UNIVERSITY OF SOUTH CAROLINA

HCM Distribution Access Form
(1) Complete this form and have it signed by your operating unit Business Manager.
(2) Email the completed form to pssecure@mailbox.sc.edu.

Important: Be sure to save this PDF to your drive or a Network folder before you fill it out. Also, be sure to save when you get to the end of the form.

Employee/ Affiliate Contact Information

EMPLID (USC ID)	
Last Name	
First Name	
Department ID Enter your Dept's 6-digit PeopleSoft ID	
Dept./College/Division Name	
Phone	
Email	
Campus/Operating Unit	
Network ID	

Requesting access to HCM Distribution: Access to view GL Distribution information.

☐ Department Access

Requesting Access to the Following Departments (6-digit PeopleSoft Department ID is REQUIRED)

☐ ☐ ☐ ☐ ☐

NOTE: Provide the 6-digit PeopleSoft Department ID for each Department for which you are requesting access.

☐ Project Access

Requesting Access to the Following Projects (8-digit PeopleSoft Project ID is REQUIRED)

☐ ☐ ☐ ☐ ☐

Remove Role:

☐ This person has a **change in responsibilities** within their current office and requires a change in roles. Roles/Department(s) to be removed: _____

☐ This person has left their **current** USC office, but **remains employed** in a different USC office. Please remove roles and departments for old office.

☐ This person is **no longer employed/affiliated** with USC.

User Agreement for Responsible Use and Confidentiality of Data, Technology, and user Credentials

I have completed the Securing the Human training, and I understand that by virtue of my employment or relationship with the University of South Carolina (UofSC), I may have access to University Technology Assets, including data, technology, user credentials, and other assets, which must be protected according to laws, regulations, policies, procedures and guidelines. This includes being granted access to Payroll data for my department.

My signature below denotes that I have read and understand my responsibilities as outlined in the following UofSC policies and others available on the UofSC policy website http://www.sc.edu/policies/:

UNIV 1.51	Data and Information Governance
UNIV 1.52	Responsible Use of Data, Technology, and User Credentials
ACAF 3.03	Handling of Student Records
FINA 4.11	Credit/Debit Card Processing and Security
HR 1.22	Telecommuting
HR 1.69	Official Personnel Files and Records Release
IT 3.00	Information Security
LESA 3.06	Reporting Loss or Theft of University Property

I acknowledge that unauthorized access or disclosure, through my deliberate actions or negligence, of any data, information, technology, user credential, or another asset could subject me to criminal and civil penalties imposed by law. I further acknowledge that unauthorized disclosure or access may also constitute just cause for disciplinary action. In the event access is determined to be contrary to university policy or applicable law, appropriate measures will be taken, including referral to student, employee, or faculty disciplinary processes. If I am ever in doubt about my responsibilities regarding UofSC data, technology, user credentials, or other assets involving Payroll data, I will immediately consult the Payroll Data Stewards.

Employee/Affiliate Signature _____ Date _____

Business Manager Signature (only required for Workflow and/or General System Access) _____ Date _____

Print Business Manager Name _____

Chancellor, Dean, VP, or Dept. Head Signature _____ Date _____

Print Chancellor, Dean, VP, or Dept. Head Name _____

Payroll Data Steward Signature (to be signed by Payroll Department only) _____ Date _____

Print Payroll Data Steward Name _____