QUBE PENTACLE

INFORMATION RISK MANAGEMENT INFORMATION

Frequently asked by clients on security

Organisation:	Pentacle The Virtual Business School	
Collaborative Learning Social Media Platform:	http://QUBE.cc	http://QUBE.cc/security-it-support/
Technical Lead:	David Lomas	
Address:	20 London End, Beaconsfield, HP9 2JH	
General Queries:	QUBE@PentacleTheVBS.com	
Phone Number:	+44 1494 678 555	
Software Type	Collaborative Learning Social Media Platform	

Topic	Response	Comment
Project Engagement		
1. Has Pentacle agreed to non-disclosure with the client?	yes	
2. Will any services provided to the client be sub-contracted to an additional vendor?	yes	Encrypted data hosting services
Information Security Policies		
1. Are information security policies, standards and procedures documented?	yes	
2. Are information security policies, standards and procedures periodically reviewed and updated as needed?	yes	
3. Is compliance with information security policies monitored and measured?	yes	
Compliance		
1. Is your organization under obligation to uphold security controls in support of data protection laws, such as US HIPAA, EU Data Protection Directive, US Safe Harbor, etc.?	yes	
2. Is the company's data protection program aligned with a recognized framework, such as ISO 27001, COBIT, ITIL, NIST, etc.?	no	
3. Has a third party or internal audit performed an information security assessment or audit in the last 12 months on the data protection program? (If so, please attach copies.)	no	
Human Resources Security		
1. Are background checks (including employment and criminal history) performed for new employees and contractors?	no	sensitive information access held by key personell
2. Are all employees and contractors required to sign a non-disclosure agreement?	yes	
3. Is the non-disclosure agreement available to the client upon request?	yes	
4. Is there an information security awareness and training program in place?	no	
5. Are employees and contractors required to be aware of and follow all information security policies, standards and procedures?	yes	
Data Protection Practices		
1. Is data classification addressed in data handling procedures (e.g. confidential or private data)?	yes	
2. Is client data securely separated from other clients' data?	yes	
3. Is the data processing equipment used to provide customer services securely separated from the equipment used for the vendor's own data processing?	yes	
4. When the business relationship is terminated, can all of the client's data be immediately returned and/or destroyed at the client's request?	yes	
5. Is client data encrypted when stored on PCs, databases, fixed media or portable media?	n/a	Recommend clients locally encrypt if required
6. Is client data encrypted during transmission within the vendor's internal network?	yes	
7. Is client data encrypted during transmission within the vendor's dedicated customer network?	yes	
8. Is client data encrypted during transmission from the vendor to destinations outside the vendor's network(s)?	yes	
9. If data-level encryption is used, is AES (Advanced Encryption Standard) the minimum technique used?	yes	
10. If transport-level encryption is used, is 128-bit SSL (Secure Sockets Layer) the minimum technique used?	yes	
11. Are the encryption keys centrally managed and controlled?	yes	
12. If encrypted, does the vendor have the ability to un-encrypt client data without the client's involvement?	yes	

