

IVIPS USE AND DISCLOSURE CONTRACT
ATTACHMENT E
DATA SECURITY REQUIREMENTS
For Web-based Access

1. Computer Security

Contractor shall maintain the computers that access DOL data by ensuring the operating system and software are updated and patched, such that they remain secure from known vulnerabilities as declared by security notifications (e.g., US-CERT, SANS, Microsoft). Contractor further agrees that the computer device(s) are installed with an Anti-Virus solution and signatures updated regularly.

2. Data Security

Contractor shall preserve the confidentiality, integrity and accessibility of DOL data with administrative, technical and physical measures that conform to generally recognized industry standards and best practices.

3. Data Storage

Contractor shall ensure any and all DOL data will be stored, processed, and maintained solely on DOL designated systems and that no DOL data at any time will be processed on or transferred to any other computing device or storage medium.

4. Data Transmission

Contractor shall ensure any and all electronic transmission or exchange of system and application data with DOL will be conducted via a secure solution (e.g., HTTPS, SFT, or equivalent).

5. Distribution of Data

Contractor shall ensure no DOL data of any kind shall be transmitted, exchanged or otherwise passed to other contractors/vendors or interested parties except on a case-by-case basis as specifically agreed to in writing by DOL. Contractor further agrees not to provide screen prints outside their control. Any screen print must be disposed of as referenced in the next section, *Destruction of Data*.

6. Destruction of Data

Contractor shall, upon termination of this Contract, erase, destroy, and render unrecoverable all DOL data and certify in writing using the *Attachment F, Destruction of Data* (located online at <https://fortress.wa.gov/dol/ivipsprod/>) that these actions have been completed within thirty (30) days of the termination of this Contract or within seven (7) days of the request of an agent of DOL, whichever shall come first. At a minimum, media sanitization is to be performed according to the standards enumerated by the National Institute of Standards and Technology (NIST), Guidelines for Media Sanitization, SP 800-88, Appendix A—<http://csrc.nist.gov/>.

7. Security Breach Notification

Contractor shall comply with all applicable laws that require the notification of individuals in the event of unauthorized release of DOL data or other event requiring notification. In the event of a breach of any of the Contractor's security obligations, or other event requiring notification under applicable law, Contractor agrees to the following:

- a) Notify by telephone and e-mail of such an event within 24 hours of discovery:
DOL Help Desk, phone: (360) 902-0111; email: hlbhelp@dol.wa.gov and
Contract Contact, phone (360) 359-4001; email: vsdisclose@dol.wa.gov.
- b) Indemnify, hold harmless and defend DOL and its trustees, officers, and employees from and against any claims, damages, or other harm related to such notification event.
- c) Mitigate the risk of loss and comply with any notification or other requirements imposed by law and implement any reasonable requirements from DOL that will mitigate future risk of loss.

8. Access to Data

Access to the data will be restricted to authorized users by requiring a login using a unique user ID and complex password or other authentication mechanism which provides equal or greater security. Further, passwords must be changed on a periodic basis. The sharing of user ID accounts and passwords is strictly prohibited.