**Cloud Vendor Security Questionnaire and Assessment**

|  |  |  |
| --- | --- | --- |
| **Item****No.** | **Description** | **Response** |
| **0.0** | DOHMH Project Name and ID? |  |
| **Vendor** |
| **1.0** | Vendor/Company Name? |  |
| **1.1** | Company web site? |  |
| **1.2** | Company Main Office Address? |  |
| **1.3** | Primary Contact Info (Name, email, phone)? |  |
| **1.4** | Primary Technical Contact Info (Name, email, phone)? |  |
| **1.5** | Any security certificates or support document? e.g. FedRAMP, HIPAA, PCI, SOC1, SOC2, ISO27001, SOC1/SSAE16/ISAE3402 Security Assessment Document (SAD) etc.  |  |
| **Solution** |
| **2.0** | Solution type (IaaS, PaaS, SaaS)? |  |
| **2.1** | Solution Category (Security, Case Management System, Storage, Survey, Collaboration etc,.)? |  |
| **2.2** | Does your solution partner with other cloud providers to host your solution? |  |
| **2.3** | Solution host location (on premise, AWS, MS Azure etc)? |  |
| **2.4** | COTS product or product with custom code? |  |
| **2.5** | Does your company provide a copy of topology/data flow diagram? |  |
| **2.6** | Does the solution have a staging Environment Available? |  |
| **Data** |
| **3.0** | What is the solution of data encryption at rest? Encryption level? |  |
| **3.1** | What is the solution of data encryption In transit? Encryption level? |  |
| **3.2** | Does the solution have Data Loss Prevention (DLP) functions? |  |
| **3.3** | What is the data retention policy and plan for this solution? |  |
| **3.4** | Data location (On Premise, in cloud, In U.S, out side U.S.)? |  |
| **3.5** | What is the data backup plan? Schedule? Location of backup files? |  |
| **Security** |
| **4.0** | Does the solution have network segregation with firewall based on Data Classification, client or there is no network segregation? |  |
| **4.1** | What is the solution password policy and standards? |  |
| **4.2** | Can the solution support and integrate with DOHMH Azure AD for Single Sign On (SSO)? |  |
| **4.3** | Can the solution support multi-factor authentication (MFA)? What type? |  |
| **4.4** | Does the solution have an audit logging system? |  |
| **4.5** | Can the solution track login attempts, both successful and unsuccessful log? |  |
| **4.6** | Can DOHMH access the audit log? |  |
| **4.7** | Does the solution have Disaster Recovery plan? |  |
| **4.8** | Does your company have an Access Control Plan (ACP), Who provision account, who approve account changes, approval process and document management and frequency of account status review? |  |
| **4.9** | Does your company have an Incident Response Policy and Protocol to notify DOHMH when an incident occurred? |  |
| **4.10** | Can your company provide a recent penetration testing report to DOHMH? |  |
| **4.11** | Can your company allow NYC Cyber Command Center to conduct a penetration testing on your staging environment? |  |
| **4.12** | Can your company provide a recent vulnerability Scanning report to DOHMH? |  |
| **4.13** | Does the solution have a Mobile Device Management (MDM) features? |  |
| **4.14** | Does the solution send out outbound email to registered users or public users? |  |
| **4.15** | Does the solution support email DKIM/DMARC? |  |
| **Physical Security** |
| **5.0** | Does your company have a physical and Environmental safety plan? |  |
| **5.1** | Does your company have access ID control? |  |
| **5.2** | Does your company track guest entry/login information? |  |
| **5.3** | Does your company have Surveillance Monitoring system? |  |
| **Legal** |
| **6.0** | Any Legal Agreement available with DOHMH or NYC DOITT (contract, Cloud Service Agreement or subscription of service)? |  |
| **6.1** | Any DOHMH IRB Approval or Business Associate Agreement (BAA) available with DOHMH (For Patient Info Related Project)? |  |
|  | Today’s Date (yyyy-mm-dd): |  |