Hawaii State Dept. of Health (DOH) Information Security 3rd party Accreditation Questionnaire

Introduction

Hawaii Department of Health (DOH) has information security program and control requirements in place for the safeguarding of our sensitive information. These requirements are applicable regardless of whether such information is stored, processed, or transmitted on DOH systems or by a third party. These questions are intended to determine if the appropriate program and control requirements are in place for the protection of our sensitive information at your organization.

Instructions for Completion

Please answer each question and provide relevant discussion in the fields provided. Please attach documentation supporting your response to the questions. When providing attached evidence please use the reference ID of the Section and Question Number when naming the attachment. For example, if you have a Type II SAS70 or SSAE 16 you would answer the question Yes and then attach the report with the Reference ID of A.1. Please use the discussion field to explain your Yes or No answers in detail. This discussion will assist in the review of these answers by the Information Security Office and minimize the follow-up required to complete this accreditation.

Once the questionnaire is completed please submit the document and any attachments along with a signed copy of the representation letter attached here:

QHS -Company representation Letter

If your services include providing access to a web application for use by DOH (e.g., SaaS) or storage, processing, or transmission of DOH data on externally accessible systems please also provide a completed copy of the Security Testing Authorization Letter attached here:

Security Testing - Authorization letter.d

A. Policies and Procedures

	Accreditation				
	Question	Yes	No	Discussion	Reference ID
1	Do you have a Type I, Type II SAS70, or SSAE 16 report? Please provide.	☐	☐		
2	Do you have a current Vulnerability/Risk Assessment? Please provide.	☐	☐		
3	Do you have other accreditation or third party assurance reports relating to Information Security or your IT Control Environment? Please provide.	☐	☐		
4	If your services include the hosting of a web application for use by DOH, will your organization consent to the DOH Information Security Office performing security testing against the web application and supporting systems/infrastructure? Please refer to Appendices for an example authorization letter that would be executed to cover testing activities.	☐	☐		
5	If you will not allow such testing, will you be able to provide a recent (within the last six months) independent 3rd party report indicating that no critical or high risk issues were identified within the web application and supporting systems/infrastructure?	☐	☐		
	Information Security Policy				
	Question	Yes	No	Discussion	Reference ID
6	Do you have Information Security Policies that will govern DOH' data? Please provide.	☐	☐		
7	If not part of your Information Security Policies do you have a separate Acceptable Use and Privacy policy that will govern DOH' data? Please provide.	☐	☐		

8	Have your Information Security Policies and Acceptable Use and Privacy policies have been distributed and acknowledged by your employees? Please provide documentation.	☐	☐		
9	Please provide your Information or Data Classification Policy and indicate which category DOH data will be assigned at your organization.				
	Regulatory: Please complete if handling DOH' PII, PCI or PHI				
	Question	Yes	No	Discussion	Reference ID
10	Will you implement special measures for protection of DOH' data containing **Personally Identifiable Information (PII)**? Please explain. .	☐	☐	*Note NA in the discussion field if you your services do not handle PII*	
11	How will you protect DOH' financial data (e.g., **credit / debit card numbers**)? Are you PCI compliant? Please provide appropriate evidence.	☐	☐	*Note NA in the discussion field if you your services do not handle PCI.*	
12	Will you handle DOH' **protected health information**? Are you HIPAA compliant? Please provide appropriate evidence.	☐	☐	*Note NA in the discussion field if you your services do not handle PHI.*	
13	Have you ever had a security incident (or incidents) that led to the breach of PII, PCI, or HIPAA related information? Please explain	☐	☐		

B. Operations Security

	Incident and Breach Handling				
	Question	Yes	No	Discussion	Reference ID
14	Do you have a Computer Security Incident Response Plan and Procedure related to DOH data? Please provide.	☐	☐		
15	Did you review and test the Computer Security Incident Response Plan in the last 12 months? Please explain.	☐	☐		
16	Have you documented all security incidents that have occurred as well as the action taken in response to each incident? Please provide a summary of any major incidents that could have potentially impacted DOH data and the actions taken to remedy the issues that led to the incident?	☐	☐		
17	Do you have a privacy breach notification process that is aligned with Hawaii State Law requirements for DOH' data? Please provide a copy of your breach response process. Information on Hawaii State requirements for PII breach notification can be	☐	☐		

	found here: http://hawaii.gov/dcca/id_theft_info/laws/ID_Theft_Info_For_Businesses				
	Outsourcing				
	Question	Yes	No	Discussion	Reference ID
18	Do you outsource any portion of the services that you will be providing to DOH?	☐	☐		
19	How do you ensure that the outsourced service provider is adequately protecting DOH information? Please explain.	☐	☐		
20	Have you identified any significant risks to DOH information by outsourced service providers? Please explain.	☐	☐		
	Logical Access Control				
	Question	Yes	No	Discussion	Reference ID
21	Please provide your password policies and standards that will be used to protect DOH data	☐	☐		
22	Please provide procedures implemented to ensure that user access to DOH' data is reviewed in a timely manner.	☐	☐		
23	Please provide procedures implemented to ensure that multiple failed login attempts to access DOH' data is reviewed				
	Patch Management				
	Question	Yes	No	Discussion	Reference ID
24	Do you have a formal documented Vulnerability/Patch Management Process to safeguard technology handling DOH' information? Please provide documentation to demonstrate that the process is implemented, monitored, and performing as expected.	☐	☐		
	Personal				
	Question	Yes	No	Discussion	Reference ID
25	Do you have an Information Security Officer? Please provide Org Chart showing the position of the security function within the organization.	☐	☐		
26	Do you have other supporting roles associated with information security (e.g., Privacy Officer, Security Analysts, Security Engineers)? Please provide Org Chart showing positions.	☐	☐		
27	Do you perform security checks (e.g., background) for each new hire with access to DOH' data? Please explain background check process.	☐	☐		

