Antares Technologies / Andre Castillo / Jorge Perez / 04 Sep 2019

DFARS Compliance Self-Assessment Checklist

Complete

Inspection score	Failed items
20.17%	3

Company Name Antares Technologies
Contractor Andre Castillo
Audited by Jorge Perez
Conducted on 4th Sep, 2019 3:40 PM +08
Location Fourth and Madison Building, 909 5th Ave, Seattle, WA 98164, USA

Failed items

3 Failed

Inspection / Access Control

Do users with multiple accounts (privileged and nonprivileged) typically logon with the least privileged account when not performing privileged functions?	No
Do you prevent the execution of privileged functions by non-privileged users?	No

Inspection / Awareness and Training

Do users, managers, and system administrators receive annual training on potential indicators and possible precursors of an insider threat?	No

— Notes

Asked around and checked records, last training was held 2 years ago.

Inspection

3 Failed 20.17%

Access Control

2 Failed

Does the company have an authentication mechanism?	Yes
Does the company require users to log in to gain access?	Yes
Are account requests authorized before system access is granted?	Yes
Do you use access control lists to limit access to applications and data based on role and/or identity?	Yes
Do you have architectural solutions to control the flow of system data? (e.g., firewalls, proxies, encryption, and other security technologies)	Yes
Is there a division of responsibilities and separation of duties of individuals to eliminate conflicts of interest?	Partially
Do you only grant enough privileges to users to allow them to do their job?	Partially
— Notes Accounts for upper management have some functions available that isn't necessary for their scope of work. This was setup by the previous IT so I will have to review these accounts and verify which is needed and what's not.	
Do users with multiple accounts (privileged and nonprivileged) typically logon with the least privileged account when not performing privileged functions?	No
Do you prevent the execution of privileged functions by non-privileged users?	No
Is the system configured to lock the login mechanism for a predetermined time after a predetermined number of invalid login attempts?	Yes
— Notes Maximum of 3 login mistakes and then the account will be locked	
Is the system configured to end a user session after a predetermined period based on duration and/or inactivity of session?	Yes
— Notes 10 minutes of inactivity to be exact	
Do you run network and system monitoring applications to monitor remote system access and log accordingly?	Yes
Is cryptography used to protect the confidentiality and integrity of remote access sessions?	Yes

Does the system route all remote access through a limited number of managed access control points?	Yes
Is remote access for privileged actions (such as software installation) only permitted for necessary operational functions?	Yes
Is wireless access to the system authorized, monitored and managed?	Does Not Apply
Is wireless access encrypted according to industry best practices?	Does Not Apply
Has company management established guidelines for the use of mobile devices?	Yes
Does the company encrypt CUI on mobile devices?	Yes
Are guidelines and restrictions placed on the use of personally owned or external system access?	Yes
Are restrictions imposed on authorized individuals regarding the use of company-controlled removable media on external systems?	Yes
Is the proposed content of publicly accessible information reviewed prior to posting?	Yes

Awareness and Training 1 Failed

Is basic security awareness training provided to all system users before authorizing access to the system when required by system changes and at least annually thereafter?	Yes
Do all users, managers, and system administrators receive initial and annual training commensurate with their roles and responsibilities?	Yes
Do employees with security-related duties and responsibilities receive initial and annual training on their operational, managerial, and technical roles and responsibilities?	Yes
Do users, managers, and system administrators receive annual training on potential indicators and possible precursors of an insider threat?	No
— Notes Asked around and checked records, last training was held 2 years ago.	
Does security training include how to communicate employee and management concerns regarding potential indicators of an insider threat?	Yes

Completion

Name & Signature of Assigned IT Specialist  Jorge Perez 5th Sep, 2019 8:52 AM +08
Name & Signature of Contractor  Andre Castillo 5th Sep, 2019 8:52 AM +08