Campus International Travel Policy

CSU Bakersfield Policy

Document Number:	ITS-90.022	**Last Revision Date:**	
Responsible Office:	Information Technology Services	**Effective Date:**	11/1/2021
Primary Author:	CIO & AVP of Information Technology		

General Description

Purpose:

Traveling internationally can pose significant risks to information stored on or accessible through computers, and smartphones. Some of the risk is associated with increased opportunities for the loss or theft of the device and just merely the distraction of traveling. Additionally, our devices are put at risk because they will use networks that may be managed by entities that may monitor and capture network traffic for competitive or malicious purposes.

Definition:

Disk Encryption - Is a technology which protects information stored on a hard drive by converting it into unreadable code that cannot be deciphered easily by unauthorized people. Disk encryption uses disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume.

Virtual Private Network (VPN) - A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

Scope:

This policy applies to all CSUB departments, employees, and auxiliaries. For anyone who is accessing CSUB data from a state-owned or personal device when traveling abroad.

Policy/Procedure

When traveling to any location outside of the United States you must observe the following security practices:

- If you hae accevss to level one or two data, any state-owned computer must have its disk encrypted to prevent disclosure.

Data Classification Standard Policy # 8065.00 Data Classification Standard

- Any time you are accessing campus data across the internet you must utilize the campus Virtual Private Network (VPN) solution Global Protect.

Before departing, please coordinate a visit with the CSUB Service Center or call at 661-654-HELP to ensure the device(s) you intend to travel with have Local Disk Encryption and Global Protect installed and working before your trip.

Encryption Controls

Disk encryption and VPN software are critical tools to help protect your data from compromise. However, many foreign countries do not permit encryption software to be imported or used without prior approval. For example, China requires international travelers to apply for a license to use encryption software before arrival.

To learn more about the laws in the country you are planning to visit see:https://www.gp-digital.org/world-map-of-encryption/. If you are not able to use encryption software at your destination, it is strongly recommended to leave your data and device at home and bring a loaner device instead. Contact the ITS Security office informationsecurity@csub.edu for advice.

Additional Information

How to use the Global Protect VPN: https://csub.service-now.com/sp?id=kb_article&sys_id=7b3aa913dbe5e30069c77b5b8c9619ba
U.S. Office of Counterintelligence advice on overseas travel with personal devices:
https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-travel-tips
If you have questions, please contact the CSUB Service Center at 661-654-HELP.

Review (Frequency and Process)

This policy should be reviewed and updated if needed on a biannual basics by the Information Security Officer (ISO) and/or the Chief Information Officer (CIO) or a designate and provided to the Vice President Business and Administrative Services for approval and then to Cabinet for final approval.