AEM SCREENS SECURITY CHECKLIST

Security Area	Checklist item	Yes/No/NA
AEM and Screens Software Updates	Has the latest AEM service pack been applied?	
	Has the latest AEM Screens Feature Pack been applied?	
	Are you using the latest available player software from https://download.macromedia.com/screens/?	
Physical Security	Have you disabled all unnecessary ports?	
	Have you secured cabling and hardware?	
	Are you using any containers if applicable?	
Network Security	Are you using an isolated subnet for your signage devices?	
	Does the isolated subnet allow access to the required endpoints including AEM, Analytics or other required services?	
	Have you secured your Wi-Fi using enterprise best practices?	
	If using synchronized playback have you allowed TCP 24503 for WebSocket only on the master device(s)?	
	Have you whitelisted the IP ranges of the player devices so only authorized devices can access the registration service on author?	
Operating System Security	Have you upgraded to the latest version of the operating system and applied all necessary security patches?	
	Have you disabled all unnecessary services and removed unnecessary applications?	
	Have you enrolled the device into device management to enforce enterprise policies?	
	Have you locked down the device to single application (player) kiosk?	
	Do you have a Standard Operating Procedures (SOP) in place for installing Operating System (OS) security updates over time?	
	Have you followed the security best practices for the OS in use? (such as anti-malware software, non-administrative user)	
Application Security	Have you disabled the Admin UI, Channel Switcher and Activity UI for production?	
	Have you minimized the log level for production?	
	Are you using https for connecting to AEM?	
	Are you using a CA signed certificate or an enterprise PKI? (not self-signed certificates)	
	Are you using TLS and not SSL v3?	
	Are you validating the registration token on device and AEM when registering?	

	Have you classified the data being used and that no Personally Identifiable Information (PII) or Protected Health Information (PHI) exists on device?	
	Have you configured monitoring E-mails, and do you have an SOP in place for responding to monitoring emails and handling non-pinging devices?	
Access Control	Do you have a Role Based Access Control (RBAC) identified and managed in-house?	
	Have you followed the principle of least privilege in providing access to authors, administrators and players using best practices from Adobe?	