

Employee Last Name: _____

Employee UCD Email: _____

Advance Security and Use Statement

Please send completed form to the DEVAR Helpdesk (fax 754-1156)

I understand that in the performance of my duties at UC Davis, I must hold information in confidence. I have read and understand the Acceptable Use Policy. I understand that unauthorized disclosure of personal/confidential information may result in charges of Invasion of Privacy.

I understand that it is against UC Davis and Development & Alumni Relations policy to seek out or use personal or confidential information relating to others or make use of University equipment or software for my own interest or advantage. I understand that it is also against UC Davis and Development & Alumni Relations Policy to access private data belonging to other users without their express consent.

I understand that the Advancement Information System (AIS), Michelangelo, and the data contained therein are the property of The Regents of the University of California, and are for official University Business only. No release of this information may be made to outside organizations or persons without written authorization. No use of this information may be made following the termination of University employment.

I am aware that the References and Related Policies on page 3 outline University policies and State and Federal laws governing use of computer systems and disclosure of information. Violation of local, state, or federal statutes may carry the additional consequence of prosecution under the law, where judicial action may result in specified fines or imprisonment, or both, plus the costs of litigation or the payment of damages, or both.

I acknowledge receipt of a UC Davis Development & Alumni Relations computer access code (user id) and password and understand that I will be responsible for all entries made thereunder. I understand that my user id and password are to be accorded the same significance as my handwritten signature and that the delegation of my user id and password to another person, or my use of another person's user id, may be considered False Representation.

I understand that under California State Law any person who maliciously accesses, alters, deletes, damages, or destroys any computer system, network, computer program, or data is guilty of a felony. I understand that failure to comply with these regulations may result in disciplinary action, which could include release from employment.

In order to have Advance access, users must also complete HIPAA training. Please visit lms.ucdavis.edu and search for Privacy and Security Training (eCourse) – DAHS-CDPST10. Upon finishing the training you will get a certificate of completion. **Please submit your certificate of completion with this signed security acknowledgement form.**

By signing below, I certify that I have viewed and understand the content of the Security Video located on the Advancement Services website.

Employee
Signature: _____

Date: _____

Print Name: _____

Job Function: _____

This Security Form grants access Advance Web; please watch the appropriate training videos and submit pages 1 (security page) & 2 (training acknowledgement) of this document.

.....
I authorize access to Advance Web for the employee named above and have verified that this employee has watched and understood the content of the AIS Security video, as well as the training videos associated with his/her needed access.

In accordance to UC Davis draft policy on Access to Institutional Data (PPM 320-24), when an employee vacates the position held in conjunction with his/her currently approved access to institutional data, his/her supervisor or department head shall communicate such status change to the DEVAR Help Desk devarhelpdesk@ucdavis.edu or (530) 754-1106 . Based on the changed status, the AIS Security Manager will take the appropriate action, which may include revoking access.

Supervisor's Signature: _____

Date: _____

Print Name: _____

Dept/Unit: _____

Official Use Only:

Unit/School/College	End Date (Temporary Employees ONLY)	Ais-Director Signature
Campus Login Id/Username	AIS Entity Id #	Notification re: Account Creation
Phone	Advance User Profile Date	Login Check Date
Permissions (based on training videos & need)		

Training Acknowledgement for Advance Web Access

All videos can be found at <http://ais.ucdavis.edu/learningcenter/systemaccess.html> or by going to ais.ucdavis.edu, mouse over the Learning Center tab and clicking on Advance Web. Once there, click on Advance System Access found in the menu on the left side of the screen.

Report Only Access:		Inquiry Access:	
Prerequisites: <ul style="list-style-type: none"> • Keberos Access • Viewed the security video 	Videos: <ul style="list-style-type: none"> <input type="checkbox"/> Introduction to Advance <input type="checkbox"/> Navigation in Advance <input type="checkbox"/> Lookups Pt 1 <input type="checkbox"/> Lookups Pt 2 <input type="checkbox"/> Entity Overview <input type="checkbox"/> Advance Web Reports 	Prerequisites: <ul style="list-style-type: none"> • Reports Only Requirements • Reports Only Training 	Videos: <ul style="list-style-type: none"> <input type="checkbox"/> Entity Lookup Video

