BOARD OF WATER SUPPLY

CITY AND COUNTY OF HONOLULU
630 SOUTH BERETANIA STREET
HONOLULU, HI 96843
www.boardofwatersupply.com

INFORMATION SECURITY QUESTIONNAIRE

Date: _____

Vendor Name: _____

Point of Contact Name: _____

Phone Number: (___) ___-____

Mailing Address: _____

Email Address: _____

I affirm that the information provided in this questionnaire is accurate as of the date noted above.

_____ _____

Signature *Title*

Description of Services the Vendor is providing the Board of Water Supply (BWS) as related to Data being requested or produced, access to, or provisioning of, IT Resources (Equipment, Network, Applications, Cloud Services – IaaS, PaaS, SaaS, etc., whether BWS's or Vendor's), etc. *Attach additional pages if necessary*:

Who is primarily responsible for your organization's Information/Cyber Security?

Name: _____
Phone Number: (___) ___-____
Mailing Address: _____
Email Address: _____

Who is the BWS's primary point of contact for Information/Cyber Security issues in your organization? (if different from above)

Name: _____
Phone Number: (___) ___-____
Mailing Address: _____
Email Address: _____

*Please provide responses to the following questions, as related to the services being provided to the BWS (**indicate N/A where not applicable due to the type of services being provided**). Attach responses and copies of related documentation as appropriate.*

Section 1 - Architecture Overview

(a) Please provide a general description of the architecture for the software, hardware data storage, and/or the methodology for services being provided or utilized by Vendor to fulfill the engagement with the BWS.

(b) Please provide a general architecture and data or process flow diagram for the services that the Vendor is providing the BWS to include where BWS data is processed, stored and replicated, including physical endpoints, servers and cloud-based platforms.

(c) Under which security compliance regulations or standards is Vendor's services or infrastructure currently certified or audited? Please provide copies of the certifications or audit reports.

Section 2 - Security Development Lifecycle

(a) 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 the BWS.

(b) 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/or similar attack libraries.

- Are third party audits and penetration tests conducted on Vendor's service delivery infrastructure, software and systems and what is the frequency?
- Please provide a report on the last third-party security assessment of Vendor's software services.

(c) Describe the security controls imposed on software developers (especially developers remotely accessing and modifying source code) to ensure the security of Vendor's systems and customer data.

- From which non-U.S. countries (if any) are Vendor's developers and administrators accessing code, systems and data?

Section 3 - Physical Security

(a) List the datacenters (and their physical addresses) whose infrastructure is utilized to support the application, software, storage and processing services Vendor is providing the HBWS.

(b) 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 the BWS data.

(c) Are third party audits and penetration tests conducted on the physical infrastructure (e.g. datacenter) and what is the frequency?

- Please provide copies of the latest audit and assessment reports for each datacenter supporting the BWS.

Section 4 - Network and Data Security

(a) Describe how the Vendor protects the application and data processing services Vendor is providing the BWS, or using to fulfill its engagement with BWS, from external network threats and attacks.

(b) Describe which transmissions of data between the BWS (including its customers and business partners) and Vendor are encrypted and unencrypted.

(c) What type and level of encryption is Vendor providing to the BWS for the services being provided?

(d) Describe the general network security controls to monitor and protect remote access connections to Vendor's infrastructure by employees and contractors.

Section 5 - Anti-Malware

(a) Please provide a general description of how Vendor's server infrastructure and application services are protected from malware.

(b) Please provide a general description of how Vendor's endpoints are protected from malware.

Section 6 - Configuration, Vulnerability and Patch Management

(a) 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?

(b) Provide a general description of how Vendor manages software vulnerabilities on its infrastructure.

(c) Provide a general description of Vendor's procedures to prioritize and apply patches to software to address security and operational issues.

Section 7 - Data Protection and Loss Prevention

(a) Since BWS may be providing sensitive information (including electronic personal health information, personally identifiable information, financial information, water system information, etc.) to be stored and processed on Vendor's infrastructure, how will Vendor provide protection and security for this information (and any information developed/derived from this information) while in its custody?

(b) Is the BWS data encrypted at-rest at all times on Vendor's systems?

(c) How is the BWS data protected to prevent unauthorized access by Vendor's other Customers, other vendors, employees, etc., through any shared infrastructure including the application, datastore, and virtualization environment used in rendering of services?

(d) If the BWS decides to obtain a copy of all data stored with Vendor, please provide a detailed description of the process to obtain a copy and indicate whether the BWS will be charged additional fees.

(e) When the 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?
- How does Vendor ensure the BWS data is returned, deleted from Vendor's infrastructure and not recoverable after termination of service?

Section 8 - Security Monitoring and Notification

(a) Provide a general description of Vendor's security monitoring capabilities and procedures to protect Vendor's infrastructure, systems and customer data.

(b) What are the severity levels that Vendor applies to the services being provided to The BWS?

(c) What notification thresholds need to be met for Vendor to notify the BWS of an incident (security or otherwise) involving Vendor's services and the BWS data requiring incident response?

Section 9 - Incident Response

(a) Identify the Cyber Security Insurance, coverage and relevant limits currently carried by Vendor.

(b) Provide a general description of Vendor's incident response policies and procedures in the event of a cybersecurity incident involving the BWS data.

(c) What audit and forensic investigation support will Vendor provide to the BWS when responding to an incident?

Section 10 - Recovery

(a) Provide Vendor's Service Level Agreement (SLA) and uptime guarantee for services it provides to the BWS.

(b) What are Vendor's SLAs for backing up the BWS data?

(c) What are Vendor's SLAs for restoring the BWS data from backups?

(d) What are Vendor's SLAs for restoring the BWS services?

Section 11 - Security Features

Please list any additional features that enhance or impact the security of Vendor's offerings or the security of The BWS data being processed, stored and managed by Vendor. Indicate where applicable features that are "Optional", "At Additional Cost" or "Future Implementation" per below.

(a) Optional (Vendor offers this feature, but it is an optional module)

(b) Additional Cost (Vendor offers this feature for additional cost)

(c) Future (Vendor will offer this feature in the future – please indicate timeline)

BWS Cybersecurity Disclosure

The Board of Water Supply (BWS), as a semi-autonomous City and County of Honolulu agency within the National Critical Infrastructure, Water and Wastewater Systems Sector (as designated by the Department of Homeland Security), is bound by national policy to strengthen and maintain secure, functioning and resilient systems. This includes ensuring cybersecurity actions are appropriate to support this policy.

Furthermore, as a recipient and provider of personal, private, or sensitive information, cybersecurity incidents could result in adverse impacts to both its Information Technology systems (IT), as well as the Operational Technology systems (OT), requiring timely response and remediation to mitigate consequences.

Cybersecurity incidents could result from unintentional actions, or from targeted and deliberate attacks by individuals, entities or nation state actors attempting to gain access to BWS IT/OT, intent on disrupting operations, damaging assets, or impacting BWS or customer finances. The attacks are often due to attempts at hacking, phishing, viruses, malware, social engineering, and even staff complacency.

To mitigate the risks to BWS IT/OT systems and operations, and the data contained within, the BWS invests in a layered cybersecurity defense program that includes technical toolsets, educational awareness, proactive threat monitoring, and appropriate policies. Additionally, in this layered cybersecurity defense posture is the inclusion of a cyber insurance policy encompassing first party costs of mitigation and loss due to business interruption, data recovery and/or cyber extortion, as well as third party loss resulting from claims due to an event.