PROCEDURE TRANSMITTAL		
SUBJECT:	**Mobile Computing**	**Procedural/Guidance No.:** IS PY 2015/16-0006
APPLIES TO:	South Florida Workforce Investment Board, dba CareerSource South Florida (CSSF) Managerial, Contractors and Sub-Contractors' Staff	**Effective Date: Immediately** **Revised Date:** **Expiration Date: Indefinite**
REFERENCE:		

A. PURPOSE

This policy defines the processes and standards for company-issued and user-owned devices while working at CSSF centers. This policy addresses accepted use for devices that connect to a wire or wirelessly, or through a mobile device while working for CSSF.

B. POLICY

This policy applies, but is not limited, to devices, services and media that fit the following types:

a. Smartphones/ cellular devices.
b. Tablet computers including and not limited to iPads, Galaxy Tablet.
c. MiFi, Air Cards, USB modems.
d. Any device capable of connecting to the corporate network.
e. Any device capable of connecting to a wireless carrier.

Users who violate this policy are subject to disciplinary actions that may include, but not limited to:

a. Suspension or revocation of computing and other account privileges.
b. Disabling access to all CSSF network resources.
c. Referral to law enforcement as necessary.
d. Personal financial responsibility for costs that may incur.
e. Disciplinary actions leading up to termination

The following actions may result in disciplinary actions while in possession, operating, or granted access for use:

a. Not reporting a lost or stolen device that contains employee and/or customer information by the end of the business day of determining the device is lost or stolen.

Approved By:	Date: 7/12/16	Issued by: Elizabeth Santis, IT Manager

b. Downloading inappropriate software on the device without prior approval by the IT unit.
c. Excessive use of mobile devices for personal use.
d. Intentional physical damage of mobile devices.
e. Fraudulent use of mobile devices and services.
f. Excessive use of mobile services while roaming.
g. Not following IT security protocols while in possession of company-owned devices.
h. Not following federal, state and city regulations regarding mobile phones which include and not limited to texting while driving or not using a hands-free device.
i. Unapproved replacement of devices or accessories.

Company issued devices may contain the ability to make calls, access the internet, or may contain applications allowing access to company resources. While in possession of such devices, the following policies apply:

Smartphones/ cellular devices

a. Personal calls using company-owned smartphones/cellular devices are not permitted.
b. Inappropriate and non-work related internet browsing are not permitting.
c. All smartphones/cellular devices must be password protected in order to avoid accidental or intentional access to: email, text messages, phone logs, and images.
d. Users are responsible for the proper log off or closing of applications, and files accessed while in possession of the smartphones/cellular devices.

Tablet computers including and not limited to iPads, Galaxy Tablet

a. Users must password-protect tablet computers, work-related application, and access to the settings area.
b. Users must lock the tablet device when not in use or if walking away for any period of time
c. Users must not let other unauthorized users access the tablet computers. Additional users needed access to the device must receive prior approval from the IT unit.
d. Users must not browse inappropriate sites and network resources after normal business hours.
e. Users must return the tablet device as instructed by the IT unit or their manager. Users must also turn in the tablet device if going on any extended leave where access to the network and work-related resources are not required.

MiFi, Air Cards and USB modems

a. Users must use the MiFi, air cards, and USB modems only when traveling or working remotely and connecting devices (computers, tablet and other networking devices) to access work-related resources, or performing internet searches using sites allowed by CSSF.
b. Excessive use of bandwidth while operating the MiFi, air cards, and USB modems is not permitted. In the event that excessive use is required, users must contact their managers, who will then consult with the IT unit for guidance/approval.
c. Users must not connect personal devices (computers, table and other networking devices) to the MiFi, air cards, and USB modems in order to gain access to the internet.
d. Users should use MiFi, air cards, and USB modems when traveling internationally or on vacation

Approved By:	Date: 7/12/16	Issued by: Elizabeth Santis, IT Manager

Other devices cable or connecting to the network or wireless carriers

a. Personal devices, even with the correct IP, are not permitted to access network resources, unless a manager's approval is obtained; in addition, devices must meet the CSSF IT security requirements on hardware and software before obtaining any access to network resources. User with personal devices may access their email using webmail as permitted by their managers.
b. Devices, even previously approved, may be have their access taken away in the event of suspicious activities, not meeting security requirements, or not permitted on the CSSF network.
c. Users are required to be mindful of all usage on all company devices.
d. No user is allowed to place any company data on removable storage cards or any smartphones or tablet computers.

The IT unit reserves the right to remote wipe any device reported lost or stolen, or posing a security threat to the CSSF network. While data traffic may use strong encryption for information traversing the internet, the IT unit may limit, restrict, or cutoff excessive traffic affecting the normal operations of the network.