

Service Level Agreement: UCI/UCSD AP Recruit

Provided by UC Irvine Network & Academic Computing Services.

This SLA describes the agreement that UCI will provide AP Recruit as a service to UCSD.

Agreement effective date: TBD

Versions

Version	Date	Revision/Description	Author
0.1	5/9/2009	Rough cut	Max Garrick
0.2	5/13/2009	Draft	Max Garrick
0.3	5/20/2009	Draft 0.1	Shohreh Bozorgmehri
0.4	6/8/2009	Draft 0.2	Jennifer Kramer
1.0	6/22/2009	Final	Max Garrick

Approval

Approvers	Affiliation	Campus	Approval Date
Shohreh Bozorgmehri	Director of Academic and Network Applications	UC Irvine	6/24/2009
Emily A. Deere	Executive Director, IT Applications Group, Administrative Computing and Telecommunications	UC San Diego	6/24/2009
Kristina L. Larsen	Assistant Vice Chancellor, Academic Affairs	UC San Diego	6/24/2009
Patricia L. Price	Assistant Vice Chancellor, Academic Affairs	UC Irvine	6/24/2009
Joan K. Tenma	Director, Academic Personnel	UC Irvine	6/24/2009

Periodic Review

This Agreement is valid from the Effective Date outlined herein and is valid until the Date of Termination. This Agreement should be reviewed a minimum of once per fiscal year; however, in lieu of a review during any period specified, the current Agreement will remain in effect.

The Business Relationship Manager (“Document Owner”) is responsible for facilitating regular reviews of this document. Contents of this document may be amended as required, provided mutual agreement is obtained from the primary stakeholders and communicated to all affected parties. The Document Owner will incorporate all subsequent revisions and obtain mutual agreements / approvals as required.

Business Relationship Manager: Max Garrick

Review Period: Yearly

Previous Review Date: N/A

Next Review Date: N/A

I. Agreement Overview

This is a Service Level Agreement (“SLA” or “Agreement”) between UC Irvine Network & Academic Computing Services (“Service Provider”) and UC San Diego Administrative Computing and Telecommunications (“Customer”) for the provision of IT services required to support and sustain the AP Recruit system (“System”).

This Agreement will be posted to the following location and will be made accessible to all stakeholders:

http://www.nacs.uci.edu/docs/agreements/ap_recruit/sla-ucsd.pdf

II. The System Provided by the Service Provider

1. Overview

During the term of this Agreement, the Service Provider agrees to provide the Customer with access to its Internet-based Recruit system (“System”) for managing online recruitment of senate-level faculty positions and diversity survey/reporting for all professorial positions. The user base of the System includes the UC San Diego campus staff, faculty, applicants, and references.

2. System Environment Scope

The System will provide three environments, each with different scope, support coverage, and user base.

Environment	Support Coverage	User base	Scope
Production	24/7	UCSD campus, applicants,	Manage recruitments that have been

		and references	approved by the AP office
Training	8-5 M-F	AP analysts	Training and experimentation
Development	8-5 M-F	IT staff	Development & testing

3. IT Support and Emergency Response

The Service Provider will provide "last line" telephone and email support to the Customer. No end users will be supported by the Service Provider. The Customer will make every effort to answer support inquiries and address issues discovered at their campus. After all avenues have been explored by the Customer, they may contact the Service Provider for assistance.

Available support communication mechanisms:

- Telephone support is available at (949) 824-2222. Emergency support is provided 24/7 and non-emergency support is provided 8-5pm Monday - Friday excluding UC holidays. Emergencies include service disruptions where a significant number of users (usually 10) cannot access the System or failure of nightly data batch load. Non-emergencies include all other issue reports and inquiries.
- Email support is available 8-5pm Monday - Friday at recruit@uci.edu . Email support is provided for non-emergency use only -- for all emergencies use telephone support since staff only monitors email 8-5pm Monday - Friday.

Support response times:

- Inquiries will be responded to within 1 business day. If programmer support is required to answer an inquiry, please allow up to 3 business days for successful resolution. An inquiry is defined as questions about the system or requests for information.
- Enhancement requests will be tracked in SFEE and made available to the collaboration for scheduling and completion. Enhancement requests are defined as improvements or changes to a System that is working as designed. The collaboration is responsible for determining priority, staff resources, and requirements. The Service Provider participates in the collaboration, however is not solely responsible for completing enhancement requests.
- Issues reported will be responded to within 1 business day and resolved within a total of 5 business days unless issue is reported during a critical window¹. Issues reported during a critical window will be resolved as soon as possible. Issues are defined as problems that occur because the System is not working as designed.

