

Town of Brookline ITD
Cloud Vendor Security Questionnaire

Updated on 09/10/2020

Network	Yes	No	Details
1. Can you provide Brookline a network diagram showing how your cloud works, the diagram need not be detailed, however it must be Brookline specific, not a generic layout.			
2. Does the application in the cloud have a dedicated IP address?			
3. Does Brookline need to add/edit any DNS records?			
4. Does Brookline need to open any ports on machines, segment any devices or create firewall rules.			
Security			
1. How do Brookline employees log into the cloud?			
2. What are your password requirements?			
3. Can you allow for only certain IP addresses in Brookline to access the administrative section of your cloud?			
4. Who owns the data in the cloud, please provide your Data Privacy Policy.			
5. Do you conduct PEN tests? How often?			
6. What type of security testing has your system network and technology gone through?			
7. Have you had a security breach? If so, please describe. Please provide your protocol in the event of a data breach.			
8. What type of SSL do you use with your product?			
9. What data is encrypted and secure in the system?			
10. What level of encryption is provided?			
11. What cloud hosting provider do you use and what are their security policies?			
12. What type of audit has your data center been through?			
13. What measures have you take to protect sensitive information?			
14. Are your Query String encrypted?			
15. What measures have your taken to prevent SQL injection or users tampering with data?			
Application and Software			
1. Is this a complete cloud solutions or are any servers involved in Brookline?			
2. SLA - What percentage of uptime do you guarantee? Please provide supporting documents not limited to the Standard Terms and Conditions document.			
3. What reporting system will you use to provide uptime reports to Brookline?			
4. What are the consequences of not meeting your uptime guarantee?			
5. Can You Demonstrate Successful Similar Deployments?			
6. Do You Have a "Try Before You Buy" Program?			
7. Do You Offer Contractual Flexibility and Price Protection?			
8. Can I configure the solution to my needs?			
9. How many web developers do you have on staff?			
10. Is your app Active Directory/LDAP Integrated and how do we sync our AD with your cloud app?			
11. In what format can data be exported from the system?			
12. What browsers and what versions are supported?			
13. What Technology or development platform are your products written in?			
14. What database backend are you using?			
15. How often is system maintenance run?			
16. Does Brookline need to install any software or browser plugins to do anything on your cloud?			
17. Does your system support multi-factor authentication?			
Disaster Recovery			
1. Describe your DR plan.			
2. Do you have an alternate data center in case your primary goes down?			

3. How and in what time frame do you make a decision to switch to your alternate data center?			
4. Have you ever had to switch to an alternate data center?			
5. Do you provide extracts of data to Brookline, can we use these to set up an alternate application should your have a prolonged outage – Host ourselves?			
6. How and when are backup performed?			
Hardware			
1. Please list any equipments, computers, card readers, printers etc.. that will touch applications in the cloud.			
E-Commerce			
1. Are you PCI complaint?			
2. Can you provide a letter of attestation?			
3. Who is the merchant?			
4. Do you provide swipe devices?			
5. Can we use any vendor to verify card information?			
6. Can we see sample reports that can be downloaded from the web?			
7. When can we schedule a meeting with you and any other vendor in the e-commerce chain for this application.			
Compliance			
1. Is your application PCI compliant? If so, Please attach supporting documents. If not, please explain.			
2. Is your application FERPA compliant? If so, Please attach supporting documents. If not, please explain.			
3. Is your product COPPA compliant? If so, Please attach supporting documents. If not, please explain.			
4. Is your product CIPA compliant? If so, please attach supporting documents. If not, please explain.			
5. Is it HIPPA complaint? If so, please attach supporting documents. If not, please explain.			
6. Please provide any other compliance information and supporting documents.			
Privacy			
1. What privacy regulations must be addressed for the use cases supported?			
2. What privacy controls or frameworks are employed?			
3. What notices are given and when are they given in the process of collecting information?			
4. Are there specific notices related to personal information?			
5. Are there specific notices related to an individual's privacy or data rights or actions?			
6. Are there specific policies in the case of children?			
7. Are there policies for other special conditions, such as automated processing, health information or other special data categories?			
8. Is the process opt in or opt out?			
9. Does any tracking take place before notice is given or consent obtained?			
10. Is a privacy point of contact provided?			
11. How is the privacy policy reviewed and maintained?			
12. Are privacy controls included in any internal or third party audits?			
13. Are privacy controls included in logging?			