

INFORMATION RISK MANAGEMENT INFORMATION

| Frequently asked by clients on secur | ity | | |
|---|----------------|--|--|
| Organisation: | | e The Virtual Business School | |
| Collaborative Learning Social Media Platforn | http://QUBE.cc | http://QUBE.cc/security-it-support/ | |
| Technical Lead | : | David Lomas | |
| Address | : 20 Londo | 20 London End, Beaconsfield, HP9 2JH | |
| General Queries | QUI | BE@PentacleTheVBS.com | |
| Phone Number | : | +44 1494 678 555 | |
| Software Two | Callabarati | u Leonice Cesiel Medie Distance | |
| Software Type | | ve Learning Social Media Platform | |
| Topic Project Engagement | Response | Comment | |
| 1. Has Pentacle agreed to non-disclosure with the client? | Yes | | |
| 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 | | |
| Are information security policies, standards and procedures periodically reviewed and updated as needed? | Yes | | |
| Is compliance with information security policies monitored and measured? | Yes | | |
| Compliance | <u>.</u> | | |
| 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.? | Yes | | |
| 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? | Yes | | |
| 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 personnel | |
| | Yes | | |
| Are all employees and contractors required to sign a non-disclosure agreement? Is the non-disclosure agreement available to the client upon request? | Yes | | |
| Is the non-disclosure agreement available to the client upon request? 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 | Vac | | |
| 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 | |
| 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 | 2. If encrypted, does the vendor have the ability to un-encrypt client data without the client's involvement? | Yes | |
| Phy | sica | al and Environmental Security | | |
| | 1. | Where is the data center located? (Use Comment Field) | N/A | UK (iomart) |
| | 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 | | Physical destruction |
| | | rement)? If Yes, please describe How under "Comments". | Yes | |
| | | ation Systems Development Lifecycle | | |
| | | Are there data integrity checks for both input and output built into the software? | Yes | |
| 2. I | ls 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 3 rd party? | Yes | |
| | 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 | |
| | <i>'</i> · · | | | |
| | | Control to Systems Hosting Client Information for System Admins (not end users) | | |
| Acc | ess | Control to Systems Hosting Client Information for System Admins (not end users) | Yes | |
| Acc | ess | Control to Systems Hosting Client Information for System Admins (not end users) Is there a process to grant access rights to client information? | | |
| Acc | ess 1. | Control to Systems Hosting Client Information for System Admins (not end users) Is there a process to grant access rights to client information? | Yes | |
| Acc | ess 1. 2. 3. 4. | Control to Systems Hosting Client Information for System Admins (not end users) Is there a process to grant access rights to client information? Is there a process to ensure access rights granting and removing is performed with management approval? Is there a process to audit access rights? Are passwords required to be at least 7 characters in length with strong password characteristics? (e.g., enforcing mixed case, numeric, | Yes Yes Yes | |
| Acc | ess 1. 2. 3. 4. | E Control to Systems Hosting Client Information for System Admins (not end users) Is there a process to grant access rights to client information? Is there a process to ensure access rights granting and removing is performed with management approval? Is there a process to audit access rights? Are passwords required to be at least 7 characters in length with strong password characteristics? (e.g., enforcing mixed case, numeric, d/or special characters, words not found in a dictionary, etc.) | Yes Yes Yes | |
| Acc | ess 1. 2. 3. 4. | E Control to Systems Hosting Client Information for System Admins (not end users) Is there a process to grant access rights to client information? Is there a process to ensure access rights granting and removing is performed with management approval? Is there a process to audit access rights? Are passwords required to be at least 7 characters in length with strong password characteristics? (e.g., enforcing mixed case, numeric, d/or special characters, words not found in a dictionary, etc.) Are accounts automatically locked-out after 5 (or less) consecutive failed login attempts? | Yes Yes Yes Yes No | |
| Acc | ess 1. 2. 3. 4. and 5. 6. | Control to Systems Hosting Client Information for System Admins (not end users) Is there a process to grant access rights to client information? Is there a process to ensure access rights granting and removing is performed with management approval? Is there a process to audit access rights? Are passwords required to be at least 7 characters in length with strong password characteristics? (e.g., enforcing mixed case, numeric, d/or special characters, words not found in a dictionary, etc.) Are accounts automatically locked-out after 5 (or less) consecutive failed login attempts? Is a locked-out account unusable for at least 30 minutes? | Yes Yes Yes No Yes | |
