CareerSource
SOUTH FLORIDA

PROCEDURE TRANSMITTAL

SUBJECT:	IT Security Awareness Training	Procedural/Guidance No.: IS PY 201516-0004
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 outlines the procedures for initial security awareness training, yearly refresher training and ongoing security awareness for employees of CSSF, Centers, Access Points, Mobile Units and all others with access to the State/Local information systems.

B. POLICY

It is the policy of CareerSource South Florida to provide IT Security Awareness Training to all its users.

To manage risk, CSSF requires all its users to take initial security awareness training, yearly refresher training and ongoing security awareness. This training is necessary to ensure CSSF: communicates and documents, and trains staff on security best practices and concepts. CSSF utilizes the KnowBe4's security awareness training, designed to provide:

1. Baseline testing: this test is design to assess the phish-prone percentage of users through a simulated phishing attack.
2. On demand scenario-based exercises to raise awareness of common traps that exist if attackers attempt to hack CSSF's network and steal critical information, and how users react to potential security threats and breaches.
3. Phishing CSSF users: using Knowbe4's security awareness training, a multitude of templates will be used to help users detect phishing attacks, as currently used by real attackers.
4. Reporting: through stats and graphs, the detailed reports help the IT unit identify areas of concerns, and which center is more susceptible to attacks.

Requirements for the security awareness training:
This security awareness training is conducted initially and on a yearly basis. Users are given 10 days to complete the training before continuing to use CSSF computers and resources. In those 10 days, the user is expected to coordinate with their manager to be allowed the appropriate time for the training. In the event a user fails to take the training

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

by the due date as specified by the IT unit, all access to CSSF's network, email, and other resources, as well as DEO systems will be suspended.

Reinstatement of access:
CSSF's IT unit expects a request from the user's manager to take the training. Once the user successfully completes the training, another request is expected from the user's manager to reinstate all system accounts and proceed to perform duties as required by their position

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