VENDOR INFORMATION SECURITY QUESTIONNAIRE

*Please provide responses to the following questions, as related to the services being provided to the Board of Water Supply (BWS) as well as in the context of any vendor system (endpoint, server, etc.) that will be interacting with the vendor service environment (for management, interaction with data, etc.) or BWS network (**indicate N/A where not applicable due to the type of services being provided**). Attach responses and copies of related documentation as appropriate.*

Any questions or concerns about this questionnaire can be sent to infosec@hbws.org.

SECTION 1 – VENDOR INFORMATION		
1	Vendor Name	
2	Who is the Point of Contact serving the BWS? Include phone, address, and email information	
3	Describe the services Vendor is providing to the BWS.	
4	Which non-U.S. countries will the vendor be utilizing to access BWS systems, sensitive data, or proprietary code?	

SECTION 2 – INFORMATION SECURITY PERSONNEL		
1	Who is primarily responsible for information security for Vendor?	
2	Who is the Vendor employee that serves as the BWS primary point of contact for information security issues? Include phone, address, and email information.	

SECTION 3 – ARCHITECTURE OVERVIEW		
1	Provide a general description of the architecture for the software, hardware and services being provided by Vendor to BWS. Attach network and architecture diagrams.	
2	Provide a general architecture and data flow diagram for the services Vendor is providing to BWS. Include diagrams illustrating where	

	BWS data is processed, stored, transmitted, and replicated.	
3	List the security compliance regulations or standards Vendor's services or infrastructure currently certified? What is the date of the latest certification? Attach copies of the certifications or reports.	

SECTION 4 – SECURE DEVELOPMENT LIFECYCLE		
1	Provide a description of Vendor's software/system development lifecycle and how security is integrated into the process of developing, managing, and maintaining the Vendor software, systems and services supporting BWS.	
2	Describe how Vendor addresses the vulnerabilities, threats and risks to Vendor's software and services, including those described in the latest OWASP Top 10 threats, MITRE ATT&CK framework and similar attack libraries.	
3	Are third party audits and penetration tests conducted and what is the frequency? Please provide a report on the last third-party security assessment of Vendor's software services.	
4	Describe the security controls imposed on software developers (especially developers remotely accessing and modifying source code) to ensure the security of Vendor systems and BWS data. In addition, from which non-U.S. countries are Vendor's developers and administrators accessing production code, systems, and data?	
5	Describe how Vendor manages supply chain risk to the software, hardware, products and/or services being provided to BWS and discuss how Vendor's procedures are consistent with the NIST guidance, "Defending Against Software Supply Chain Attacks"[1].	

[1] https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf

SECTION 5 – PHYSICIAL SECURITY		
1	List the datacenters (and their physical addresses) whose infrastructure is utilized to support the application, software, storage and processing services Vendor is providing to BWS.	
2	Describe Vendor's access management policies and procedures (for users and systems) that protect the Vendor's systems and infrastructure to ensure the security of BWS's data.	
3	Are third party audits and penetration tests conducted on the physical infrastructure (e.g., datacenter) and what is the frequency? Attach copies of the latest audit and/or assessment reports for each datacenter supporting BWS.	

SECTION 6 – NETWORK SECURITY		
1	Describe how the Vendor protects the application and data processing services Vendor is providing BWS from external network threats and attacks	
2	Describe which transmissions of data between BWS (including its customers and business partners) and Vendor are encrypted and unencrypted.	
3	What type and level of encryption is Vendor providing to BWS for the services being provided?	
4	Describe the general network security controls to monitor and protect remote access connections to Vendor's infrastructure by employees and contractors.	

SECTION 7 – END POINT SECURITY AND REMOTE WORK		
1	Please provide a general description of how Vendor's server infrastructure and application services are protected from malware, including ransomware.	
2	Please provide a general description of how Vendor's endpoints are protected from	

	malware, including ransomware. Are these solutions being monitored and responded to by the vendor or vendor's MSSP when detections are raised?	
3	What is your remote work policy, including work from home policy? How do you ensure remote workers operate in a secure environment with secure tools when working remotely and handling/accessing sensitive BWS data and services?	

SECTION 8 – CONFIGURATION, VULNERABILITY, AND PATCH MANAGEMENT		
1	Describe Vendor's policies, procedures, and schedules for applying configuration changes to its services? How does Vendor minimize the impact on customer operations and data?	
2	Provide a general description of how Vendor manages software vulnerabilities on its infrastructure and the infrastructure used by Vendor to provide services to BWS.	
3	Provide a general description of Vendor's procedures to prioritize and apply patches to software to address security and operational issues.	

SECTION 9 – DATA PROTECTION AND LOSS PREVENTION		
1	BWS may store and process sensitive information (including electronic personal health information, personally identifiable information, and financial information) on Vendor infrastructure. How does Vendor provide protection for sensitive BWS data residing on Vendor's infrastructure?	
2	Is BWS's data always encrypted at-rest on Vendor's systems?	
3	How is BWS's data protected to prevent unauthorized access by Vendor's other customers, through the shared infrastructure including the application, datastore, and virtualization environment?	
4	When BWS deletes data during normal operations or if it decides to terminate service, to what extent is the data	

	recoverable after deletion and what is the process for recovery?	
5	How does Vendor ensure BWS data is not recoverable after terminating service?	

SECTION 10 – SECURITY MONITORING AND NOTIFICATION		
1	Provide a general description of Vendor's security monitoring capabilities and procedures to protect Vendor infrastructure, systems and customer data.	
2	What are the severity levels that Vendor applies to the services being provided to BWS?	
3	What notification thresholds need to be met for Vendor to notify BWS of an incident requiring incident response?	

SECTION 11 – INCIDENT RESPONSE		
1	Provide a general description of Vendor's incident response policies and procedures in the event of a cybersecurity incident involving BWS data.	
2	What audit and forensic investigation support will Vendor provide to BWS when responding to an incident?	

SECTION 12 – RECOVERY		
1	Provide Vendor's Service Level Agreement (SLA) and uptime guarantee for services it provides to BWS.	
2	What are Vendor's SLAs for backing up BWS data?	
3	What are Vendor's SLAs for restoring BWS data from backups?	
4	What are Vendor's SLAs for restoring BWS services?	

SECTION 13 – Artificial Intelligence

1	Provide a general description of the use of artificial intelligence and machine learning in the services being offered.	
2	Please describe any measures implemented to ensure the integrity and security of the artificial intelligence and underlying models.	
3	Please describe the interactions between BWS data and Vendor's artificial intelligence.	
4	Will BWS data be used in training the Vendor's artificial intelligence or machine learning models? If yes, does BWS have the option to opt out of participation?	

SECTION 14 – SECURITY FEATURES		
1	Please list the features that enhance or impact the security of Vendor's products/services or the security of BWS's data being processed, stored, and managed by Vendor. Indicate which features are "Optional (Vendor offers this feature, but it is an optional module)", "Additional Cost" (Vendor offers this feature for additional cost); or "Future" (Vendor will offer this feature in the future – please indicate timeline).	