| Acc | ess 1. 2. 3. 4. and 5. 6. 7. | Control to Systems Hosting Client Information for System Admins (not end users) Is there a process to grant access rights to client information? Is there a process to ensure access rights granting and removing is performed with management approval? Is there a process to audit access rights? Are passwords required to be at least 7 characters in length with strong password characteristics? (e.g., enforcing mixed case, numeric, d/or special characters, words not found in a dictionary, etc.) Are accounts automatically locked-out after 5 (or less) consecutive failed login attempts? Is a locked-out account unusable for at least 30 minutes? Is there a secure process to communicate passwords to users? | Yes Yes Yes No Yes Yes | |
| Acc | ess 1. 2. 3. 4. and 5. 6. | Control to Systems Hosting Client Information for System Admins (not end users) Is there a process to grant access rights to client information? Is there a process to ensure access rights granting and removing is performed with management approval? Is there a process to audit access rights? Are passwords required to be at least 7 characters in length with strong password characteristics? (e.g., enforcing mixed case, numeric, d/or special characters, words not found in a dictionary, etc.) Are accounts automatically locked-out after 5 (or less) consecutive failed login attempts? Is a locked-out account unusable for at least 30 minutes? Is there a secure process to communicate passwords to users? Are accounts prevented from reusing at least the previous 10 passwords? | Yes Yes Yes No Yes Yes No | |
| Acc | ess 1. 2. 3. 4. and 5. 6. 7. 8. 9. | Control to Systems Hosting Client Information for System Admins (not end users) Is there a process to grant access rights to client information? Is there a process to ensure access rights granting and removing is performed with management approval? Is there a process to audit access rights? Are passwords required to be at least 7 characters in length with strong password characteristics? (e.g., enforcing mixed case, numeric, d/or special characters, words not found in a dictionary, etc.) Are accounts automatically locked-out after 5 (or less) consecutive failed login attempts? Is there a secure process to communicate passwords to users? Are accounts prevented from reusing at least the previous 10 passwords? Are all accounts automatically disabled after 90 consecutive days of inactivity? | Yes Yes Yes No Yes Yes No No | |
| Acc | ess 1. 2. 3. 4. and 5. 6. 7. 8. 9. 10. | Control to Systems Hosting Client Information for System Admins (not end users) Is there a process to grant access rights to client information? Is there a process to ensure access rights granting and removing is performed with management approval? Is there a process to audit access rights? Are passwords required to be at least 7 characters in length with strong password characteristics? (e.g., enforcing mixed case, numeric, d/or special characters, words not found in a dictionary, etc.) Are accounts automatically locked-out after 5 (or less) consecutive failed login attempts? Is there a secure process to communicate passwords to users? Are accounts prevented from reusing at least the previous 10 passwords? Are all accounts automatically disabled after 90 consecutive days of inactivity? Is there a forced password change after the initial login? | Yes Yes Yes No Yes No No No No | |
| Acc | ess 1. 2. 3. 4. and 5. 6. 7. 8. 9. 10. 11. | Control to Systems Hosting Client Information for System Admins (not end users) Is there a process to grant access rights to client information? Is there a process to ensure access rights granting and removing is performed with management approval? Is there a process to audit access rights? Are passwords required to be at least 7 characters in length with strong password characteristics? (e.g., enforcing mixed case, numeric, d/or special characters, words not found in a dictionary, etc.) Are accounts automatically locked-out after 5 (or less) consecutive failed login attempts? Is there a secure process to communicate passwords to users? Are accounts prevented from reusing at least the previous 10 passwords? Are all accounts automatically disabled after 90 consecutive days of inactivity? Is there a forced password change after the initial login? Are all passwords required to change at least every 90 days? | Yes Yes Yes No Yes Yes No No No No No | |
| Acc | ess 1. 2. 3. 4. and 5. 6. 7. 8. 9. 10. 11. 12. | Control to Systems Hosting Client Information for System Admins (not end users) Is there a process to grant access rights to client information? Is there a process to ensure access rights granting and removing is performed with management approval? Is there a process to audit access rights? Are passwords required to be at least 7 characters in length with strong password characteristics? (e.g., enforcing mixed case, numeric, d/or special characters, words not found in a dictionary, etc.) Are accounts automatically locked-out after 5 (or less) consecutive failed login attempts? Is there a secure process to communicate passwords to users? Are accounts prevented from reusing at least the previous 10 passwords? Are all accounts automatically disabled after 90 consecutive days of inactivity? Is there a forced password change after the initial login? Are all passwords required to change at least every 90 days? Are privileges granted and revoked based on the principle of least privilege needed? | Yes Yes Yes No Yes Yes No No No No Yes | |