	Physical				
	Question	Yes	No	Discussion	Reference ID
28	Please identify all locations that DOH data and resources reside (e.g., servers, employee laptops, and desktops).	☐	☐		
29	Please identify systems and infrastructure supporting DOH data and processes are located? Are such locations furnished with appropriate environmental controls?	☐	☐		

C. Network and Host Security

	Host based Protection				
	Question	Yes	No	Discussion	Reference ID
30	Do you have anti-virus (AV) and/or Host-based IPS (HIPS) installed on systems with access to DOH information? Please describe	☐	☐		
31	Do you have adequate proof that the AV and HIPS alerts are being monitored on a regular basis? Please provide.	☐	☐		
32	Do you have adequate documentation that the AV or HIPS signatures are being updated on a regular basis? Please provide.	☐	☐		
33	Do you have secure base builds for the systems that will hold DOH data? Please provide description of configurations being used.	☐	☐		
	Network Perimeter Protection:				
	Question	Yes	No	Discussion	Reference ID
34	Do you have a network diagram providing firewall and security device locations for systems that protect DOH' data? Please provide a description or evidence as appropriate.	☐	☐		
35	Do you have adequate firewall technologies to protect systems supporting the technology associated with the services in this RFP? Do you have web application firewalls in place for protection of web applications that may be used to store,	☐	☐		

	process, and transmit DOH data? Please provide a description or evidence as appropriate.				
36	Do you have adequate intrusion detection / prevention technologies in place to protect DOH data and the systems associated with the storage, processing, transmission of the data? Please provide a description or evidence as appropriate.	☐	☐		
37	Do you have adequate proof that the security devices mentioned above are being monitored on a 24x7 basis and a procedure is in place for handling security events? Please provide a description or evidence as appropriate.	☐	☐		

D. Data protection

	Encryption				
	Question	Yes	No	Discussion	Reference ID
38	Do you have standard encryption guidelines for the organization that will be applied to DOH' data? Please provide.	☐	☐		
39	Do you have a list of all systems that will be used in the storage, processing, or transmission of DOH resources and the type of encryption being used? This includes encryption of end-points (e.g., workstations/laptops) that would be used to store, process, and transmit DOH data. Please provide description or evidence as appropriate.	☐	☐		
40	Do you have evidence or attestation that backup tapes storing DOH data are encrypted? Please provide.	☐	☐		
	Data Transmission				
	Question	Yes	No	Discussion	Reference ID
41	Do you have a list of all types of communications (e.g., VPN, email, FTP) that pertain to the exchange of DOH data with DOH and other organizations? Please provide.	☐	☐		
42	Will you protect (e.g., encrypt) all communications of DOH data? Please describe and provide evidence as appropriate.	☐	☐		
	Data Protection and Sharing				
	Question	Yes	No	Discussion	Reference ID

43	Will DOH data be located or processed on shared physical servers, drives, or storage media with other non-DOH resources? Please provide information.	☐	☐		
44	Is DOH data located in a shared database with other non-DOH resources? Please provide information.	☐	☐		
45	Do you have data sharing agreements and details (e.g., communication methods, protection mechanisms) with other entities aside from DOH that impact DOH resources and data? Please provide.	☐	☐		

By signing below I, <insert name>, acknowledge that the answers that have provided to this questionnaire are complete and accurate as to the best of my knowledge.

Printed Name: _____

Signature: _____

Title: _____

Date: _____

<<Please insert company letterhead>>

<<Insert Date>>

[Security Coordinator's name]

Department of Health

[Program Name]

[Address]

Dear Mr. [Sec. Coordinator's name]:

I have reviewed and completed the Hawaii Department of Health's 3rd Party Accreditation Questionnaire.

The responses provided are true and accurate to the best of my knowledge as of the date of this disclosure.

Signed on behalf of <<Insert company name>>,

<<Company Representatives Name>>

<<Representatives Title>>

<<Company Name>>

<PLEASE PRINT ON VENDOR COMPANY LETTERHEAD AND SIGN>

<Insert Date>

[Sec. Coordinator's Name]
[Address]

Dear [security coordinator's name]:

This letter sets forth the terms for permission and authorization to conduct web application vulnerability security testing against specific <VENDOR COMPANY> applications as part of Hawaii Department of Health (DOH) security certification activities.

<VENDOR COMPANY> is aware of the risks associated with security testing on the production system and has taken the necessary pre-testing steps (e.g. data backup, internal communications) to help minimize these risks.

This letter of authorization is intended to enable the Health Information Systems Office (HISO) to perform these tests without concern for being subject to action by <VENDOR COMPANY> for unintended network or system interruptions or unauthorized access to <VENDOR COMPANY> computer networks associated with the application being tested.

By acceptance of this letter and execution of the web application vulnerability security test, DOH agrees to hold confidential all related testing results.

I acknowledge that DOH's HISO is authorized to conduct the web application vulnerability scanning and testing on the URL's listed below.

I, <INSERT NAME AND TITLE OF PERSON AUTHORIZING THE TESTING>, authorize DOH's HISO to perform security testing activities against the following:

A. **List of Web Application(s)**

URL's

B. The security testing is authorized to occur between

1. <INSERT THE DATE AND TIME USING HAWAII STANDARD TIME – PLEASE SPECIFY A RANGE AS TESTING WILL TAKE MORE THAN ONE DAY>

Signed on behalf of <VENDOR COMPANY>,

_____

<Name>
<Title>
<VENDOR COMPANY>