|  |
| --- |
|  |
| Security Questionnaire For Hosted Solutions |
|  |
|  |
| **The purpose of this document is to identify security configurations, policies and standards for third party organizations hosting Seattle Genetics systems or data.** |

|  |
| --- |
|  |

Please submit this completed questionnaire to:

Chad Taylor, Principal Cyber Security Engineer [ctaylor@seagen.com](mailto:ctaylor@seagen.com)

VENDOR: SOLUTION:

| *Section* | *Description* | *Vendor Response* |
| --- | --- | --- |
| *Supporting Documentation* | [1.1] Please include the following documentation when submitting this questionnaire to Seattle Genetics:     1. Architecture diagram that specifies security configurations (as applicable) 2. Encryption leveraged by client-server connectivity including version(s) (TLS,SSL, etc) 3. Data at rest encryption 4. Incident Response Plan and any other formal Security Policy documentation available 5. SSAE SOC 2 report for hosted services 6. Include certification information, i.e. ISO 27000, SSAE 16, etc. |  |
| *Roles & Responsibilities* | [1.2] Has your organization formally appointed a central point of contact for security coordination?  a)    If so, whom, and what is their position within the organization? |  |
| *External Parties* | [1.3] Do you work with third parties, such as IT service providers, that will have access to Seattle Genetics data? If yes, please list.  a)    Does your organization have Non-Disclosure agreements in place with these third parties? | N/A |
| *Data Governance & Compliance* | [1.4] Describe your process for Data Governance and Compliance.   1. Will this system collect data or information of any type regarding individuals located in the EU? 2. How will access to Seattle Genetics data be governed? 3. Describe the physical access controls in place that prevent unauthorized access to the facilities which will host Seattle Genetics data. 4. Describe the process to review access control logs 5. How often can Seattle Genetics review these logs? 6. What happens to Seattle Genetics data once this relationship or contract is terminated? 7. Do you have an Incident Response Plan? 8. Do you have a Data Breach Notification policy? 9. Does a process exist to identify new laws and regulations with IT security implications? (e.g., new state breach notification requirements)? 10. Do you have a formal Vulnerability Management Program? 11. What is your Patch Management process? | We are using and accessing Ultimate Software cloud infrastructure; we are following and using the same Data Governance that Ultimate Software is using. |
| *Password and Access Management* | [1.5] What level of management control will Seattle Genetics have over passwords and access?   1. What type of password requirements can be managed by Seattle Genetics? 2. Do you support Multifactor Authentication (MFA)? 3. At what level can Seattle Genetics manage access to the application, i.e. role-based access? 4. Do you support Single Sign-On via Okta (SAML 2.0)? 5. Which web browsers & versions do you support? | 1. We are using the same password requirements that Ultimate have to access their system, they will be the one giving us access to the client’s environment 2. Yes to access Ultimate Software infrastructure and MFA is supported 3. Ultimate Software will be the one giving us access to the application, which supports role-based access. 4. Yes, I believe Ultimate Software support Single Sing-on |
| *Service Level Agreements* | [1.6] Please list the Service Level Agreement (SLA) in place with regard to this application.   1. What are the defined SLAs levels available to Seattle Genetics? 2. How are SLA statistics reported? |  |
| *Disaster Recovery and System Availability* | [1.7] Are there formal procedures in place for Business Continuity and/or Disaster Recovery?   1. If yes, please list. 2. In which physical location(s) will Seattle Genetics data be hosted? 3. What controls are in place to mitigate attacks on the host hardware, software or network? i.e. Denial of Service Attacks, Virus/Malware outbreak, etc. | We are using and accessing Ultimate Software cloud infrastructure data is and will still be hosted within Ultimate Software. |
| *During Employment – Training, Education & Awareness* | [1.8] Have your employees been provided formal security awareness training?   1. Are your employees required to review and signoff on the training? 2. Are your employees required to sign off on a formal acceptable use or other security policy? | Yes – we went to the same rigorous training the same that Ultimate Software employees take for security awareness. |
| *Background Checks* | [1.9] Does your organization perform background checks to examine and assess an employee’s or contractor’s work and criminal history?   1. If yes, please describe the process and third parties utilized for the background checks. |  |
| *Prior to Employment - Terms and Conditions of Employment* | [1.10] Are your employees required to sign a non-disclosure agreement?   1. If so, are employees required to sign the non-disclosure agreement annually? 2. How often is this process reviewed and renewed? |  |
| *Termination or Change in Employment* | [1.11] Do you have a formal process to manage the termination and or transfer of employees who would have access to Seattle Genetics data?   1. If so, please list. |  |