| Acc | ess 1. 2. 3. 4. and 5. 6. 7. 8. 9. 10. 11. 12. 13. | Control to Systems Hosting Client Information for System Admins (not end users) Is there a process to grant access rights to client information? Is there a process to ensure access rights granting and removing is performed with management approval? Is there a process to audit access rights? Are passwords required to be at least 7 characters in length with strong password characteristics? (e.g., enforcing mixed case, numeric, d/or special characters, words not found in a dictionary, etc.) Are accounts automatically locked-out after 5 (or less) consecutive failed login attempts? Is there a secure process to communicate passwords to users? Are accounts prevented from reusing at least the previous 10 passwords? Are all accounts automatically disabled after 90 consecutive days of inactivity? Is there a forced password change after the initial login? Are all passwords required to change at least every 90 days? Are privileges granted and revoked based on the principle of least privilege needed? Is there a process to ensure granted access rights adjust to role changes and/or role terminations? | Yes Yes Yes No Yes Yes No No No No Yes Yes Yes | |
| Acc | ess 1. 2. 3. 4. 6. 7. 8. 9. 10. 11. 12. 13. 14. | Control to Systems Hosting Client Information for System Admins (not end users) Is there a process to grant access rights to client information? Is there a process to ensure access rights granting and removing is performed with management approval? Is there a process to audit access rights? Are passwords required to be at least 7 characters in length with strong password characteristics? (e.g., enforcing mixed case, numeric, d/or special characters, words not found in a dictionary, etc.) Are accounts automatically locked-out after 5 (or less) consecutive failed login attempts? Is a locked-out account unusable for at least 30 minutes? Is there a secure process to communicate passwords to users? Are accounts prevented from reusing at least the previous 10 passwords? Are all accounts automatically disabled after 90 consecutive days of inactivity? Is there a forced password change after the initial login? Are all passwords required to change at least every 90 days? Are privileges granted and revoked based on the principle of least privilege needed? Is there a process to ensure granted access rights adjust to role changes and/or role terminations? Is there a process to authenticate a user's identity for password and/or other account administration? | Yes Yes Yes No Yes Yes No No No No Yes Yes Yes Yes | |
| Acc | ess 1. 2. 3. 4. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. | Control to Systems Hosting Client Information for System Admins (not end users) Is there a process to grant access rights to client information? Is there a process to ensure access rights granting and removing is performed with management approval? Is there a process to audit access rights? Are passwords required to be at least 7 characters in length with strong password characteristics? (e.g., enforcing mixed case, numeric, //or special characters, words not found in a dictionary, etc.) Are accounts automatically locked-out after 5 (or less) consecutive failed login attempts? Is a locked-out account unusable for at least 30 minutes? Is there a secure process to communicate passwords to users? Are accounts prevented from reusing at least the previous 10 passwords? Are all accounts automatically disabled after 90 consecutive days of inactivity? Is there a forced password change after the initial login? Are all passwords required to change at least every 90 days? Are privileges granted and revoked based on the principle of least privilege needed? Is there a process to ensure granted access rights adjust to role changes and/or role terminations? Is there a process to authenticate a user's identity for password and/or other account administration? Are users automatically logged off after 30 minutes or less of inactivity? | Yes Yes Yes No Yes Yes No No No No Yes Yes Yes | |
| Acc | ess 1. 2. 3. 4. and 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 14. 15. 16. 10. 11. 12. 10. 10. 10. 10. 10. 10. 10. 10 | Control to Systems Hosting Client Information for System Admins (not end users) Is there a process to grant access rights to client information? Is there a process to ensure access rights granting and removing is performed with management approval? Is there a process to audit access rights? Are passwords required to be at least 7 characters in length with strong password characteristics? (e.g., enforcing mixed case, numeric, J/or special characters, words not found in a dictionary, etc.) Are accounts automatically locked-out after 5 (or less) consecutive failed login attempts? Is a locked-out account unusable for at least 30 minutes? Is there a secure process to communicate passwords to users? Are accounts prevented from reusing at least the previous 10 passwords? Are all accounts automatically disabled after 90 consecutive days of inactivity? Is there a forced password change after the initial login? Are all passwords required to change at least every 90 days? Are all passwords required to change at least every 90 days? Is there a process to ensure granted access rights adjust to role changes and/or role terminations? Is there a process to authenticate a user's identity for password and/or other account administration? Are users automatically logged off after 30 minutes or less of inactivity? Is there a process to allowing personnel to access workstations and/or servers that have client data when such access is required? (e.g., | Yes Yes Yes No Yes Yes No No No Yes Yes Yes Yes Yes No | |
