CareerSource SOUTH FLORIDA		
PROCEDURE TRANSMITTAL		
SUBJECT:	**Access Controls**	**Procedural/Guidance No.:** IS PY 2015/16-0001
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 sets out responsibilities and practices which are designed to address critical access in order to minimize risks to sensitive data, physical asset and private information.

B. POLICY

This policy applies to all CSSF staff, managers, facility staff, and external parties regarding the use of computer equipment and applications, space and restricted areas requiring authorized access. To meet this obligation, CSSF has established access control to address potential security risk to physical and virtual assets. Access control is necessary to avoid the intentional and unintentional by users to avoid crashing the information system, attempting to break into bypass security features, spreading viruses over the network, browsing through non work-related websites, personal use or unauthorized software.

Physical Access

a. Access to staff area is limited only to CSSF employees and contractors. Visitors are not allowed access to any employee area. Common area access is allowed (lobby, restrooms, etc.).
b. Access to computer equipment rooms is not permitted. Only authorized CSSF IT staff, service providers and contractors supervised by IT are allowed access while they perform specific tasks involving cabling, phone, or network connectivity.
c. Users are not allowed to service computer equipment, faxes, printers, network cables and outlets.
d. Access to any areas of any of the CSSF facilities after hours is not permitted. In the event that after hour access needed, a manager's approval is required.

Systems Access

a. Access to all server systems is only permitted to authorized IT personnel, with proper approval requested and granted by the Executive Director.

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

b. File and folder access is administered by the IT unit. Any modifications, creation, sharing or permission to be given to a particular user or group is subject to prior approval by the Executive Director.
c. Users are expected to access files and folders as it pertains to their respective roles. This policy prohibits users from sharing access given to them with other employees, or allowing others to access files and folders using their computer systems.
d. Users are not to attempt to access or modify files and folders they are not granted access to.
e. All systems access or used are not be shared, discussed or reveal to non-employees of CSSF.
f. Update, upgrades, or modifications to specific systems are not permitted. The IT unit is responsible, through approval, for the update, upgrade, and modifications of systems used on the CSSF network.