

Computer Accounts Request

Please fill out form completely, including UIN and required signature at the bottom. Incomplete forms will be returned to you. Please attach proof of completion of the HR Online Information Security Awareness Training Course.*

A = Data required to request a new account that's never before existed, additional access or update.

B = Data required to **inactivate** an existing account.

Use the Up/Down and Left/Right arrows to move into the form.

(Additional instructions for this form are on page 2.)

A	B	Data Requested	Type your answers here
√	√	Employee Name (Eg: Dr. John A Smith Jr.)	
√		Universal ID Number (UIN) *	
√		Existing Banner ID number (A-Number)	
√		Date of Birth	
√		TAMU-CC phone ext.	
√		TAMU-CC Department :	
√		Building and room number	
√		Department Unit number: ZIP 4	
√		Non-TAMUCC Email account or Cell Number/Carrier	
√		Create Active Directory, Exchange email (Y/N)	
√		Banner Access Request-(Separate Form) Use link to download request form	https://ca11.fw.tamucc.edu:9191/banner_account_request.html
√		Linux/Falcon web development (Y/N) Student Workers will no longer be Assigned falcon Accounts. (**)	
	√	User IDs to inactivate/UIN	
√		Employee's Job title	
For NEW accounts, check the appropriate box, (check only one):			
√		Faculty	Research & Grad/Tech Asst
√		Staff	Contractor (***)
√		Temp Worker	Guest
√		Student Worker	Volunteer
If the account needs access to shared data directories, or if you have ANY ADDITIONAL COMMENTS, list them below. If you need shared drive access, please list what type of access (read only, read/write)			
	√	Additional Comments:	
√	√	Effective date	
√	√	Authorizing Agent's (supervisor) name	
√	√	Authorizing Agent's (supervisor) title	
√	√	Agent's (supervisor) HAND signature	

*Please direct any questions about online security training and/or UINs to Human Resources, 825-2630.

**Student workers will no longer be given access to Falcon. Student Linux accounts can be set up in the Student Computer Labs, or by logging onto <https://newuser.tamucc.edu>. Student Linux accounts are hosted on the Islander Student e-mail server.

*** Please direct any questions about Contractor/Affiliate UIN's to Accounts Admin, 825-2691.

***** Additional Instructions *****

You may type directly onto the fields of this Account Request form. You **do not have** to type onto them. You may print the form and then fill in the form with a pen. Remember to date the form and obtain necessary signatures. Please fill out the form completely or it will be returned to you and processing may be delayed. Print the appropriate pages of this form to your local printer.

Send the completed form to:

Information Technology
Attn: Accounts Admin
CCH 105A
Unit 5748

Or fax to: X-2366

After Accounts Admin receives your request they will assign it to the appropriate personnel. New accounts may take up to 3 days to create. When the account is created you will again be notified to pick up your new account information at Accounts Admin. Questions about this form may also be addressed to the Help Desk at extension **2692**.

***** Please note *****

Effective Spring 1996, all employees who use computers must sign a “**University Information Resources Security Acknowledgement pledge**” One is included on the next page. If you've already signed one, you need not sign another.

Texas A&M University-Corpus Christi

University Information Resources Security Acknowledgement

By signing this document, I acknowledge my awareness of and concurrence with all of the Texas A&M University - Corpus Christi Rules and Procedures regarding information resources which can be viewed at http://academicaffairs.tamucc.edu/Rules_Procedures/. In particular, I acknowledge that:

• University Passwords

I will log into the University network with only the username and password given to me by the University.
I will keep my University password private and not reveal it to anybody else for any reason.
If I have reason to believe that someone else has learned my password, I must 1) change the password immediately and 2) notify the Office of Information Security.

• Authorization

I will access only those information resources and data to which I am authorized by the University.
I will conduct only those transactions that I am authorized by the University to conduct.

• Confidential and University-Sensitive Information

I will protect the University's confidential/sensitive information in accordance with University Procedure 29.01.03.C2.28 - Classification and Protection of Data.
I will access or otherwise use such data 1) only when explicitly authorized to do so, 2) only in the authorized manner, and 2) only for legitimate University-business or academic reasons.
I will not copy such data onto a portable device or non-University machine unless authorized and absolutely necessary, and if I do so I must encrypt the data.

• Acceptable Use/Incidental Use/Privacy

I will keep personal use of University information resources to a minimum.
I understand that anything I store on a University information resource and anything I send or receive via the University network can be examined by authorized University personnel.

• Workstation Security

When I leave a workstation, I will log myself out of the workstation, shut down the workstation, or lock the desktop.

• Incident Reporting

I will report any weaknesses in the security of the University's information resources or any incidents of possible misuse or violation of this or any other policy to the Office of Information Security ois@tamucc.edu).

• Penalties

I understand that by violating any aspect of this pledge, I may be subject to University disciplinary action and criminal prosecution to the full extent of the law. (Chapter 33, Section 1, Title 7 of the Texas Penal Code.)

Name (print clearly)

Date

Signature

Universal ID Number (UIN)

Title

Department

Witness (print clearly)

Signature

Date