



**Staff /Faculty – AD & Oracle Self Service
 User Registration Form
 Network & Systems Operation
 Telephone: 619-260-4726 / Fax: 4235
 Please return this form to Maher Hall, rm #170**

Section One: Registration Section – For all requests (please print):

Name: _____ Phone: _____ Temp Emp?: YES or NO End Date: _____
 (Ex: Work-study, Casual Worker, Intern, etc.)

Dept: _____ Building/Room: _____ E-mail Address: _____

Section Two: Department Drives / Personal Home Drive:

1) (optional) Departmental Network Drive (ex. W: \\adpwnfwinapps): _____

2) (optional) Shared drives like another user has or same as <user>: _____

3) (optional) Personal Home Drive (ex. H:\Home): (YES / NO)

4) (optional) VPN Account: (YES / NO)

5) Do you have an existing account on any other USD computer system?

a) If so, please circle all that apply: AD, VPN, Wellness, Oracle, Banner, Xtender

b) Your Existing User Account name: _____

Please circle all that apply for Oracle Access

USD Employee Self Service: (YES / NO) USD Manager Self Service: (YES / NO)

Oracle Access same as <user>: _____

The information on this form is true and complete to the best of my knowledge. I have received a copy of the Usage Guidelines & Policies.

User Signature: _____ USD ID #: _____ Date: _____

Authorizing Signature is Required:

Immediate Supervisor:

Title: _____

Print Name: _____

Signature: _____



**5998 Alcalá Park
San Diego, CA 92110**

ITS Guidelines and Policies

Use of university computing resources is limited to authorized users only. Any suspicious activity or attempt to gain unauthorized access to this System or Network should be reported immediately to:

Network and Systems Operation
Maher Hall Room 170
Telephone 619-260-4726

1. Read policy for responsible use
<http://www.sandiego.edu/legal/policies/community/technology/computing.pdf> .
2. Each system user is assigned a unique user login name and password.
3. The login name and password must be kept confidential at all times. This information must not be shared with anyone including co-workers.
4. Each user is responsible for protecting their own user login name from unauthorized access. User workstations must never be left unattended while logged on.
5. Passwords must be at least 8 characters in length and contain at least 1 number special character OR 1 UPPERCASE character.
6. Passwords must not contain the user name (ex. User: JohnD, password ljohn# won't work).
7. Users will be required to reset their passwords every 90 days.
8. If departing USD, the employee/user or their supervisor is required to notify Network and Systems Operation regarding disposition of the user account. To make arrangements call Yolanda Abitan at extension 4726 or abitan@sandiego.edu or contact the Help Desk at extension 7900 or tsc@sandiego.edu . A clearance form must be signed by the Operations Manager. Contact HR for clearance form.

I have read the policy on responsible use of university computing resources.

Signature _____ Date _____

Print Name _____