California State University

Division Of
TECHNOLOGY & COMMUNICATION
CHANNEL ISLANDS

Telecommuter Information Security Review

NOTES: See instruction page. This form may accompany a VPN access form. Fill this form out as completely as possible.

Contact Information

	VPN User	Appropriate MPP Administrator
Name		
Department		
E-mail Address		

Storage of Protected Data

Question	Yes	No
(1) Do you require the local storage of protected data in order to telecommute? Note that ***accessing*** protected data, such as the remote use of CMS, is ***not local storage***.		
(1a) If yes, describe the specific means you will use to secure the locally-stored data:		
(2) Will you need to print out protected data in order to telecommute?		
(2a) If yes, describe the specific means you will use to protect the printed data from unauthorized access or disclosure, including how you will destroy the data when it is no longer required.		

Computer Use

Question	Yes	No
(1) Do you require access to the VPN in order to telecommute? (If yes, complete and include a VPN Access Form.)		
(2) If you answered 'yes' above, will you use a University-issued computer to access the VPN?		
(3) If you answered 'no' to question (2), please describe the specific hardware and software you will use with the VPN. Note that your configuration is subject to the review and approval of the Information Security Officer and VP for Technology & Communication. Include: Hardware brand and model number MAC address Operating System and version Antivirus Software and version		

Telecommuter Information Security Review

I certify that this information accurately represents my use of protected data and VPN while telecommuting. I agree that I will notify the T&C Help Desk immediately if there are any changes to the information on this form.

____ __________
Signature of Employee Date

I have reviewed this information with my employee, and determined that the above safeguards, as required, are sufficient to protect the University. I have attached, or otherwise provided, a written business justification for the storage of Level 1 and Level 2 data by the telecommuting employee.

____ __________
Signature of Appropriate MPP Administrator Date

FOR T&C ADMINISTRATION USE ONLY

Administrative Review	Approved Disapproved	Signature	Date
ISO			
VP for T&C			

California State University

Division Of
TECHNOLOGY & COMMUNICATION
CHANNEL ISLANDS

Telecommuter Information Security Review

Instructions

Fill this form out as completely as possible, and submit it to the T&C Help Desk. Incomplete forms may result in delays. If you have questions about this form, please contact the Information Security Officer or the T&C Help Desk for consultation.

Consult T&C Business Practice BP-03-004, available at www.csuci.edu/tc/policy.htm, for details on T&C standards regarding the use of the Channel Islands VPN. Consult the Interim Policy on Responsible Use, IT.03.001, for details on acceptable use of T&C network resources.

Contact Information

Your Division executive’s approval is required for the storage or printing of Level 1 and Level 2 data by telecommuting employees. For all other employees, ‘Appropriate MPP Administrator’ means your MPP supervisor.

Storage of Protected Data

“Protected data” means data that is defined as Level 1 or Level 2 by the CSU Data Classification Standard. Please consult University Policy IT.01.001, available at policy.csuci.edu, for definitions of Level 1 and Level 2 data.

Computer Use

Except as authorized by the Information Security Officer and VP for Technology & Communication, only University-owned and –managed computers may be used on the Channel Islands VPN. Do not complete Block 3 of the Computer Use section unless you will use a non-University-owned computer to access the VPN.

To gather the information required by Block 3 of the Computer Use section, consult your hardware, operating system, and antivirus software documentation.