DARS ESO Vendor Agreement Appendix G

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

The Employment Support Organization (ESO) shall comply with all Virginia Information Technologies Agency's requirements. Specifically, the ESO must meet the IT Information Security Standard (SEC501) or subsequent version for all computer 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 and Confidentiality Policy. Any staff or volunteers accessing the ESO's IT systems must sign an Information Security Agreement (ISA) acknowledging the users' acceptance of the Acceptable Use Policy and "Confidentiality Statement". The vendor shall maintain the ISA on file. A most current copy can be found at http://www.vadars.org/essp/esos.htm .

The ESO must perform a background investigation of all users (employee, student, volunteer or contractor) 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

Employees hired before July 1, 2013 are excluded from the background investigation. Copies must be kept on file.

The ESO must designate an individual responsible for managing system users. This individual must notify the DARS application administrator 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 a sensitive IT system or data is required to complete and certify annual refresher security awareness training. DARS provides a basic training course at https://covkc.virginia.gov/drs/Kview/CustomCodeBehind/customization/login/accountstateselection.aspx . 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.

Data collected by the DARS is considered sensitive Commonwealth of Virginia data. It is a DARS responsibility to insure 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. It is envisioned the audit results will be published on a public website. ESOs that are not in compliance will be required to submit a Corrective Action Plan (CAP).