PROCEDURE TRANSMITTAL		
SUBJECT:	**IT Password Management Procedure**	**Procedural/Guidance No.:** IS PY 2015/16-0002
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 procedure defines the purpose and applicability of CSSF's State/Local systems password management within the CSSF network.

B. POLICY

It is the policy of CareerSource South Florida to ensure protection of CSSF's information technology resources and promote accountability for its misuse.

1. Passwords are mandatory and enforced through Active Directory Group Policies. Active Directory is a database where all accounts and their attributes and permissions reside and passwords are encrypted using Microsoft Kerberos protocol.
2. Applications that are not active-directory integrated will require their own passwords and will require scheduled password changes that meet the complexities mention below.
3. Storing or writing passwords is strongly discouraged
4. Users are accountable for protecting their passwords and how his or her credentials are use.
5. Password must not be shared with anyone and must be kept secret.
6. Default contractor password\credentials will be changed before computer system\appliance or device is deployed into production.
7. All passwords in all applications will be masked or obscured to prevent unauthorized use.
8. Password history will be enforced to remember the last 3 passwords used.
9. Maximum password age is 89 days. On or before day 90 password must be changed to continue accessing CSSF resources and \or computer systems.

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

10. Password complexity is required and enforced. The following minimum requirements need to be met:
    a. Password cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters
    b. Cannot use words found in a dictionary
    c. Be at least six characters in length
    d. Contain characters from three of the following four categories:
        i. English uppercase characters (A through Z)
        ii. English lowercase characters (a through z)
        iii. Base 10 digits (0 through 9)
        iv. Non-alphabetic characters (for example: !, $, #, %)
    e. Complexity requirements are enforced when passwords are changed or created.
11. Account lockout duration is set to 15 minutes with a lockout threshold of five (5) invalid logon attempts.
12. Password reset requests must be handled by the employee's supervisor\manager and submitted in writing to the Help Desk. Only the help Desk staff is allowed to reset any given password related to Active Directory or any other application they may manage.
13. Network Managers are responsible for resetting Remote Access passwords.
14. IT Unit staff who have the need to share passwords, such as passwords for servers, applications, etc., are required to store the shared passwords in an encrypted format.

It is the responsibility of

1. All and any CSSF staff, vendor, contractor or anyone engaged in doing business or working on behalf of CSSF to understand this policy and follow its content as well as understand the ramifications of the activities related to their given credentials.
2. All managers, supervisors, and\or center's directors are required to communicate with the Help Desk when a staff member, vendor, contractors leaves the organization, retires, is dismissed or reassigned to a different organization or no longer requires access to a CSSF computer system or application.
3. Everyone working for or engaged by CSSF to do work on behalf of CSSF to safeguard their credentials and abide by the content of this policy.
4. Anyone suspecting their credentials have been compromised must report it to the Help Desk by either phone (305.594.7615 x281) or email addressed to helpdesk@careersourcesfl.com
5. Application developers, either in-house or on contract must ensure their applications support individual authentication instead of group authentication.
6. Applications must not store passwords in clear text.
7. Applications must not transmit passwords in clear text over the network or remote access connections.
8. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

CSSF, contractors/subcontractors staff found in violation of this policy may be subject to disciplinary action, up to and including termination of employment and\or contract.