UCF Stands For Opportunity

UCF Account/Access/Termination Request Form

This form is for requesting an institutional account, access to network resources, or application level access for associates, consultants, contractors, or guests of the University of Central Florida. Account or access requested will need a University sponsor (head of business unit, department, faculty, administration, etc.) and granted for persons for official university business.

Once the form, with all the required fields completed, is submitted, please allow 5 to 10 business days for processing and verification. In some cases training may be required before access is granted. Access terminates after midnight on the end date specified in section two of this form. The maximum length of time allowed for the account or access is 1 year. The sponsor must submit a new request form prior to the end date to avoid disruption of service. It is also the responsibility of the sponsor to immediately submit this form (complete section 1 and 3) for termination of access if the account/access is no longer required prior to the specified end date.

The privacy of student and employee information is protected by University, State and Federal laws. Access granted to University resources might be protected, but not limited to the following laws or standards: Family Educational Rights and Privacy Act (FERPA), HIPAA, PCI DSS, GLBA. Moreover, UCF imposes its own policies and standards regarding the safeguarding of the University assets. Please review the policies governing the use of UCF's institutional data and computing resources at www.policies.ucf.edu. Standards governing computing resources are found at www.infosec.ucf.edu

Please complete each section and fax it to the Information Security Office at 407-882-9006.
Allow 10 business days for full completion.
All fields outlined in red, in necessary sections are required.

Requested Date

Request Type New (complete sections 1 - 6)

Section 1: Individual needing an account or access to University resource:

Last Name: First: Middle:

Company Name (if applicable):

Position with Company (if applicable):

Daytime Phone: Cell Phone:

Address:

City: State AL Zip:

Email:

UCF Employee ID (if applicable, renewal/termination):

The following data fields are required in order to prevent creation of duplicate accounts. All information will remain confidential.

Date of Birth Gender Male

Section 2: University account, access or resource requested:

- ☐ PeopleSoft Access (complete all sections, sign and return. FERPA course SR100W and a basic navigation course will be required before working with institutional data (academic records.))
- ☐ Access to Institutional Data (e.g., academic records) outside of PeopleSoft (complete all sections, sign and return. FERPA course SR100W will be required before working with institutional data (academic records.))
- ☐ Access to Human Resources Data (complete sections 1, 3, 5 & 7 with HR's DSC approval)
- ☐ College/Departmental Server (complete sections 1, 3, 5, &7)
- ☐ VPN (Virtual Private Network) for remote access (complete sections 1, 3, 4, 5, & 7)
- ☐ Wireless access on campus (complete sections 1, 3, & 7)
- ☐ Enterprise e-mail account (complete sections 1, 3, & 7)

Purpose for request (include general statement of business reason for access; specify if access will be required to systems and type of data, etc.): If more room is needed, please attach a separate form.

Access Begin Date _____ End Date _____ Maximum length of 1 year from begin date.

Section 3: University sponsor (unit head, faculty, admin, etc.) for requested account/access:

I understand that is my responsibility to submit a termination of access request immediately, if this access is no longer required prior to the specified end date. I understand that a new request must be submitted to extend an account beyond the expiration date.

Last Name: _____ First: _____ Middle: _____ Last 4 digits of EmplID _____

Title: _____ Dept.Name: _____ Dept. #: _____

Campus Address: _____

Campus Phone: _____ Campus Email: _____

Sponsor Signature _____ Date _____

Section 4: Details of the computer system(s) being accessed (if necessary):

If the account you are requesting will be used to access computer systems and resources on the UCF network, please provide the details of that resource you will be accessing below.

Computer Name _____ IP Address _____ OS _____

System Administrator _____ System Admin Phone # _____

Network service(s) used _____ (Windows Share, SSH, sFTP, on campus SSL website, http, https, etc.) Building/Room _____

Section 5: College/Departmental Security Coordinator (DSC) Authorization (if necessary):

Departmental or College Security Coordinator must review the requested access if it involves their departmental system(s) and impose access limitations when applicable to mitigate risk to university data: (you can find DSC information here: http://www.infosec.ucf.edu/dsc)

Last Name _____ First _____ Middle _____

Department _____

Campus Email _____

DSC Signature _____ Date _____

Section 6: Institutional Research Authorization (if necessary):

Access to institutional data (e.g., academic, etc.) will require authorization from the University Data Administrator or designee.

University Data Administrator, or designee, name: _____

University Data Administrator, or designee, signature: _____

Section 7: Requestor confidentiality and non-disclosure agreement:

The undersigned UCF associate, consultant, contractor, or guest in the course of their relationship with UCF may have access to or acquire confidential personally identifiable information, including but not limited to student and/or employee names, addresses, telephone numbers, bank and or credit card numbers, social security numbers, and income and credit history.

The signee acknowledges his or her responsibility to abide with for various State and Federal regulations regarding privacy and security of confidential information maintained by the University, including the Family Educational Rights and Privacy Act (FERPA), the Payment Card Industry Data Security Standards (PCI DSS), the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), and the State of Florida Statutes on identity theft, and agrees to cooperate, and shall cause its officers, employees, agents, and subcontractors to cooperate with the University, as necessary, to comply fully with these legal obligations.

The signee agrees to keep confidential all student academic records, employee personnel records, and other personally identifiable information that is deemed to be confidential in accordance with applicable Federal, State and University laws and policies.

The signee declares his or her capability of safeguarding any confidential information accessed or viewed. Signee agrees to implement such safeguards that may be necessary to maintain the security and confidentiality of all information accessed or viewed, and to prevent the disclosure of the information except as required by law.

Signee shall indemnify, protect, defend, and hold harmless the University and its trustees, officers, agents, employees, representatives, and the State University System of Florida and its governors, officers, agents, employees, representatives, and against any and all claims, demands, suits, and causes of action and any and all liabilities, costs, damages, expenses, and judgments, incurred in connection therewith relating to or arising out of unauthorized use or disclosure of confidential information.

Signee will immediately report to the University any unauthorized use, access, or disclosure of confidential information.

Signature: _____ Date: _____

NOTE: Account information and initial credentials will be e-mailed to the sponsor unless the intended individual already has a UCF e-mail address.