Ohio Administrative Code

Rule 3341-3-71 Travel and data security policy for BGSU-owned devices.

Effective: June 12, 2020

(A) Policy statement and purpose

This policy offers protections to the intellectual property and privileged data of the university and BGSU faculty, staff, and students when travelling to countries identified by the U.S. government as being high risk for engaging in cybersecurity threats on foreign visitors. The required data security precautions listed below are designed to limit breaches of student data, institutional data, research data, and other types of privileged information that could occur while BGSU personnel are traveling abroad.

Individual travelers are responsible for compliance with this policy.

(B) Policy scope

This policy encompasses the use of university-owned computer laptops, mobile tablets, and data storage devices while traveling in high risk countries, regardless of the purpose of the travel. It pertains to BGSU faculty, staff, and graduate student teaching assistants and research assistants who have been individually assigned a university-owned laptop or mobile tablet.

(C) Policy definitions

High risk countries refers to countries, regions and cities which are the subject of relevant travel warnings issued by the U.S. state department and other government agencies. The university reserves the right in its sole discretion to designate other locations as high-risk. A list of high risk countries is maintained by ITS and provided on its international travel website.

(D) Policy

(1) Required protections

Use of technology during international travel to countries identified as being high risk countries must adhere to the required protections provided by the information technology services department. The list of countries as well as the required protections for information technology resources can change frequently. Faculty and staff must visit the BGSU information technology international travel website and adhere to the required protections for travel to high risk countries. The minimum list of required protections are:

(a) Consult the ITS international travel website to determine if the country to which you are travelling is listed as a high risk country and for an updated list of required protections.

(b) Do not take your individually assigned BGSU device(s) such as a laptop computer or a mobile tablet device to a high risk country; instead, contact the ITS service desk at least ten working days prior to travel to obtain a clean laptop.

(c) Only load necessary data onto the clean BGSU laptop.

(d) Use the BGSU VPN to connect back to BGSU resources.

(e) Do not connect a flash drive to any foreign device while in a high risk country.

(f) Do not connect a foreign flash drive to the clean BGSU laptop at any time.

(g) Immediately upon your return to the United States, bring all devices back to ITS for forensics review and cleaning. Do not connect any device, including personal mobile phones, to the BGSU server prior to its being checked by ITS.

(h) Change your BGSU password once you have returned back to BGSU using your individually assigned BGSU device.

(i) Travelers are strongly urged to use a disposable mobile phone while in a high risk country.

(2) Use of BGSU devices on personal travel

Faculty or staff members who are travelling to high risk countries for non-job-related reasons are not allowed to bring BGSU owned electronic devices with them unless they are in compliance with this policy.

(E) Enforcement and sanctions

Individuals or entities in violation of this policy will be referred to the appropriate disciplinary process. A violation of this policy may result in disciplinary action, up to and including termination of employment.

(F) Implementation of policy

This policy is owned and maintained by the office of the provost. However, the elements contained within the policy are impacted by various departments across the university, including, but not limited to, international programs and partnerships, office of sponsored programs and research, risk management/environmental health and safety, and information technology services.

(G) Related policies

rule 3341-6-07 of the Administrative Code (BGSU information technology)

rule 3341-6-18 of the Administrative Code Data (use and protection)