

SUPPLIER ONBOARDING CYBERSECURITY CHECKLIST

Supplier Name:

Name of Person in Charge of IT:

IT Technical Contact:

Email:

Please provide response to each question below.

QUESTION		RESPONSE
1.	Does your company have a cybersecurity Acceptable Use Policy (AUP) that is enforced and communicated to all users/employees?	
2.	Does your company enforce password complexity for all users/employees on company computers?	
3.	Does your company use multi-factor authentication (MFA) for all users/employees?	
4.	Does your company allow VPN connections to your environment? If yes, is MFA enforced for all VPN connections?	
5.	Does your company have a formalized cybersecurity training program for all users/employees?	
6.	Does your company allow users/employees to use personal email to conduct company business? (i.e., Gmail, Yahoo, etc.)	
7.	Please describe how your company handles patching and security updates for your servers and endpoints.	
8.	Does your company use a managed anti-virus on company computers? If yes, how is it updated? Is automatic scanning and remediation performed? If yes, how often?	
9.	Are Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication Reporting and Conformance (DMARC) technologies implemented on your mail server? If yes, what are the configured settings for each?	
10.	Can your company enforce Sender Policy Framework (SPF) feature on the Wellbore Integrity Solutions email domain: wellboreintegrity.com?	
11.	Does your company have an email protection system in place to inspect all incoming emails?	
12.	Does your company have its own email domain?	
13.	Does your company enable firewalls on all company computers?	
14.	Does your company have a cybersecurity incident management and escalation plan that informs clients of incidents within 24-48 hours of the event?	