IRVING
Independent School District

Irving ISD Cyber-Security Assessment Questionnaire

Organization:

Physical Data Centers

Does your company protect its data center against physical intrusion? What security measures are in place to limit and manage access to your company's data center?	
Does your company protect its data center against power outages?	

Network

Does your solution require the use of two-factor authentication for the administrative control of servers, routers, switches and firewalls? ***Please explain functionality.***	
Does your solution support IPsec or Secure Sockets Layer with Extended Validation certificates and two factor authentication for connecting to the service? ***Please explain functionality.***	
Does your solution provide redundancy and load balancing for firewalls, intrusion prevention, and other critical security elements? ***Please explain functionality.***	

Does your company perform (or have an experienced third-party consultancy perform) external penetration tests at least quarterly and internal network security audits at least annually? *Please include how often test is conducted.* *The audits should be against International Organization for Standardization (ISO) 27001/2 and in compliance with Statement on Auditing Standards No. 70, Service Organizations (SAS 70 Type II).* *SAS 70 Type II audits are expensive, and are not necessarily more insightful than other audits, but all major auditing firms accept the SAS 70 Type II format and structure.* *Please elaborate on testing strategy.*	
Can your solution show documented requirements (and audit procedures) for network security to ensure that other customers will not compromise its shared-service infrastructure? *Please provide documentation or summary of procedures.*	
Does your company contract for, or provide protection against, denial-of-service attacks against its Internet presence? *Please describe protection solution.*	

Platform

Can your company present a documented policy for "hardening" the underlying virtualized infrastructure that its services run on? *Please provide policy documentation.*	
Can your company provide validated procedures for configuration management, patch installation, and malware prevention for all servers and PCs involved in cloud service delivery? *Please provide documentation or summary of procedures.*	
Does your company have a documented set of controls that it uses to ensure the separation of data and security information among customer applications? *Please provide control information.*	

Applications and Data

How does your company review the security of applications and any supporting code, such as Ajax, ActiveX controls and Java applets that it develops and uses?	
Does your solution provide audit trails that can be reviewed to determine historical changes?	
Can your company provide documented procedures for configuration management, including the installation of security patches, for all applications? ***Please provide documentation or summary of procedures.***	
How are enhancements and new features implemented? ***What type of notification is provided to the user?***	
For companies providing regulatory or other compliance requirements, does your company meet the applicable requirements for data protection? ***For example, requirements of the U.S. Sarbanes-Oxley Act, the U.S. Health Insurance Portability and Accountability Act, and the Payment Card Industry Data Security Standard.*** ***Please describe in detail.***	

Operations

Does your company perform background checks on personnel with administrative or other privileged access to servers, applications or customer data? ***When are background checks performed and how often?***	
Does your company have super user privilege management and database activity monitoring controls (or the equivalent) to detect inappropriate behavior by provider employees with administrative access? ***How is this monitored?***	
Can your company provide a documented process for evaluating security alerts from OS and application vendors, shielding systems from attack until patched, and installing security patches and service packs? ***Please provide documentation or summary of process.***	
Does your company employ security monitoring and log management functions, and use write-once technology or other secure approaches for storing audit trails and security logs? ***Please provide documentation or summary of functionality.***	
Can your company demonstrate established procedures for vulnerability management, intrusion prevention, incident response, and incident escalation and investigation? ***Please provide documentation or summary of procedures.***	
Can your company provide procedures for business continuity management and disaster recovery management that include the individual client's enterprise-specific applications and data, as well as evidence that it has tested those procedures during the past 12 months? ***Please provide documentation or summary of procedures.*** ***Please provide date of last test.***	

End Services

Does your company's security staff average more than four years experience in information and network security?	
Does more than 75% of your security staff have security industry certification, such as Certified Information Systems Security Professional (CISSP), Global Information Assurance Certification (GIAC), or equivalent?	
Please provide the vendor certification for the specific firewall equipment your company will manage.	
Can your company show documented identity management and help desk procedures for authenticating callers and resetting access controls? *If establishing and deleting accounts is part of the cloud service offering, then can your company show those procedures as well?* *If yes, then please provide documentation or summary of procedures.*	

Data Retention / Exportation After Service Termination

After termination of services, what does your company do with customer data?	
Can Irving ISD request a purge of all or our data? ***Can your company provide proof of the data purge?***	
Can Irving ISD request an export of our data from the vendor system? ***If yes, are there additional costs?***	

Signature

Name:	
Title:	
Date completed:	