ACCESS TO COMPANY'S CYBER RESOURCES

a) Seller personnel who are granted access to Company's cyber resources are subject to Company's cyber security policies and procedures. Cyber resources include, but are not limited to, computing systems, remote access, networks, associated servers, as well as data storage, mobile devices, switching, display, control devices, and information on these resources.
b) Access to Company's cyber resources by Seller may be permitted as required to perform this Agreement. Company's cyber resources may be used only to perform work authorized in this Agreement.
c) Computer software or documentation developed on or for Company cyber resources is the property of the Company and the Government unless provided otherwise in the Agreement.
d) Information or data furnished by Company or obtained from a Company computer by Seller personnel must be protected by the Seller to prevent disclosure to any person other than Seller's personnel or agents having a need to know unless such disclosure is authorized in writing by Company.
e) Classified material or information shall be protected in accordance with the security provisions of this Agreement, if applicable. If this Agreement does not include security provisions and the Seller is furnished or comes into contact with classified material or information, it shall be reported immediately to ORNL Laboratory Shift Superintendent at (865) 574-6606.
f) Files of any other user of Company's cyber resources may not be accessed without specific written permission from the user.
g) Seller's personnel or agents must acknowledge in writing that they have no expectation of privacy when using Company's cyber resources and they will permit access by the Company or other entity designated by Company to any Company cyber resources used by them during their time of access and for a period of three years thereafter.
h) Company reserves the right to monitor the use of cyber resources or electronic communications by reviewing the contents of such data on Company computers.
i) Computer passwords are issued to individuals and must not be shared. Computer passwords must be protected by Seller personnel or agents to prevent disclosure or potential disclosure of Company information. If password is compromised, Seller personnel or agents must notify Company immediately so that a new password can be issued.
j) Seller personnel or agents with access to ORNL cyber resources must complete ORNL Cyber Security Awareness training. If the scope of work is longer than one year, Seller personnel must take refresher training annually.
k) Any events or unusual situations involving Company's cyber resources must be reported to ORNL Laboratory Shift Superintendent at (865) 574-6606.
l) Company or DOE may unilaterally deny or revoke access to Company's cyber resources to an employee or agent of Seller.
m) Seller agrees to comply with any IT Special Provisions regarding cyber security associated with the Agreement.
n) The Seller shall insert this clause, in its entirety, in all subcontracts that may provide access to Company's cyber resources.
o) Seller agrees to protect all personally identifiable information (or PII), or sensitive personal information (or SPI) in accordance with applicable Federal, State, and other regulatory requirements for the collection, use, and protection of PII and/or SPI.