Policy

SECTION: INFORMATION TECHNOLOGY	POLICY#020-C0061	PAGE: 1 of 4
TITLE: LAPTOP/TABLET COMPUTER USE	EFFECTIVE DATE: 03.20.20	
REPLACES: N/A	DATED:	

DISTRIBUTION: CAREERSOURCE TAMPA BAY STAFF

PURPOSE: The purpose of this policy is to establish acceptable use of laptops, tablet electronic devices and mobile network resources at CareerSource Tampa Bay ("CSTB") in conjunction with its established culture of accountability, trust, integrity and in compliance with Florida Sunshine Law.

BACKGROUND: The use of laptops and tablets, and similar devices ("mobile assets"), and related communication services by CSTB employees in the course of their work is common. CSTB often provides these devices to employees to improve communication, productivity and work efficiency, to facilitate teleworking , working between multiple onsite locations and to otherwise enhance the contributions of employees. CSTB policies generally require mobile assets to be used only for business use.

OBJECTIVE: The objective of this policy is to define guidelines for acceptable use of CSTB mobile assets. This policy requires the users of mobile assets to comply with company policies and establishes the responsibilities of the employee and CSTB regarding any use of mobile assets. The policy sets further requirements regarding the use and maintenance of mobile assets.

SCOPE: All employees, contractors, consultants, temporary and other workers at CSTB, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information technology mobile assets owned or leased by CSTB, or to mobile devices that connect to a CSTB network or reside at a CSTB site.

GENERAL GUIDELINES

- Staff are responsible for exercising good judgment regarding appropriate use of CSTB mobile assets in accordance with CSTB policies, standards, and guidelines. CSTB mobile assets may not be used for any unlawful or prohibited purpose.

- For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic. Devices that interfere with other devices or users on company network may be disconnected. IT prohibits actively blocking authorized audit scans. Firewalls and other blocking technologies must permit access to the scan sources.

SYSTEM ACCOUNTS

- Staff are responsible for the security of data, accounts, and systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

- Staff must maintain system-level and user level passwords in accordance with the Password Policy that is set by IT.

- Staff must ensure through legal or technical means that proprietary information always remains within the control of CSTB. Conducting CSTB business that results in the storage of proprietary information on personal or non-CSTB controlled environments, including mobile assets maintained by a third party with whom CSTB does not have a contractual agreement, is prohibited.

COMPUTING ASSETS

- Staff are responsible for ensuring the protection of assigned CSTB assets that includes the use of computer cable locks and other security devices. Mobile assets left at CSTB overnight must be properly secured or placed in a locked drawer or cabinet. Mobile assets should not be left in plain view in a vehicle, but if necessary, should be hidden or locked in the trunk.

- Promptly report any theft of CSTB mobile assets to direct supervisor. A police report must also be filed for CSTB records and management.

- If an employee's laptop is stolen due to negligence or not returned upon ending employment with CSTB, the employee will be responsible for the cost of replacing the laptop.

- All mobile assets are secured with a password protected screensaver that is issued by IT at 10-minute intervals. Staff must lock the screen or log off when the device is unattended.

- Mobile assets that connect to the CSTB network must comply with the Computer Use Policy.

- Mobile assets must not interfere with IT device management, or security system software, including, but not limited to Symantec Endpoint, Malwarebytes, Dameware and Microsoft Intune.

NETWORK USE: Staff are responsible for the security and appropriate use of CSTB network resources under your control. Using CSTB resources for the following is strictly prohibited:

- Causing a security breach to either CSTB or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device, or sniffing network traffic.
- Causing disruption of service to either CSTB or other network resources.
- Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software.
- Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws.
- Use of the Internet or CSTB network that violates the Computer Use Policy or local laws.
- Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, email bombs, spyware, adware, and keyloggers.
- Port scanning or security scanning on a production network unless authorized in advance by IT.

ELECTRONIC COMMUNICATIONS: The following are strictly prohibited:

- Inappropriate use of the communication of equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates CSTB policies against harassment or the safeguarding of confidential or proprietary information.
- Sending Spam via e-mail or other forms of electronic communication.
- Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.
- Use of a CSTB email or IP address to engage in conduct that violates CSTB core values, policies and guidelines. Staff must exercise good judgment to avoid misrepresenting or exceeding your authority in representing CSTB.

ENFORCEMENT: An employee and/or DEO managed staff found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in termination of their contract or assignment with CSTB.

EXCEPTIONS TO THE POLICY: Exceptions to the guiding principles in this policy must be documented and formally approved by the IT Coordinator. Policy exceptions must describe:

- The nature of the exception
- A reasonable explanation for why the policy exception is required
- Any risks created by the policy exception
- Evidence of approval by the IT Coordinator

AMENDMENTS: Amendments to this policy will be published from time to time and circulated to CSTB staff.

ROLES AND RESPONSIBILITIES

Stakeholder	Responsibilities
CSTB Staff	Review and formally support this Policy.
IT Coordinator	Develop and maintain this Policy Review and approve any exceptions to the requirements of this Policy. Take proactive steps to reinforce compliance of all stakeholders with this Policy.
CSTB Managed Services Provider	Communicate with CSTB, directly or through CSTB representatives, in informal or formal instances, to understand CSTB needs and expectations, explain the capabilities of the existing technology in production, including mobile devices and networks.

INQUIRIES: Inquiries regarding this policy can be directed to the IT Coordinator.