ORANGE COUNTY SHERIFF'S OFFICE

GENERAL ORDER

Effective Date: December 4, 2025	☒ **Amends** - GO 13.1.1 (October 7, 2024)	**Number:** 13.1.1
Distribution: All Personnel	**Review Month:** October	**Reviewing Authority:** Undersheriff / Information Technology
Subject: Agency Technology Equipment and Software Modifications		

This order consists of the following:

1. Purpose
2. Policy
3. Definitions
4. Procedures

1. Purpose

The purpose of this policy is to prevent unnecessary repairs, delays and damage to agency-owned technology equipment and software. Unauthorized alterations to technology equipment and software may also invalidate any agency contracts or warranties. Prohibit the use of applications from foreign countries of concern on government-issued devices. This policy aims to prevent security risks associated with unauthorized applications, safeguard sensitive data, and maintain the integrity of agency operations.

2. Policy

It shall be agency policy to prevent unnecessary repairs, costs, delays and damage to agency owned technology equipment and software by verifying alterations that are made in accordance with service contracts or warranties. Installation of software must be strictly controlled in accordance with SO 13.1.17 and measures are implemented to block, restrict, and remove applications to protect against potential security threats and ensure compliance with Florida Statutes and other applicable regulations.

3. Definitions

A. Computer Virus - A computer program intentionally written to disrupt and/or damage computer software and/or hardware.

B. Foreign Country of Concern - The People's Republic of China, the Russian Federation, the Islamic Republic of Iran, the Democratic People's Republic of Korea, the Republic of Cuba, the Venezuelan regime of Nicolás Maduro, or the Syrian Arab Republic, including any agency of or any other entity under significant control of such foreign country of concern.

C. Foreign Principal - Any government or official of a foreign country of concern, political party or member thereof, any organization or entity under such a country's control, or any individual domiciled in such a country and not a U.S. citizen or lawful permanent resident.

D. Government-issued Device - Any electronic device capable of connecting to the

Internet, owned or leased by a public employer and issued for work-related purposes.

E. Printer Supplies - all supplies consumed during normal use of printers including, but not limited to, ribbons, toner cartridges, ink cartridges and paper.

F. Prohibited Application - An application created, maintained, or owned by a foreign principal that poses security risks such as data collection, cyber-espionage, surveillance, disinformation, or any other threat as determined by the department.

G. Software – any programs, including operating systems, installed on agency owned technology equipment.

H. Technology Equipment - any computers, servers, PCs, laptops, MDTs/MDCs, printers, scanners, terminals, modems, speakers, monitors, personal devices, etc.

I. Security Accreditation: A documented risk-based evaluation process resulting in a formal recommendation to approve, conditionally approve, or deny the use of a system or service. Accreditation establishes accountability and provides a risk-informed decision to leadership.

4. **Procedures**

A. Agency technology equipment and software must not be installed, relocated or in any way altered without the consent of the Chief Information Officer or designee. The only exception is the replacement of printer supplies. Printer supplies are the responsibility of each division. Printer ribbons, toner cartridges, ink cartridges and similar items must be replaced by each division as necessary.

Process for requesting installation, relocation or alterations, other than printer supplies:

1. Employees must call or submit a request to the Service Desk, stating the desired installations, relocations or alterations.

2. IT personnel must determine if the request is feasible and can be accomplished according to agency directives.

3. IT personnel must obtain a cost analysis and submit the same in writing to the requesting personnel, when new technology equipment or software purchases are necessary to accomplish the request per GO 13.1.3.

4. IT personnel must coordinate, schedule, and as necessary, perform the requested changes. IT personnel must keep the agency personnel involved informed as to status of the request.

B. IT personnel must not approve or support the installation of agency-owned software on non-agency equipment unless specifically authorized by the Chief Information Officer or designee.

C. Only legally obtained and licensed software, with proof of licensing for each instance of use, and authorized for agency use, must be installed on agency-owned technology equipment. IT personnel must not install, support or maintain any other software. The Chief Information Officer must submit a memorandum to the involved person's Division Commander via chain of command and copied to the Assistant Chief Information Officer, reporting all instances of:

1. Installation of unlicensed or unauthorized software on agency owned equipment.

2. Any alterations to agency owned technology equipment and software without the consent of IT.

D. Blocking, Restricting, Removal and Uninstallation of Prohibited Applications

1. IT personnel must block access to all prohibited applications from public networks and virtual private networks (VPNs) owned, operated, or maintained by the agency.

2. IT personnel must restrict access to any prohibited application on all government-issued devices.

3. IT personnel must have the ability to remotely wipe and uninstall any prohibited application from a government-issued device suspected of being compromised.

   Within 15 calendar days of the Florida Department of Management Services issuing or updating the list of prohibited applications, IT personnel must remove, delete, or uninstall any prohibited applications from government-issued devices.

4. Employees are prohibited from downloading or accessing any prohibited application on a government-issued device.

E. Exceptions for the use of Prohibited Applications

1. Exceptions are allowed for sworn personnel if the use of prohibited application is necessary to protect public safety or conduct investigations within the scope of their employment. All exceptions for sworn and non-sworn employees must be approved by the Undersheriff via the chain of command. Upon approval of the exception, staff must submit a Service Request via the Help Desk Portal. The request must include the Undersheriff's approval. The IT Department shall provide access to the staff members' device(s).

2. The Sheriff or designee must submit a waiver request to the Florida Department of Management Services to allow designated non-sworn employees to use prohibited applications under specific circumstances.

The waiver must be limited to a timeframe of no more than 1 year. The agency must request an extension if necessary.

F. All agency employees must scan all removable media with virus protection software prior to use. Any employee who has reason to believe a computer virus has infected agency owned technology equipment and/or software shall immediately notify the IT Service Desk. IT personnel must assist employees in identifying, and, whenever possible, removing viruses from agency-owned technology equipment and software. All removable media used on the suspect equipment must be located and tested. Any equipment that may have come in contact with the suspect removable media must also be checked.