COUNTY TRAVEL TO ELEVATED RISK COUNTRIES

SUMMARY

When traveling to countries identified as “elevated risk” by the United States Department of State, County employees are vulnerable to cyber-attacks, cybercrime, monitoring, or surveillance of voice, text, and data traffic.

Cyber espionage related to travel in certain countries is continuing to increase. It is in the best interest of the County to minimize these risks. Miami-Dade County’s Information Technology Department (ITD) will take appropriate steps to minimize the risk of Zero Day attacks, which is a cyber intrusion method for which there are no known countermeasures.

PROCEDURE

Before international travel:

1. Three weeks prior to traveling to any international destination, the Department shall provide the name of the County employee, dates of travel and itinerary to the Information Technology Department (ITD).
2. Upon being advised of any County business-related international travel, ITD shall contact the Department of State (travel advisories are found on this webpage: https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/), the local field office of the Federal Bureau of Investigation (FBI) and the Department of Homeland Security to obtain current concerns, cautions, and warnings related to the employee’s itinerary. ITD shall advise the Department and the employee of the concerns, cautions, and warnings.
3. Employees are strongly cautioned to leave personal devices at home.
4. Employees who have County-issued telecommunication devices are prohibited from taking those devices. ITD will provide a temporary device to the employee, with Voice and SMS capability, to be used specifically for the international trip.
5. ITD will ensure that when the temporary device is issued to the employee, the operating system and software is fully-patched and up-to-date with all security software.

During the trip:

1. The temporary device will be password protected with a strong password. The employee should memorize this password (the password should not be kept in a place where it could be found and accessed.)
2. When not in use, the temporary device must be turned off. The device should not be placed on “sleep” or “hibernation” mode when inactive.

3. Employees must be aware that anything done on the device, via the Internet, is at high risk of being intercepted. Encrypted data can be decrypted.
4. Employees must never use computers in cyber cafes, public areas, hotel business centers, or any other non-secure location to access the County Network.
5. Hotel-provided WiFi, or public WiFi services, should be considered non-secure and employees should never utilize these services to connect to the County Network including but not limited to Virtual Private Network (VPN), Office 365, and / or, Citrix Virtual Desktop Environment.
6. Under no circumstances should an employee accept or acknowledge a prompt to install a certificate or software. These prompts can be presented via a wireless or WiFi connection.
7. Devices must remain in the physical possession of the employee at all times during travel.
8. Prior to boarding the return flight, employees must turn off any temporary device and immediately discontinue use.

Upon Return:

1. Upon return, the employee must immediately visit ITD return the device to the technician who originally provided the device to the employee.
2. ITD will examine the device and insure that all data is extracted and preserved, subject to Chapter 119 of the Florida Statutes.
3. ITD will reset the device to its factory defaults.

CONTACT(S):
Department/Division
Information Technology Department

REFERENCE DOCUMENT(S):

- Administrative Order 5-5
- U.S. Department of State Bureau of Consular Affairs: https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/)
- Multi State – Information Sharing and Analysis Center - MS-ISAC Security Primer – Cybersecurity While Traveling: https://www.cisecurity.org/white-papers/cybersecurity-while-traveling/