Physical and Environmental Security		
1. Where is the data center located? (Use Comment Field)	N/A	Amazon AWS Ireland
2. Does the company manage the security of the facility?	no	
3. If Yes, do you have a SAS70 or equivalent certification?	n/a	
4. If No, does the third-party owner have a SAS70 or equivalent certification? (N/A if #2 is "Yes")	yes	
5. Are physical assets tracked throughout their lifecycle?	yes	
6. Are physical assets (e.g. harddrives, USB drives, Tapes, printer harddrives) destroyed when no longer in use (due to failure and/or retirement)? If Yes, please describe How under "Comments".	yes	physical destruction
Information Systems Development Lifecycle		
1. Are there data integrity checks for both input and output built into the software?	yes	
2. Is it possible to federate identities with the client?	no	
3. How is are the credentials protected within the application? (e.g. Salted Hash, MD5 hash, other) (Use Comment Field)	N/A	md5 hash
4. Is the application penetration tested by a 3rd party?	no	
5. Are all of the OWASP Top Ten vulnerabilities tested for? (Cross site scripting, SQL injection and others.)	n/a	Not a web application
6. Can the client get a copy of the test results or prior to new releases?	n/a	
7. Can the client test against their own instance in a staging area?	yes	
Access Control to Systems Hosting Client Information for System Admins (not end users)		
1. Is there a process to grant access rights to client information?	yes	
2. Is there a process to ensure access rights granting and removing is performed with management approval?	yes	
3. Is there a process to audit access rights?	yes	
4. Are passwords required to be at least 7 characters in length with strong password characteristics? (e.g., enforcing mixed case, numeric, and/or special characters, words not found in a dictionary, etc.)	yes	
5. Are accounts automatically locked-out after 5, (or less), consecutive failed login attempts?	no	
6. Is a locked-out account unusable for at least 30 minutes?	n/a	
7. Is there a secure process to communicate passwords to users?	yes	
8. Are accounts prevented from reusing at least the previous 10 passwords?	no	
9. Are all accounts automatically disabled after 90 consecutive days of inactivity?	no	
10. Is there a forced password change after the initial login?	no	
11. Are all passwords required to change at least every 90 days?	no	
12. Are privileges granted and revoked based on the principle of least privilege needed?	yes	
13. Is there a process to ensure granted access rights adjust to role changes and/or role terminations?	yes	
14. Is there a process to authenticate a user's identity for password and/or other account administration?	yes	
15. Are users automatically logged off after 30 minutes or less of inactivity?	no	
16. Is there a process for allowing personnel to access workstations and/or servers that have client data when such access is required? (e.g., visitor sign-in, visitor escort, identity authentication and verification protocols, etc.)	yes	
17. Is remote access to systems hosting client information permitted?	yes	
18. Does remote access use IPSec or 128-bit SSL encryption?	no	ssh with rsa keys
19. Does remote access require two-factor authentication, such as RSASecurID® tokens?	yes	
Communications and Operations		
1. Is the internet connection business-class and fault-tolerant?	yes	
2. Is access controlled between the internal network and the Internet by ICSA-certified, single-purposed firewalls?	yes	SonicWALL TZ100
3. Are all wireless LAN segments secured to allow only controlled authenticated and authorized access?	yes	
4. Is the internal network segmented, or otherwise controlled, to prevent unauthorized access and to ensure data integrity?	n/a	
5. Is there a process to automatically detect and respond to suspicious activity on the networks?	yes	
6. Is there a management process in place to identify, assess, test, and deploy appropriate security patches for network and security infrastructure?	n/a	
7. Are network and infrastructure security patches assessed as "critical" deployed in less than 5 days?	yes	
8. Is Intrusion Prevention (IPS) installed and executing effectively?		
9. Are there logical and physical controls in the network infrastructure to isolate or otherwise restrict access to sensitive network segments or applications (e.g., dedicated e-commerce infrastructure)?	yes	
10. Are there network-based intrusion detection and/or prevention devices deployed to protect sensitive network segments or applications?	yes	

11. Is there logging of the:	N/A	<Leave Blank>
a. System	yes	
b. File/Folder level access	no	
c. Application	yes	
d. Administrative Privileged Use	yes	
12. Are security-related logs from key network and security infrastructure devices aggregated?	no	
13. Can security-related logs be made available to the client if requested? If Yes, how long is the log-retention period?	yes	6 months
14. Is anti-virus software installed and executing on all workstations and servers connected to the network?	yes	
15. Are workstation and server virus anti-virus software signatures updated automatically?	yes	
16. Are there tools deployed within the network infrastructure to detect, prevent or otherwise hinder malicious code outbreaks?	yes	
Incident Response and Notification to the Client		
1. Is there a computer security incident response process in place to define roles and responsibilities to minimize an incident's impact?	yes	
2. Are there procedures for employees to report and respond to (suspected) information security policy violations?	yes	
3. Will the client be notified immediately if an incident occurs that may affect its data or services?	yes	
Backup, Disaster Recovery, and Contingency Planning		
1. Is client data backed up to tape and stored off-site at a secure facility (i.e., fire detection and suppression, climate control, secured access, UPS, etc.) at least twenty miles away from the primary data processing location?	no	not backed up to tape, but to disk
2. Is there a comprehensive, documented and secure process to handle all media on-site, off-site and during	n/a	
3. Are backups tested periodically to ensure data can be recovered?	yes	
4. Are backup tapes encrypted?	n/a	no tapes
5. Are client monthly backup tapes available to be restored for at least seven years?	n/a	
6. Is there a secure secondary recovery site for recovery and continuity?	yes	
7. Are the primary and secondary site located in secure, business-grade facilities?	yes	
8. Is the Disaster Recovery plan tested successfully with the results documented at least once per year?	yes	
9. Are all of the employees aware of the Disaster Recovery plan and prepared to execute it successfully?	yes	
10. Will client representative(s) be notified of a disaster declaration immediately?	yes	Please provide contact details
eDiscovery - Access to Data		
1. Do you have a defined process for processing eDiscovery requests on behalf of your customers? If yes, please describe your process in "Comments"	n/a	