UNIVERSITY OF CENTRAL ARKANSAS™ | INFORMATION TECHNOLOGY

COMPUTER USE OUTSIDE OF THE UNITED STATES

RATIONALE

The Division of Information Technology (IT) at UCA must maintain the integrity and security of all UCA owned technology assets and data. Traveling outside of the United States poses a large number of risks in terms of technology assets including data loss, malware injection, hardware and software security compromises and thus exposes UCA liability.

This policy is subject to revision annually or as needed.

SCOPE

This policy applies to all technology assets owned by the University.

POLICY

A. Related Policies and Laws

This policy does not supercede or replace either UCA Board Policy 412 or the UCA Mobile Device Security Policy. Employees should also be familiar with these policies and related laws.

1. Board Policy 412
    a. http://uca.edu/board/files/2010/11/412.pdf

2. UCA Mobile Device Security Policy
    a. http://uca.edu/go/mdspolicy

3. US Export Administration Regulations (EAR)
    a. https://www.bis.doc.gov/index.php/regulations/exportadministrationregulationsear

4. International Traffic in Arms Regulations (ITAR)
    a. https://www.pmddtc.state.gov/regulations_laws/itar.html

5. Office of Foreign Asset Control Sanctions (OFAC)
    a. https://www.treasury.gov/about/organizationalstructure/offices/Pages/OfficeofForeignAssetsControl.aspx

B. UCA Owned Devices

1. Employees are prohibited from taking personally assigned, UCA owned devices on international trips. This includes computers, tablets, and cellular phones.

C. Approved Loaner Devices

1. With approval of the employee's department chair (or director), and dean (or vice president), UCA will provide a "loaner device" that can be used during the employee's time outside of the US (form available on the UCA IT website uca.edu/it).

2. Only the information and/or software necessary for the pending trip will be loaded onto the device.

2. The loaner device will be subject to whole disk encryption.

3. As smartphones and tablets are subject to the same search and seizure guidelines and security risks, travelers will be provided with a "loaner phone" or "loaner tablet" (subject to availability and division vice president or college dean approval).

D. Prior to Travel Outside the United States

1. Any employee who will be traveling outside of the US on university business or taking technology assets owned by the university must notify ItT at least 30 days in advance of their departure and give his/her anticipated return date to ensure availability of loaner devices.

E. After Return to the United States

1. Upon return to the United States, the loaner device(s) must be returned to IT within 7 days (unless other arrangements are agreed to in writing by IT) to allow the device to be securely wiped of all data.

    a. UCA is not responsible for any personal data stored on the device(s). All personal data should be removed prior to returning the loaner device to IT.

2. Due to the risk of malware infection, loaner devices SHOULD NOT be connected to your home network nor to the UCA network prior to returning it to IT.

3. In the event that the device is lost or stolen, the employee should notify the IT Help Desk (helpdesk@uca.edu or 501-450-3107) immediately.

G. Enforcement

Failure to comply with this policy will be investigated in accordance with UCA disciplinary procedure. Noncompliance with this policy and/or its resulting procedures may be cause for disciplinary action up to and including (but not limited to):

1. Forfeiture of University Owned mobile device(s)

2. Suspension of network account and/or email privileges

3. Administrative disciplinary action

4. Suspension of employment with or without pay

5. Termination of employment

6. Civil action initiated by the University and/or other parties

7. Referral to appropriate law enforcement agencies

H. Acknowledgements

1. Failure to comply with federal export regulations can result in substantial fines to the University.

2. Failure to comply with federal export regulations can result in substantial personal penalties including fines and/or imprisonment.

3. All employees who will be traveling outside of the US on university business or taking technology assets owned by the university must provide documentation of receipt of this policy.

TRAVEL SUGGESTIONS FOR PERSONALLY OWNED DEVICES

University travelers should be extremely vigilant when traveling with their personal laptops, tablets or other communication devices such as smartphones. Many foreign countries monitor, intercept, and/or record electronic communications as well as introduce viruses, trojans and other malware onto electronic devices without the traveler’s knowledge. As such, there are a number of precautions a traveler can take in order to minimize the risk associated with unintended data loss or theft. These precautions include:

- Never leave your electronic devices unattended, including in room safes, hotel lockboxes and hotel safes located in the lobby. These can often be accessed by hotel personnel or by foreign intelligence personnel and should be viewed as providing no security for your technology devices.

- When traveling with a laptop, be sure to utilize hard drive encryption to protect the data stored on your computer.

- Be wary of hotel and other public wifi networks and never use them to transmit or receive sensitive information. These wifi networks are notorious for data interception and theft as well as creating a convenient attack vectors for hackers to intercept your data, personal information, and other network traffic.

The best course of action is to take as little sensitive information as possible when traveling overseas. As stated previously, all technology assets should remain in your possession at all times. This includes any other types of media such as flash drives or other computer disks.

THINGS TO REMEMBER AT THE U.S. BORDER

- Data loss can occur at the U.S. border. The agencies of the Department of Homeland Security have the right to search and seize laptops and other electronic devices at the nation’s border. Under the agency directives for the Immigration and Customs Enforcement Agency, searches are allowed absent any individualized suspicion and agents can confiscate a digital device for up to 30 days without any supervisory approval.

- Under Customs and Border Protective guidelines, agents can keep a device for up to five days without any further approvals. Given that laptops or other digital devices are subject to search and seizure at the U.S. border without probable cause of suspicion, it is prudent that travelers carefully think about what information is absolutely necessary for their overseas travel.

Review/Revision Tracking

Date	Action
2/23/16	Adopted
2/20/24	Reviewed, edited for grammar and formatting