Business Practice for Telecommuting Computer Use

PURPOSE:

To protect the confidentiality, integrity and availability of CSU Channel Islands' information assets by ensuring that telecommuting users take adequate measures to secure their computers and workstations.

BACKGROUND:

Government Code Sections 14200-14203 authorize every State Agency to incorporate telecommuting as a work option. CSU Channel Islands has been delegated authority to establish a telecommuting program within this authority. The University policy is located at http://policy.csuci.edu (policy FA.31.014 – Policy on Telecommuting).

Telecommuting presents particular information security challenges. Telecommuters must access University ITS resources via untrusted and possibly unsecured networks. Additionally, the fact that telecommuters are not physically on campus means that physically securing access to the University's ITS resources may not be technically practicable.

This Business Practice implements information security-related provisions of the CI Policy on Telecommuting.

BUSINESS PRACTICE: Accountability:

Applicability: All

telecommuting users

Definitions:

1) **VPN:** Virtual Private Network. The remote access service provided by ITS through our VPN portal.

Business Practice for Telecommuting Computer Use

Text: *All*

users

All users who telecommute must take adequate measures to protect the confidentiality of the University's data. Pursuant to the Policy on Telecommuting, information classified as Level 1 – Confidential or Level 2 – Internal Use by the CSU Data Classification standards must be protected against unauthorized disclosure by password and encryption if stored on a home computer of the telecommuter. Additionally, this data must only be transmitted by VPN. Storage or transmission of Level 1 and Level 2 data by a telecommuting user must be specifically approved in writing and in advance by the appropriate administrator, the CISO, and the AVP for Information Technology Services.

The campus reserves the right to inspect any software and hardware used by the telecommuting employee to access or store Level 1 or Level 2 data.

For users that require VPN access

Telecommuting users whose job functions require VPN access to Channel Islands' ITS resources must use University-owned and –managed computer equipment to protect the integrity of the campus network. Equipment used by the telecommuting user to connect via the VPN must be reviewed in writing by the CISO, and the AVP for Information Technology Services. The CISO and AVP for Information Technology Services may grant deviations to this paragraph in writing if they can determine that an equivalent level of security exists and can be maintained using non-university equipment.

Non-regular employees, such as contractors, must receive the approval of a Channel Islands MPP to access the VPN. Such users must also have Dolphin Names and ID numbers. Contractor access to the CI VPN is reviewed every 90 days.

ITS Infrastructure will employ technical means to exclude non-University-owned or otherwise approved computers from the VPN.

VPN users agree to sustain a level of security patches to keep the endpoints secure.

Business Practice for Telecommuting Computer Use

Exhibits:

Policy on Telecommuting (Finance and Administration)
CSU Data Classification Standard

Assessment Requirements

Assessment requirements and history are listed in the grid below.

Description	Frequency	Role Assigned	Date Completed
Contractor VPN access review	Every 90 Days	Director, Infrastructure	99/99/9999

Revision History

BP Nbr:	BP-03-004	**Enacted Date:**	08/10/2010		
Revision Nbr:	001	**Revision Date:**	02/02/2017	**Revised By:**	N Fisch
	002		01/02/2024		C Miranda