INDEX

REVISION AND APPROVAL HISTORY

Revision No.	Description	Page(s)	Made by	Date	Approved by	Date
1	General Revision	All	C.Santos	31/07/2024	B.Azevedo	12/08/2024

Summary

The Information Security for Traveling Policy is a document that defines the baseline for the behavior of ADDVOLT people when travelling on business with ADDVOLT assets containing classified information.

1. Scope

Managers and employees, who travel with laptops, phones, and other mobile devices, are subject to many risks, namely that of loss, seizure, or tampering. Please use these recommendations as a guide to reduce the risks associated with travelling with these devices' data.
All employees, contractors, temporary, and other workers at ADDVOLT are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with ADDVOLT's policies and procedures as well as local laws and regulations.

2. References, Definitions and Terminologies

None.

3. Policy Description

3.1 General Guidelines

- Depending on where you plan to travel abroad, electronic communication devices may be subject to involuntary official governmental review and possible duplication of the hard drive's contents.
- The ADDVOLT requires the use of encryption on all organizational devices. Use of encryption to protect information may be forbidden in some countries, you should check with ADDVOLT IT before you travel abroad to ensure compliance with foreign countries' laws. And, if your encryption product allows you to "hide" information, those "hidden" areas can be detected, and you could be subject to criminal charges by the country's government. Because it is difficult to monitor encrypted traffic, use of secure ("https") websites and/or use of virtual private networks (VPNs) may be blocked by some countries.
- Some countries may censor certain content or sites. Attempts to circumvent national censorship of websites, such as some mainstream western social media sites, is discouraged by the ADDVOLT. You should only use VPN to access necessary files and sites to conduct your business. If you are found to be using a product to circumvent the blocking of censored websites, you may be warned, have your electronic devices confiscated, or you may become subject to criminal charges.
- Personal privacy may not be respected. Even private spaces such as hotel rooms, rental cars, and taxis may be subject to video, audio, or other monitoring. This type of surveillance may be able to track your whereabouts, what you may be doing, what's on your electronic device, and what you may be entering into it. Conversations either in person or on a phone may be monitored

3.2 General Recommendations

- Configure a password to logon to any devices you are taking. A password prevents others from accessing your data if your device is lost or stolen.
- Be sure that any device with an operating system and software is fully patched and up-to-date with all institutional recommended security software (e.g. Antivirus).
- Encrypt your devices but check with ADDVOLT IT before you travel abroad to ensure compliance with foreign countries' laws.
- When not in use, turn off or lock the devices.
- DO NOT store information classified as confidential on any devices you carry with you, if it is not essential for work with it.
- DO NOT copy confidential information to memory sticks or other easily lost media.
- DO store data that you need for your trip in a "OneDrive" account or on another service defined by ADDVOLT IT.
- Upon your return, immediately change your System password and the passwords of any accounts used while abroad.
- DO NOT use public chargers (e.g. at the airport) to charge your mobile phone or laptop because you don't know what is on the other end of the cable. But if you really need to charge your device, before plugging in the cable switch off the device completely.
- DO NOT work on confidential information in places where people may be or pass by behind your back and see and/or photograph your screen.
- To work in means of transport (e.g. airplane, train) it is strongly recommended to use a privacy screen on your monitor.

3.3 Additional Recommendations

- Set Wi-Fi to "do not automatically connect to Wi-Fi" on all devices capable of wireless connections.
- DO NOT update your computer while connected to a public or hotel wireless network.
- Disable Bluetooth on your laptop, mobile phone, and other devices.
- Set your mobile device to be wiped after 10 login attempts. Backup your device before traveling in case your device is wiped.
- Tape over any integrated laptop cameras or disable them to prevent a hacker from viewing you while you use your laptop.
- Ensure host-based firewalls are configured and enabled on Windows and Mac laptops.
- Leave unneeded car keys, house keys, smart cards, credit cards, swipe cards, or fobs you would use to access your workplace, or other areas, and any other access control devices you may have at home.
- Clean out your purse or wallet of any financial information such as bank account numbers, logins and passwords, any RFID cards (including U.S. Government Nexus "trusted traveler" cards) should be carried inside an RF-shielded cover.
- If you need to send and receive email while traveling, create a temporary "throw away" account on Microsoft Outlook or a similar service before you travel.

3.4 Traveling to High Cyber-Risk Countries

Traveling with IT devices to some countries, most notably China and Russia, is considered high cyber-risk.

The U.S. government has issued several advisories that travellers be aware that they could be targets of espionage activities when visiting these countries. Travelers are strongly encouraged to follow these recommendations:

- DO NOT travel with encrypted devices to China unless you have advance approval from China. China severely restricts the import of unapproved encryption. If you attempt to cross the border with an encrypted device, you may be asked for the decryption key, or your device may be confiscated.
- The U.S. government prohibits traveling with encrypted devices to countries that are considered to support terrorism, namely Cuba, Iran, North Korea, Sudan, and Syria. DO NOT bring encrypted devices to these countries.
- Use caution when connecting a USB device to an unknown computer or charger as it may become infected with malware.
- Upon your return, immediately discontinue use of the devices. The hard drive of the devices should be reformatted, and the operating system and other related software reinstalled, or the device properly disposed of. Contact your IT administrator to assist you.

4. Monitoring and Compliance

ADDVOLT reserves the right to periodically audit networks and systems to ensure that they are following the requirements defined in this standard.

Accordingly, the Security team must monitor compliance with this standard through the various methods at its disposal and consider all Information Security requirements, including, but not limited to, management reports, internal and external audits and feedback information officer, information assets or information processing resources of the ADDVOLT.

Under no circumstances is an employee or ADDVOLT interested party authorized to engage in illegal activities under national or international law using the ADDVOLT resources in their possession.