**Knowledge Anywhere**

* 1. **Frequently Asked Security Questions for SaaS**

1. What are Knowledge Anywhere’s data security policies?
   1. **The client Learning Management System will be installed on a server hosted by Amazon Web Services (AWS).  The system will be audited for SOC 1, SSAE 16, and ISAE 3402. Knowledge Anywhere does not solicit external 3rd party audits of our systems or processes. Our IT security policies are agreed upon by all staff as a condition of employment and are reviewed/updated periodically for efficacy. Additionally, our systems generally do not house sensitive information beyond level 2 and are therefore considered low risk for security breach ramifications. Definitions of security levels as classified by Knowledge Anywhere are stated below:**
      1. **Level 1—Low Sensitivity  
         Information at this level requires a minimal amount of protection. This level includes information that is considered to be in the public domain, such as names and email addresses. At this level, any disclosures could be reasonably expected not to have an adverse effect. Regardless, Knowledge Anywhere realizes that all information should be considered important, and will always make reasonable precautions for its safeguard.  
           
         Unintentional alteration or destruction is the primary concern for low sensitivity information.**
      2. **Level 2—Moderately Sensitive  
         Level 2 or Moderate Sensitivity includes data that is important to Knowledge Anywhere and our customers, and therefore will be protected against acts that are considered to be malicious and destructive. However, disclosure problems are usually not significant since this type of data is often collected for analytical reasons.  
           
         This level includes information that pertains to training materials, basic learner profile information, and learner education transcripts whose release or distribution outside of Knowledge Anywhere and its customers should be controlled. Access to Level 2 data needs to be restricted only to a limited degree. The data must be protected from unauthorized alteration or modification, however, it may be disclosed in some format eventually.  
           
         Moderately sensitive data can include information that must be protected to meet Privacy Act requirements. At this level, unauthorized disclosures could cause embarrassment to an individual.**
      3. **Level 3—High Sensitivity  
         Everyone at Knowledge Anywhere will be most aware of the protection requirements for Level 3 or High Sensitivity information. This level covers the most sensitive information collected and maintained within Knowledge Anywhere hosted applications and requires the greatest security safeguards at the user level.  
           
         This data could include computerized correspondence and document files that are regarded as highly sensitive and/or critical to an organization, and therefore must be protected from unauthorized alteration, modification, and/or premature disclosure; proprietary information that has inherent informational value, such as trade secrets, financial data that is used to authorize or make payments to individuals or organizations, automated systems or records subject to the privacy regulations for which unauthorized disclosure would constitute a clearly unwarranted invasion of personal privacy.  
           
