



PROCEDURE TRANSMITTAL

SUBJECT:	Remote Access	Procedural/Guidance No.: IS PY 2015/16-0008
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 purpose, scope and controls used to provide access into CSSF's network when connecting from outside CSSF's network. These requirements aim to minimize potential CSSF's exposure from damages due to unauthorized access to CSSF's resources. Potential damages refer to destruction\loss\misuse of confidential\sensitive information, damage to CSSF's computer systems and damage to CSSF's public image.

B. POLICY

This policy applies to all types of remote access connections regardless of technology or medium used to establish the connection and covers all vendors, contractors, staff, IT Unit staff, Web-RS users and anyone using electronic type device to connect to CSSF's computer systems and resources or offered through CSSF's computer systems and resources.

Remote access into CSSF's network will be provided on specific cases such as:

1. CSSF staff and/or vendor\contractor staff requiring access to the State's Web-RS website (<http://refugee3.dcf.state.fl.us:7001/ords/rpdprod/f?p=MAIN:login:>)
2. CSSF's vendors\contractors requiring access to specific resources.
3. IT Unit staff requiring access after normal business hours due to the nature of the work performed. IT Unit staff includes, programmers, network managers & IT Manager.

The IT Unit is currently using a Barracuda VPN 180 appliance to provide remote access. This appliance allows strict control over the resources remote access users are allowed to access.


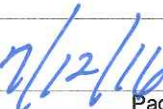
With the exception of the IT Unit staff mentioned above, all other staff, vendors\contractors are presented with a web page containing the resources they have been granted access to. By design, the Barracuda appliance restricts access only to

Approved By: 	Date: 	Issued by: Elizabeth Santis, IT Manager
--------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------	--------------------------------------------

resources presented through the web page. No other traffic is allowed. All traffic between the Barracuda appliance and the remote access user will be secured by the use of Secure Sockets Layer (SSL) certificates.

The following are general guidelines and requirements to be followed by all CSSF's remote access users:

1. All remote access users are expected to comply with CSSF's IT Policies and Procedures.
2. It is the responsibility of all remote access users to familiarize themselves with CSSF's IT Policies and Procedures as well as to follow CSSF's business practices.
3. Remote access into CSSF's computer systems and resources or offered through CSSF's computer systems are resources is not a right; it is a privilege and can be revoked without previous notification by CSSF.
4. Remote access will be strictly controlled by the use of credentials in the form of user name & password or any other method implemented by CSSF.
5. Password will contain a combination of letters and numbers and be no less than six characters in length.
6. All accounts will be controlled by settings and/or policies specifying
 - a. Resources to be accessed
 - b. Day\time resources will be available
 - c. Profile to be used.
 - d. Password refresh interval (90 days)
 - e. Only one connection per user account.
 - f. Only once connection per device
7. Remote access passwords are not to be shared and will be only used by the individuals issued to.
8. The use of split-tunneling to access CSSF's resources and/or computer systems or services offered through CSSF's resources and/or computer systems is not allowed.
9. All electronic devices connecting through CSSF's remote access service must have:
 - a. An up-to-date antivirus\antispysware solution installed.
 - b. A current operating system with latest patches\fixes installed.
10. Regarding Web-RS users:
 - a. All users will be given a remote access account only after CSSF's Help Desk completes confirms user has satisfied the requirements set forth by the Department of Children and Families account access and has been granted access to the WebRS.
 - b. All user accounts will be required to have an email address from the domain name of their respective employer.
 - c. Any change to the user account will need to be generated by the contractor's director or supervisor.
 - d. Documentation of contractor's director and user information will be kept by the network managers
11. No other type of remote access other than through CSSF's Barracuda VPN is allowed.
12. Only Network Managers are authorized to reset remote access passwords.

Approved By: 	Date: 	Issued by: Elizabeth Santis, IT Manager
--------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------	--------------------------------------------

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Deliberate, unauthorized disclosure of confidential information may result in civil and/or criminal penalties.

Approved By: 	Date: 	Issued by: Elizabeth Santis, IT Manager
-----------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------	--------------------------------------------