

B.20. VA Cyber Security and Privacy Training Requirements for Contractor Employees

(a) Definitions. As used in this clause –

(1) *Contractor employee* means an employee of the prime contractor or of any subcontractor, affiliate, partner, joint venture, or team members with which the Contractor is associated. It also includes consultants engaged by any of those entities.

(2) *Information technology resources* means any equipment or interconnected system or subsystem of equipment, including telecommunications equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

(3) *VA sensitive information* means all Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of federal programs.

(b) All Contractor employees requiring access to VA information technology resources shall complete the following prior to contract performance and annually thereafter:

- (1) *successfully complete VA Cyber Security Awareness training;*
- (2) *successfully complete VA General Privacy training.*

(c) The Contractor shall provide a copy of VA Cyber Security training certificates and VA General Privacy training certificates for each applicable employee to the Contracting Officer prior to contract performance and annually thereafter. These online courses are located at the following web site: <https://www.ees-learning.net>

(d) All Contractor employees that do not have access to VA information technology resources, but do have access to VA sensitive information shall annually complete VA General Privacy training. The

Contractor shall provide a copy of VA General Privacy training certificates for each applicable employee to the Contracting Officer prior to contract performance and annually thereafter. This course is available online at <https://www.ees-learning.net/> or <http://www.vhaprivacytraining.net/frame.htm>

Failure to complete mandatory training within the timeframe required will be grounds for suspension or termination of all physical and/or electronic access privileges and removal from work on the contract until such time as the training is completed. In addition, the contract may be terminated for cause should the Contractor fail to meet mandatory training requirements.