. • If the request requires additional approvals (i.e. University wide access), FSS will process the request upon receipt of approval.	• ARs submit a completed HUBS user security form via email to hubssecurity@harvard.edu. • See HUBS user security form in Appendix C	• GMAS ARs submit requests in body of an email to gmassecurity@camail.harvard.edu and include the following details: o Schools who own their standing teams submit the following: ▪ User name ▪ HUID ▪ Action required (either set GMAS user flag to Yes or No) o Schools who do not own their standing teams submit the following: ▪ User name ▪ HUID ▪ Action required (either set GMAS user flag to Yes or No) ▪ Standing team to which user needs to be added/removed

REQUESTING ACCESS			
User Category	**Oracle and CREW**	**HUBS**	**GMAS**
Affiliated Hospital Employee	• **The Form must specify the affiliated hospital employee's expected termination date (not to exceed January 31st of the following year).** • FSS reviews the request and grants systems access accordingly. • If the request requires additional approvals (i.e. University wide access), FSS will process the request upon receipt of approval.	• ARs submit a completed HUBS user security form via email to hubssecurity@harvard.edu. • See HUBS user security form in Appendix C	• GMAS ARs submit requests in body of an email to gmassecurity@camail.harvard.edu and include the following details: o Schools who own their standing teams submit the following: ▪ User name ▪ HUID ▪ Action required (either set GMAS user flag to Yes or No) o Schools who do not own their standing teams submit the following: ▪ User name ▪ HUID ▪ Action required (either set GMAS user flag to Yes or No) ▪ Standing team to which user needs to be added/removed
Consultant/Agency Employee	• ***Tub AR must first email FSS to set user up in Oracle before access to specific systems can be granted.*** • Tub AR submits request via the Oracle user security request online form to FSS Client Services. • **The Form must specify the consultant/agency employee's expected termination date (not to exceed one-year term).** • FSS reviews the request and grants systems access accordingly. • If the request requires additional approvals (i.e. University wide access), FSS will process the request upon receipt of approval.	• ARs submit a completed HUBS user security form via email to hubssecurity@harvard.edu. • See HUBS user security form in Appendix C	• GMAS ARs submit requests in body of an email to gmassecurity@camail.harvard.edu and include the following details: o Schools who own their standing teams submit the following: ▪ User name ▪ HUID ▪ Action required (either set GMAS user flag to Yes or No) o Schools who do not own their standing teams submit the following: ▪ User name ▪ HUID ▪ Action required (either set GMAS user flag to Yes or No) ▪ Standing team to which user needs to be added/removed

TERMINATING/EXTENDING ACCESS AND EMPLOYEE TRANSFERS			
User Category	**Oracle and CREW**	**HUBS**	**GMAS**
Harvard Employee	• A terminated Harvard employee will automatically be disabled as a financial-systems user when that employee terminates from all jobs according to PeopleSoft. • In emergencies, an employee's access can be immediately disabled via phone call to Client Services; requestors must follow up with documentation/ written request for tracking purposes. • FSS regularly runs PeopleSoft reports to identify employee transfers. If a Harvard employee transfers to another position within the University, FSS notifies the tub's AR that the transferred employee's financial-systems access will be terminated unless the tub's AR requests otherwise.	• ARs email termination/extension request to hubssecurity@harvard.edu	• GMAS ARs submit requests in body of an email to gmassecurity@camail.harvard.edu
Temporary Harvard Employee	• FSS will terminate a temporary employee's access on the specified termination date or when the employee terminates from all jobs according to PeopleSoft, if sooner. • If a temporary employee transfers to another position within the University, FSS notifies the tub's AR that the transferred temporary employee's financial-systems access will be terminated unless the tub's AR requests otherwise. • If a temporary employee terminates employment before his or her expected termination date, the tub's AR must notify FSS. • In emergencies, a temporary employee's access can be immediately disabled via phone call to Client Services; requestors must follow up with documentation/ written request for tracking purposes.	• ARs email termination/extension request to hubssecurity@harvard.edu	• GMAS ARs submit requests in body of an email to gmassecurity@camail.harvard.edu

TERMINATING/EXTENDING ACCESS AND EMPLOYEE TRANSFERS			
User Category	**Oracle and CREW**	**HUBS**	**GMAS**
Affiliated Hospital Employee	• FSS will terminate an affiliated hospital employee's access on the specified expected termination date or on January 31st of the following year, whichever date occurs first. • If the affiliated hospital employee needs continued access, the tub's AR must request an extension from FSS; the extension must not exceed January 31st of the following year. • If an affiliated hospital employee terminates employment before his or her expected termination date, the tub's AR must notify FSS. • In emergencies, an affiliated hospital employee's access can be immediately disabled via phone call to Client Services; requestors must follow up with documentation/ written request for tracking purposes.	• ARs email termination/extension request to hubssecurity@harvard.edu	• GMAS ARs submit requests in body of an email to gmassecurity@camail.harvard.edu
Consultant/Agency Employee	• FSS will terminate a consultant or agency employee's access on the specified expected termination date. • If the consultant or agency employee needs continued access, the tub's AR must request an extension from FSS; the extension must not exceed one year. • If a consultant/agency employee terminates employment before his or her expected termination date, the tub's AR must notify FSS. • In emergencies, a consultant/agency employee's access can be immediately disabled via phone call to Client Services; requestors must follow up with documentation/ written request for tracking purposes.	• ARs email termination/extension request to hubssecurity@harvard.edu	• GMAS ARs submit requests in body of an email to gmassecurity@camail.harvard.edu

HUBS USER SECURITY REQUEST FORM

AR DETAILS

AR Last Name		**AR First Name**	
AR Email			
Tub			

SAMPLE REQUEST

User Information		Request Type			Planner/Viewer	Security Profile	Indicate Org Access and Write or Read	Alt Org Hierarchies Access and Write or Read	Optional Access	Comments
HUID	Name	Request Type (Add, Mod, Del or Copy)	Copy HUID	Copy Name	Planner/Viewer	Security Profile	TUB.ORG *separate ranges with commas*	Alt TUB.ORG *separate ranges with commas*	Smartview Write Access	Request Comments
Examples										
12345678	Denzel Washington	Add			Planner	EmplCINA	All orgs-write	Alt_All Tub_Orgs-read		Sample comment
87654321	John Harvard	Delete								Delete this user
11112222	Jane Smith	Copy	57681233	Jennifer Aniston						
33334444	George Michael	Mod					S1234-write, S6789-write	Alt_Admin-read, Alt.Staff-read		

ENTER DATA HERE

User Information		Request Type			Planner/Viewer	Security Profile	Indicate Org Access and Write or Read	Alt Org Hierarchies Access and Write or Read	Optional Access	Comments
HUID	Name	Request Type (Add, Mod, Del or Copy)	Copy HUID	Copy Name	Planner/Viewer	Security Profile	TUB.ORG *separate ranges with commas*	Alt TUB.ORG *separate ranges with commas*	Smartview Write Access	Request Comments