1.0 PURPOSE 3

This policy is intended to mitigate to the extent possible the risks to state owned devices and networks used by employees during international travel and to safeguard the state's information systems.

2.0 SCOPE

This policy applies to all Executive Branch employees, contractors, or vendors who travel outside the United States for State of West Virginia business, or personal travel with a state owned device.

3.0 POLICY

3.1 ALL business related international travel must be approved by the employee's supervisors, up through the agency executive director. Once approved by the executive director, the travel request must be electronically submitted to the Chief of Staff/Governor's Office, by the executive director, or his or her designee. The Chief of Staff/Governor's Office will then make the final decision as to whether to approve or decline the request.

3.2 If an employee is traveling internationally to a low-risk country for personal reasons, state owned devices shall not be taken out of the country, unless pre-approved in writing by the Cabinet Secretary of the Department by whom the employee is employed, and the CTO or CISO of West Virginia Office of Technology.

3.2.1 If the employee is not employed by a Department, the highest ranking Executive of the section of West Virginia Government by whom the employee is employed, must approve the travel with a state owned device in order for an employee to take a state owned device with him or her.

3.2.2 Devices cannot be taken to high or moderate risk countries for personal trips.

3.2.3 If approved to take a state owned device internationally, the employee shall follow all other guideline set forth in this policy.

3.3 Employees shall register your trip with the State Department at https://step.state.gov/step/

3.4 If the state employee holds a federal government CLEARANCE that is sponsored by the West Virginia Intelligence/Fusion Center (WVI/FC), or the United States Department of Homeland Security, DHS Form 11043-1 “Notification of Foreign Travel” must be submitted to the WVI/FC at wvfusion@wv.gov

3.5 Employees shall notify the West Virginia Fusion Center, and the State Office of Technology, no later than sixty days, prior to official foreign travel. In the event travel is scheduled less than 60 days prior to travel, the employee shall make such notification as soon as possible

3.6 The state employee must attend a pre-travel briefing prior to their approved international travel. The pre-travel briefing, required prior to every international travel, will be conducted by the WVI/FC, WVOT, and/or the West Virginia National Guard, provided that the West Virginia National Guard will only conduct these briefings if the traveler has a security clearance. In the event of short notice travel, a written briefing will be provided to the state employee.

Pre-travel briefings will include:

- Foreign Travel Risk Reduction/Preparation
- Security Tips
- Foreign Intelligence Overview/Collection Methods
- Terrorism and Criminal Violence
- Reporting/Emergency Contacts
- State issued electronics/technology

3.6.1 Travelers shall contact the West Virginia Fusion Center to determine if the destination, or lay over destination, to determine what level of security is necessary for that trip.

3.6.2 Any user going to a country with a “high” or moderate” risk, as determined by the West Virginia Fusion Center, must participate in the OT Loaner Program

3.7 The OT loaner program will provide loaner devices, such as a computer and cell phone for use during your trip.

3.7.1 These loaner devices come loaded with basic tools such as Microsoft Office and limit the amount of data you have, which minimizes the risk should the device be stolen or lost. OT will assist in uploading the data which has been approved to be loaded onto those devices.

3.8 Travel Service Email Accounts

3.8.1 When traveling to or through a moderate or high risk country, an employee will be issued a temporary email account to use while traveling. Emails will be forwarded to the temporary account for the duration of the trip. At the end of your travels, the temporary email account will be deleted.

3.9 Hardware and software travel restrictions

3.9.1 The United States restricts the transporting of certain types of hardware and software products to specific countries (referred to as "export controls"). Many other nations restrict the transporting of certain types of hardware or software into their country (referred to as "import controls"). The West Virginia Fusion Center shall advise travelers of what these restrictions are for each of the countries associate with the travel.

3.10 Assume everything you do, or have, on your devices is being intercepted

3.11 When possible, keep your device with you. If you cannot, secure your device in the manner as instructed by the West Virginia Fusion Center.

3.12 Information contained on your devices may be monitored. Assume everything you do, or have, on your devices is being intercepted and monitored.

3.12 Limit Data and Devices

3.12.1 International travelers shall limit the amount of sensitive information that is stored on or accessible to any mobile device taken on the trip. Examples of data that should be left or afforded exceptional protection include:

3.12.2 A “clean” device shall be issued to the traveler, and only necessary information will be uploaded onto that device. If traveler is traveling through or to a country that bans encrypted devises or software, then the traveler shall be issued a clean device that conforms to the laws of those countries.

3.12.3 Travelers shall avoid contact with the State network in general, specifically when traveling to high risk countries, Communications shall be accomplished by voice call, or facsimile.

3.13 Identify "HIGH” or “MODERATE” Risk Countries

3.13.1 Do not use unknown storage devices

3.13.2 Only plug items into your devices that you have brought with you.

3.13.3 Public charging stations at airports or hotels should also be avoided, as they can transmit harmful software to your devices.

3.14 Employees, unless instructed, shall not use public WiFi, publicly shared computers or devices or devices belonging to other travelers while out of country. The West Virginia Fusion Center and the Office of Technology shall advise employees on appropriate methods to access a network.

3.15 Employees should always be aware of his or her surroundings when logging in or inputting data

3.16 Employees, unless instructed, shall not use public WiFi, publicly shared computers or devices or devices belonging to other travelers while out of country. The West Virginia Fusion Center and the Office of Technology shall advise employees on appropriate methods to access a network.

3.17 Notify the local US Embassy and West Virginia Fusion Center as soon as possible, if theft, loss, or confiscation occurs.

3.18 Upon return

3.18.1 Any and all passwords used during travel must be changed

3.18.2 Employees shall not connect, or attempt to connect to a State Network, with either a hard connection or wi-fi, with the loaner device at any time, until instructed by the Fusion Center, or OT

3.18.3 Upon return from international travel, the state employee must attend a post-travel briefing. The post-travel briefing will be conducted by the WVI/FC, WVOT, and/or the West Virginia National Guard.

3.19 Post-travel briefings will include:

3.19.1 Reporting of foreign contacts during the international travel

3.19.2 If the state employee holds a government CLEARANCE that is sponsored by the WVI/FC, or the United States Department of Homeland Security, DHS Form 11053-5 “Foreign Contact Form” must be submitted to the WVI/FC at wvfusion@wv.gov

3.19.3 Employees shall return the loaner device to OT as soon as possible once the employee has returned from travel.