¹ Critical window – defined as the week preceding fiscal closing (June 30) and week following any major software release.

24/7 emergency response procedure:

1. The Customer will call the NACS Response Center (949) 824-2222.
2. The Customer will provide the Response Center with the following information.
 1. Need: immediate response to emergency situation.
 2. URL: affected AP Recruit website.
 3. Customer name.
 4. Customer telephone number: the System's technical contact will call this number with status updates.
 5. Problem description: description of the incorrect/undesirable behavior.
3. The Response Center will contact the System's technical contact(s).
4. The technical contact will resolve the issue ASAP and notify the Customer.
5. If the issue is not resolved within 30 minutes, the technical contact will provide a status update to the Customer.

The Memorandum of Understanding ("MOU") between Service Provider and Customer encourages the collaborative development of new System releases. This includes new development that resolves issues or enhances the System. Please refer to the MOU for more information.

4. End-user Support Strategy

The System has a built-in delegated support structure. The Service Provider is responsible for the Service Provider's end-user support and the Customer is responsible for the Customer's end-user support.

Business-related help: configurable by the AP analyst responsible for the recruitment.

- Applicants & references: routed to the position's "Help Email Address".
- Faculty and administrators: routed to the recruitment's "Recruitment Contact Email".

Technical or general help: routed to Customer's technical support email address.

- If business-related, route question to appropriate business-related help.

In general, end-user support elevates accordingly:

- Faculty contact committee chair
- Committee chair contacts department analyst

- Department analyst contacts school analyst
- School analyst contacts Customer IT help
- Customer IT help contacts Service Provider

Typical business hours are Monday – Friday 8am-5pm, excluding campus holidays.

5. Reasonable Service Level

The Service Provider recognizes that unplanned downtime and reliability issues may adversely affect the Customer and will take precautions to minimize downtime and performance problems. The Service Provider will perform automated fault and performance monitoring. All Customer data will be replicated to a failover system and backed up nightly.

The System yearly uptime target is 99.9%, excluding scheduled maintenance and network/power outages outside of the Service Provider's control.

6. Release and Maintenance Management

The Service Provider is responsible for maintaining the System's underlying infrastructure. It is important to provide the Customer with advance notice of any maintenance or non-trivial releases as they may adversely impact the Customer's users. It is also important that the Service Provider work around any critical windows where the Customer needs the System to be available. In order to effectively schedule and carry out important maintenance or releases, the Service Provider will ask the Customer to report concerns by a specific date. After this date, the Service Provider will assume no concerns and proceed with required work.

The Service Provider will send a notification of upcoming service downtime at least 5 days in advance and accept Customer concerns for at least 3 days. This notification will include the following information:

- Description of maintenance to be performed
- Date / time of downtime
- Duration of downtime
- Contact information
- "Report any concerns by" date

The Service Provider will notify the Customer of non-trivial releases 30 days prior to scheduled launch date and accept Customer concerns for at least 10 days. A non-trivial update is defined as any work that requires more than 30 days to complete. This notification will include the following information:

- Description of update, enhancement, or major bug fix
- Date / time
- Extend of downtime (if any)
- Contact information
- "Report any concerns by" date

In the case of required emergency maintenance (e.g.: patch that resolve exploitable security vulnerabilities), the Service Provider will make every attempt to notify the Customer and then perform the maintenance. This decision to perform maintenance with little to no warning will be balanced against the cost of service disruption for all Customers, and must resolve a significant problem.

7. Documentation

The Service Provider will make the latest version of help & how-to and training material source files available in response to Customer requests.

8. Automated Data Updates

To facilitate automatic and regular updates of data, the System will accept feeds for the following data:

- Directory: user attributes, including name, email, department, and more.
- Authorization: user-role-resource relationships.
- Schools & departments: names of each campus unit and any parent/child relationships.
- Titles: codes and names of Customer faculty titles used to determine eligibility for online application management.
- Specialties: codes and names of Customer specialties used to determine availability pools for diversity reporting.
- Availability data: used in generating diversity reports.

To facilitate the real-time update of authorization data, the System will provide an API for updating Authorization data.

III. Customer Responsibilities

Customer responsibilities and/or requirements in support of this Agreement include:

1. Deliver data required for the correct operation of the System.

2. Provide necessary user interface elements in order to maintain a campus-branded System.
3. Perform any required security audits to ensure the System meets security standards.
4. Provide end-user support.
5. Customize/brand any training documentation.
6. Develop and execute a training program.
7. Initiate any required pilot programs
8. Other items needed to support the System.