DARS ESO Provider Agreement Appendix G

Information Security Requirements Associated with the use of DARS Owned Systems.

The Employment Service Organization (ESO) shall comply with all Virginia Information Technologies Agency's requirements or provide industry standard and reasonable security controls to safeguard any IT systems used to handle DARS data. Specifically, the ESO must meet the Commonwealth of Virginia VITA Information Technology Resource Management Information Security Standard (SEC530) for all IT systems operated by DARS. For the purpose of this section, sensitive IT systems or data is considered to be any system or information, which contains data that could have a material adverse effect on the interests of the ESO or the Commonwealth of Virginia.

Specific Information Technology Security requirements include the following:

The ESO shall implement the DARS Acceptable Use Policy and Agreement (AUPA). All staff or volunteers accessing the ESO's IT systems must sign this Agreement acknowledging the users' acceptance of the Acceptable Use Policy and Agreement. The vendor shall maintain the Agreement on file.

The ESO must perform a background investigation of all users accessing sensitive IT systems or data. A background check includes:

- Signed application for employment (volunteer or contractor) status on file
- Identity verification (documentation provided for Employment Eligibility Verification. An I-9 form satisfies this requirement)
- Reference checks

The ESO must designate a Vendor Administrator as the individual responsible for managing system users. This individual must notify the DARS LTESS-EES Agency Staff Administrator within 24 hours of the occurrence of any changes needed (i.e. deletion or suspension of a user account) as well as periodically verify that access remains appropriate. Notification is also required when a user changes roles, no longer is affiliated with the ESO, or is on leave more than 30 days.

Every user accessing the LTESS-EES Requisitioning System is required to complete the current DARS External Users Cyber Security Training Curriculum offered through the Commonwealth of Virginia Learning Center. The ESO will maintain records of the training including participant and training date. If an individual does not complete the annual training, the ESO is required to suspend access to the system. The Vendor Administrator is responsible for ensuring that all users complete the annual training.

Gaining Access to the LTESS/EES Requisitioning System:

DARS ESO Provider Agreement Appendix G

To gain access to the LTESS/EES Requisitioning system, contact Anita Mundy, Agency Staff Administrator, at anita.mundy@dars.virginia.gov.
The following steps must be completed to set up an account and include:

1. Complete the current DARSS External Users Cyber Security Training Curriculum
2. Read Appendix G of the DARS ESO Agreement
3. Read and Sign the Acceptable Use Policy and Agreement (AUPA)
4. Complete and Sign the LTESS/EES Internet System Access Form

Please be advised that LTESS/EES System Users may not share their account information.

Data collected by the DARS is considered sensitive Commonwealth of Virginia data. It is a DARS responsibility to ensure that DARS computer systems, both hardware and software, are addressed in a Disaster Recovery Plan (DRP). It is the ESO's responsibility to supplement the DARS DRP as follows:

- PCs or laptops used to access DARS systems are interchangeable so that if one PC goes bad, another can be used to access DARS systems.
- If ESO network access is compromised, there is an alternative site planned for access. This can be demonstrated by showing that the ESO has physical access in two separate facilities that are interchangeable, a local facility is available that provides wireless access and / or a letter of agreement with another organization for network access. These three alternatives can be used in combination.
- The ESO must generate evidence that they have tested this DRP at least once during the past year.

DARS will perform periodic audits of ESOs to ensure compliance. ESOs that are not in compliance will be required to submit a Corrective Action Plan (CAP).