

CITY OF MARQUETTE, MICHIGAN

ADMINISTRATIVE POLICY

Policy Number: 2010 - 05	Revision Date:
Date Approved: 12-09-10	

POLICY: Foreign Travel and City Electronic Communication Devices

Overview

The Department of Home Land Security has released a warning and recommendation regarding electronic communication devices (cell phones, PDAs, laptops, etc.). U.S. citizens traveling abroad face heightened risk of surreptitious cyber monitoring and data theft. Corporate and government leaders are at greatest risk due to their access to non-public systems and deliberative private discussions. Further, many foreign governments own or control public telecommunications infrastructure and support business intelligence gathering. As a result, roaming services provided through these companies are particularly well postured to collect information from foreign travelers without the knowledge of the traveler.

Scope

This policy applies to all personnel who utilize City-owned electronic communication devices.

Policy

To prevent the possible compromising of City data and networks, all personnel who travel outside the boundaries of the United States are prohibited from taking any City-owned electronic communication devices with them. Hotel rooms, Internet cafes, offices, and public places may be subject to on-site or remote technical monitoring. Travelers should assume that all information processed and transmitted on fax machines, foreign computers, copiers, or telephones is subject to interception. This vulnerability extends to personal cell phones, laptops, and PDAs brought from the United States that transmit over a foreign country's networks.

In addition, spy software which intercepts and transmits information without a user's knowledge can be implanted through both wired and wireless Internet portals in cafes, hotels, transportation depots, and elsewhere. Universal Serial Bus (USB) memory sticks and similar storage devices may become infected with malicious software if used on devices in a foreign country or loaded with malicious software when they are not in the owner's possession.

Recommendations

When traveling in foreign countries, personnel are advised to purchase single use cell phones. If it is necessary to use electronic devices and media abroad, travelers should not use them to communicate with any City networks, and upon return should submit them to the IT Department for evaluation.

When in transit or separated from a computer or PDA, travelers should keep sensitive and proprietary information continuously in their possession. Upon returning home, these storage devices must be submitted to the City IT Department for thorough review and evaluation before use with devices connecting to government networks. Travelers should use strong passwords on devices and encryption programs for electronic files and e-mails.

Compliance

Failure to comply with this policy may result in disciplinary action up to, and including, termination.

Exceptions

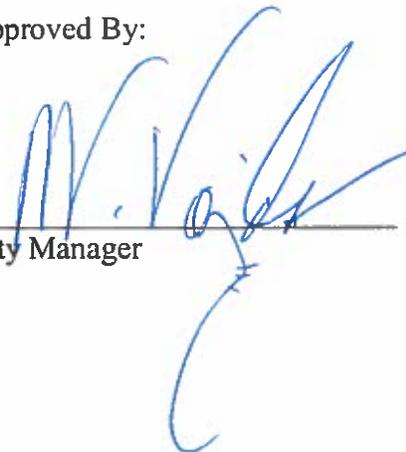
Any privately owned, laptops, cell phones, etc., are exempt from this policy. However, if private devices are operated outside the United States, they will not be permitted to connect to any City systems until submitted for evaluation and clearance by the City IT Department. Failure to report such use may result in disciplinary action up to, and including, termination.

Recommended By:



Director of Administrative Services

Approved By:



City Manager