         Highly sensitive data must be protected from unauthorized disclosure.**
      4. **Level 4—High Sensitivity and National Security  
         This level of data does not typically apply to solutions developed and hosted by Knowledge Anywhere. Separate, specific considerations will be considered and outlined if a project of this nature is requested of Knowledge Anywhere.**
2. Can I have a copy of Knowledge Anywhere’s security policy, or at least that part of it which applies to the hosted solution?
   1. **The Knowledge Anywhere internal staff follows standard security protocols for secure user access administration.  The system information security policy provided by the Amazon Web Services IT Support is followed by the Knowledge Anywhere staff.  This policy is maintained and updated on the site:** [**http://aws.amazon.com/security/**](http://aws.amazon.com/security/)**. Knowledge Anywhere IT policies may be provided upon written request and under separate cover.**
3. What software development processes does Knowledge Anywhere use to ensure that software products that are part of the solution are free of security defects?
   1. **Knowledge Anywhere implements standard code protocols to prevent security breaches by adhering to standards limiting the application to vulnerabilities like Cross-site scripting attacks (XSS) or SQL Injection attacks.  All code changes are initiated by customer requests and formal team oversight for Service Order processes documents the change. The release management process provides safeguards against possible code updates that may introduce security defects from development through production implementation. Knowledge Anywhere’s engineering staff (re)certify on OWASP standards annually.**
4. Would Knowledge Anywhere clients ever have occasion to log on to hosted infrastructure systems in any way while using a Knowledge Anywhere solution or product?
   1. **No. Persons outside of Knowledge Anywhere or their approved vendors are not allowed direct access to any server located on site or at data centers utilized by Knowledge Anywhere.**
5. How quickly would Knowledge Anywhere inform a client if a security incident or data exposure occurred? What steps would be taken to mitigate any damage to clients if such an incident occurred?
   1. **The Amazon Web Services IT Support provides 24/7 notification of any incident that may be encountered on the servers.  This information is available on the site:** [**http://aws.amazon.com/security/security-bulletins/**](http://aws.amazon.com/security/security-bulletins/) **and the customer may utilize the rss feed as an alternative:** [**http://aws.amazon.com/rss/security.rss**](http://aws.amazon.com/rss/security.rss)
   2. **If a breach were identified and determined to be credible and impactful, Knowledge Anywhere would notify the client point of contact based on the service contract agreement in place. Timing of notice may be affected by when in the day a breach is identified. Knowledge Anywhere will strive to provide notice as quickly as possible (within 24 hours) along with as much pertinent information about the nature of the breach and the known ramifications (if any) of the breach. Based upon the severity of a breach, Knowledge Anywhere will take relative actions to stop the breach and patch the flaw that allowed it as quickly as possible.**
6. What steps would Knowledge Anywhere take to mitigate any damage to the client if such a vulnerability were discovered?
   1. **Server and other applicable application-specific software is updated with the latest updates and patches on a regular basis (monthly).**
   2. **If vulnerability is discovered, the Knowledge Anywhere team will implement enhancements that would stop/mitigate any possible damage to client learning platforms and course content.  These enhancements would be deployed immediately, if needed. Otherwise enhancements are released during regular maintenance scheduled times.**
7. Are the data centers used as part of Knowledge Anywhere solutions ISO 27001 certified? If any payment card data is involved are the data centers also PCI DSS certified?
   1. **The Amazon Web Services data centers are ISO 27001 certified and PCI DSS Level 1. Knowledge Anywhere does not process or store credit card information and instead, passes information on to 3rd party payment providers for credit card processing. No user payment information (e.g., credit card numbers) are stored on Knowledge Anywhere servers.**
8. Are any third-parties or subcontractors involved in the provision of a Knowledge Anywhere solution either as hosting providers, software providers, service providers, or in any other way? If so, how does Knowledge Anywhere ensure that these third parties or subcontractors cannot negatively affect the security level of the solution?
   1. **Knowledge Anywhere contracts 3rd party resources for hosting of our production environments and IT Management of our infrastructure. Amazon Web Services provides hardware and site support. All contractors of Knowledge Anywhere are required to agree to our IT security policies and are only given access to resources as/when needed.**
9. Are Knowledge Anywhere employees aware of their obligation to maintain the confidentiality of all customer data? How is this documented? Are your business partners aware of their obligation to maintain the confidentiality of all customer data?
   1. **All Knowledge Anywhere employees are aware of their obligation to maintain confidentiality of customer data as stated in their signed Employment Agreement.  As stated previously, as a condition of employment, all Knowledge Anywhere employees are required to review and agree to (via signature) the posted IT security policies.**
   2. **Although no highly sensitive data is stored on Knowledge Anywhere systems, vendors and 3rd parties that have access to the data are** **required to sign Non-Disclosure Agreements stating they are aware of their obligations to protect the customer’s data and maintain confidentiality of any sensitive information they are exposed to.**
10. What does Knowledge Anywhere do to protect against information security breaches by highly privileged insiders, such as inappropriate access to data by a system administrator?
    1. **Server logs are routinely reviewed to identify and/or discourage security breaches.**
    2. **In the event of separation of employment and/or business arrangement with a privileged resource, measures are taken both before and after separation to prevent negative, unauthorized, and/or illegal actions against Knowledge Anywhere infrastructure, applications, or customer data.  Such measures include revocation of server credentials, domain and VPN access restriction, reclaim of company IT equipment (i.e., laptop) and office access (i.e., key), etc.**
11. Will Knowledge Anywhere allow the client or its agents to carry out information security and data protection audits of a hosted solution? Will clients also be able to carry out such audits on Knowledge Anywhere sub-contractors? For example, audits for penetration tests against your hosted solution and software, security processes as they relate to the solution, software development process, and technical and organization processes as they relate to the solution.
    1. **Scheduled audit process would be considered upon request at the expense of the client.  This must be authorized by the data owner.**
12. Will client data be protected by encryption both in transit and at rest?
    1. **All data is encrypted using TLS 1.2 in transit, by default.**
    2. **Databases are stored on encrypted volumes using AES 256bit.**
13. Is Knowledge Anywhere prepared to assist a client to produce its data as necessary for litigation (E-Discovery)?
    1. **Within the context and constraints of currently support agreements on file, Knowledge Anywhere can provide data requested in writing by authorized client representatives upon request at the expense of the client.   A copy of the discovery request and applicable data formats must be provided by the client.**
    2. **Client is responsible for engaging third party vendors to conduct data collection and preservation.**
14. How do Knowledge Anywhere system administrators enforce the principle of least privilege? Do any administrators have unrestricted access to customer data or the systems and networks used to process the data?
    1. **Knowledge Anywhere users are blocked from access to all systems which they do not need access.  Customers are only allowed access to the information and systems in the scope of their solution.  Operation Administrators that have accounts with unrestricted access are only allowed on systems where those accounts reside and those accounts are not the Operation Administrator’s primary user account.  There are no Knowledge Anywhere users that have accounts with unrestricted access to all systems.**
15. Do Knowledge Anywhere solutions comply with all applicable national and international data protection laws and regulations?
    1. **To the best of our knowledge, our solutions comply with known laws and regulations applicable to learning software solutions.**
16. Are Knowledge Anywhere employees aware of their responsibilities under applicable national and international data protection laws and regulations?
    1. **To the best of our knowledge, all employees on staff are aware of their responsibilities regarding the international data protection laws and regulations.**
17. Are Knowledge Anywhere solutions entirely hosted in the United States including hosting, storage of backups, and disaster recovery?  If not, where is it hosted?
    1. **Yes, our solutions are entirely hosted in the United States, unless otherwise specified by customer-specific requirements.**