Maintenance Access:		Development Officers Access:	
Prerequisites: <ul style="list-style-type: none"> • Inquiry Access Requirements • Inquiry Training 	Videos: <ul style="list-style-type: none"> <input type="checkbox"/> How to Add a New Entity Record <input type="checkbox"/> How to Add an Address <input type="checkbox"/> How to Add a Telephone <input type="checkbox"/> How to Add an Email Address <input type="checkbox"/> How to Add a Web Address/Social Media Information <input type="checkbox"/> How to Add an Alias and/or Nickname <input type="checkbox"/> How to Create a Contact Report 	Prerequisites: <ul style="list-style-type: none"> • Maintenance Access Requirements • Maintenance Trainings 	Videos: <ul style="list-style-type: none"> <input type="checkbox"/> DO Home Page <input type="checkbox"/> Quick Links <input type="checkbox"/> Entity Overview Screen <input type="checkbox"/> Prospect Overview Screen <input type="checkbox"/> Proposal Overview Screen <input type="checkbox"/> Left Hand Navigation Tree

<input type="checkbox"/> HIPAA Training Course

If PMATS access is needed, please refer to the PMATS section of the Development Officers Toolkit (DOT).

I acknowledge that I have watched the above Advance training materials that pertain to my job function. I understand that I am responsible for all entries made thereunder.

Employee
Signature: _____

Date: _____

Print Name: _____

I acknowledge that the above employee has watched the above videos that directly pertain to their job function. I authorize the appropriate security rights and profile be assigned to this employee in Advance Web to perform their job function.

Supervisor's Signature: _____

Date: _____

Print Name: _____

Dept/Unit: _____

<p>RULES FOR CONDUCT - UNIVERSITY EMPLOYEES INVOLVED WITH INFORMATION REGARDING INDIVIDUALS</p> <ul style="list-style-type: none">A. Employees responsible for the collection, maintenance, use, and dissemination of information about individuals which relates to their personal life, including employment and medical history, financial transactions, marital status and dependents, shall comply with the State of California Information Practices Act. PPM-320-20 shall be used as a basic guide in administering the Act's provisions.B. Employees shall not require individuals to disclose personal or confidential information about themselves which is not necessary and relevant to the purposes of the University or to the particular function for which the employee is responsible.C. Employees shall make every reasonable effort to see that inquiries and requests by individuals for their personal or confidential records are responded to quickly, courteously and without requiring the request to repeat the inquiry to others unnecessarily.D. Employees shall assist individuals who seek information pertaining to themselves in making their inquiries sufficiently specific and descriptive so as to facilitate locating the records.E. Employees shall not disclose personal or confidential information relating to individuals to unauthorized persons or entities. The intentional disclosure of such information to such persons or agencies may be cause for disciplinary action.F. Employees shall not seek out or use personal or confidential information relating to others for their own interest or advantage. The intentional violation of this rule may be cause for disciplinary action.G. Employees responsible for the maintenance of personal and confidential records shall take all necessary precautions to assure the proper administrative, technical, and physical safeguards are established and followed in order to protect the confidentiality of records containing personal information and to assure that such records are not disclosed to unauthorized individuals or entities.H. Employees shall respond to inquiries from individuals, and requests from them to review, obtain copies of, amend, correct, or dispute their personal records in a courteous and business-like manner, and in accordance with PPM-480-3.	<p>REFERENCES</p> <ul style="list-style-type: none">A. Policy and Procedure Manual (PPM 320-21) Responsibilities and Guidelines for Handling Records Containing Information about IndividualsB. University Policy, Guidelines, and Legal Requirements on Privacy of and Access to Information, June 9, 1978C. University Policies Applying to the Disclosure of Information from Student Records, February 1, 1977D. California Public Records Act (1976)E. California Information Practices Act (1977)F. California Education Code, Chapter 1.2 Division 16.5G. California Penal Code, Section 502, Chapter 858, relating to Computer CrimeH. Federal Privacy Act of 1974I. Federal Family Education Rights and Privacy act of 1974J. Electronic Communication Privacy Act of 1986 <p>RELATED POLICIES</p> <ul style="list-style-type: none">A. POLICY AND PROCEDURE MANUAL (PPM)<ul style="list-style-type: none">a. 320-All Records and Archivesb. 380-25 Disclosure of Information from Personnel Recordsc. 200-45 Administrative Information Systemsd. 260- All Gifts and EndowmentsB. BUSINESS AND FINANCE BULLETIN<ul style="list-style-type: none">a. RMP-8 Legal Requirements on Privacy of and Access to Informationb. IS-3 Electronic Information SecurityC. INFORMATION TECHNOLOGY POLICIES<ul style="list-style-type: none">a. Acceptable Use Policy 12/15/98
--	--