Setting up your Supervisory Organization

Workday Naming Conventions

I. Policy
Supervisory organizations are necessary in Workday. These organizations are used to manage the USC’s human capital by creating a structure based on hierarchy. Each Supervisory Organization should be unique and equated to one particular department within a school or division and reflect the departmental leadership.

Recommendations
USC supervisory organization naming conventions should include the School or Division Name, Department Name, and a unique numerical designation. All names should reflect the formal directory listing of schools and not be abbreviated.

Note: There are no character limits to the names of your supervisory organizations.

The proposed naming convention for your supervisory organization should follow:
School/Division Name: Department Name

The manager’s name should not be viewable. Schools and divisions may be permitted to name their own departments. Please avoid redundancy when naming your organization.

Here is an example of an approved Supervisory Organization name.
Engineering: Viterbi Business Affairs

II. Process

Special Characters to Avoid

<table>
<thead>
<tr>
<th>Pipe</th>
<th>Double Quotes &quot;&quot;</th>
<th>Hash #</th>
<th>Dollar Sign $</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caret ^</td>
<td>Back Tick `</td>
<td>Backslash \</td>
<td></td>
</tr>
</tbody>
</table>
The need for a new supervisory organization should first be assessed and then formally requested through the HR Partner who will then review and approve all requests.

Your HR Partner will then provide a *Supervisory Organization Request Form*. All areas of the form must be completed and submitted.

Once your request is approved, it will then be routed to the Human Resources Shared Services department who will initiate the request and configure your updated Supervisory Organization in Workday.

### III. How to Change

#### Supervisory Organization Setup Form

<table>
<thead>
<tr>
<th>Reason for New Organization</th>
<th>(Please select one)</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Department ☐</td>
<td>New Supervisor ☐</td>
</tr>
</tbody>
</table>

**Reason Comments:**

Supervisor Name: ___________________________ Employee ID: ___________________________

School and Department this employee will be supporting (no abbreviations): ___________________________

Effective Date ___________________________

Approver Name: ___________________________ Date: ___________________________

Approver Signature: ___________________________
University Records Security and Confidentiality Agreement

The University of Southern California is committed to controlling and protecting the access to, use of, and storage and disposal of employment records and the information they contain. This includes (but is not limited to) personal information (such as Social Security numbers, addresses, telephone numbers, tax information, bank accounts, credit cards); payroll and employment information (such as employment history, salaries and wages, payment instructions, garnishments, immigration documentation, terms and conditions of employment, performance evaluations, disciplinary action, terminations, legal agreements, investigative reports); and benefits information (such as dependent and beneficiary information, medical claims, account numbers, financial data). Those with access to Workday, ais-c2000 (PPBS), timekeeping systems, Glacier and other payroll, human resources and benefits systems or data are in a unique position of trust, required to maintain the security and confidentiality of employment records. In light of this, each user must agree and adhere to the following principles and requirements:

1. Unauthorized access, use, storage or disclosure of employment records or reports is prohibited, including any access, use, storage or disclosure for any reason other than the legitimate execution of duties and responsibilities assigned by the university.

2. Each user has unique access codes (login ID, password, operator code, etc.). Users may not divulge or allow anyone else to use these codes. If users suspect someone knows or is using their access codes, they must immediately notify the Human Resources Service Center at: ushr@usc.edu The Service Center can also be reached Monday through Friday, from 8am – 6pm (213) 821-8100

3. Users may not leave a system unattended without properly and fully exiting from all systems.

4. Users may not inquire or look up any data on any employee unless authorized to do so and as required in the course of executing the duties and responsibilities of their job.

5. Users may not update or alter in any way their own records or records of family members or other close relations.

6. Users may not knowingly include or cause to be included any false, inaccurate or misleading information in any records.

7. Users may not personally benefit or allow others to benefit from knowledge of any confidential information to which they have access or exposure.

8. No official records or any copy thereof may be physically removed from the office where they are maintained or downloaded or in any way electronically transmitted, except in the performance of duties.

9. Use of university computer equipment requires adherence to all ITS policies (see http://www.usc.edu/its/policies/).

10. Users may not aid, abet, or act in conspiracy with another to violate any part of this agreement.

Violation of this agreement may result in cancellation of access, and also lead to reprimand, suspension, dismissal and/or termination consistent with the university policy.

I have read and agree to abide by the above principles and requirements:

Print name legibly: __________________________ Department: __________________________
Email: __________________________ Phone: __________________________
Signature: __________________________ Date: __________________________
Supervisor acknowledgment: __________________________

3