| Acc | ess 1. 2. 3. 4. and 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 14. 15. 14. 15. 14. 15. 15. 10. 10. 10. 10. 10. 10. 10. 10 | Control to Systems Hosting Client Information for System Admins (not end users) Is there a process to grant access rights to client information? Is there a process to ensure access rights granting and removing is performed with management approval? Is there a process to audit access rights? Are passwords required to be at least 7 characters in length with strong password characteristics? (e.g., enforcing mixed case, numeric, d/or special characters, words not found in a dictionary, etc.) Are accounts automatically locked-out after 5 (or less) consecutive failed login attempts? Is a locked-out account unusable for at least 30 minutes? Is there a secure process to communicate passwords to users? Are accounts prevented from reusing at least the previous 10 passwords? Are all accounts automatically disabled after 90 consecutive days of inactivity? Is there a forced password change after the initial login? Are all passwords required to change at least every 90 days? Are privileges granted and revoked based on the principle of least privilege needed? Is there a process to ensure granted access rights adjust to role changes and/or role terminations? Is there a process to authenticate a user's identity for password and/or other account administration? Are users automatically logged off after 30 minutes or less of inactivity? Is there a process for allowing personnel to access workstations and/or servers that have client data when such access is required? (e.g., tor sign-in, visitor escort, identity authentication and verification protocols, etc.) | Yes Yes Yes No Yes Yes No No No Yes Yes Yes Yes No Yes | |
| Acc | ess 1. 2. 3. 4. and 5. 6. 7. 8. 9. 10. 12. 13. 14. 15. 14. 15. 14. 15. 14. 15. 17. 14. 15. 10. 17. 10. 10. 10. 10. 10. 10. 10. 10 | Control to Systems Hosting Client Information for System Admins (not end users) Is there a process to grant access rights to client information? Is there a process to ensure access rights granting and removing is performed with management approval? Is there a process to audit access rights? Are passwords required to be at least 7 characters in length with strong password characteristics? (e.g., enforcing mixed case, numeric, d/or special characters, words not found in a dictionary, etc.) Are accounts automatically locked-out after 5 (or less) consecutive failed login attempts? Is a locked-out account unusable for at least 30 minutes? Is there a secure process to communicate passwords to users? Are accounts prevented from reusing at least the previous 10 passwords? Are all accounts automatically disabled after 90 consecutive days of inactivity? Is there a forced password change after the initial login? Are all passwords required to change at least every 90 days? Are privileges granted and revoked based on the principle of least privilege needed? Is there a process to ensure granted access rights adjust to role changes and/or role terminations? Is there a process to authenticate a user's identity for password and/or roler account administration? Are users automatically logged off after 30 minutes or less of inactivity? Is there a process to authenticate a user's identity for password and/or servers that have client data when such access is required? (e.g., itor sign-in, visitor escort, identity authentication and verification protocols, etc.) Is remote access to systems hosting client information permitted? | Yes Yes Yes No Yes Yes No No No No Yes Yes Yes No Yes Yes Yes | |
| Acc | ess 1. 2. 3. 4. and 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 14. 15. 14. 15. 14. 13. 14. 13. 14. 13. 14. 13. 14. 15. 10. 13. 14. 15. 15. 10. 11. 12. 13. 14. 15. 15. 15. 16. 17. 16. 17. 17. 18. 19. 10. 11. 12. 13. 14. 15. 16. 17. 16. 17. 17. 18. 19. 11. 15. 16. 17. 18. 19. 11. 15. 16. 17. 17. 18. 19. 11. 15. 16. 17. 17. 17. 17. 17. 17. 17. 17 | Control to Systems Hosting Client Information for System Admins (not end users) Is there a process to grant access rights to client information? Is there a process to ensure access rights granting and removing is performed with management approval? Is there a process to audit access rights granting and removing is performed with management approval? Is there a process to audit access rights granting and removing is performed with management approval? Is there a process to ensure access rights and removing is performed with management approval? Is there a process to ensure access rights and removing is performed with management approval? Is there a process to ensure access rights of the at least 7 characters in length with strong password characteristics? (e.g., enforcing mixed case, numeric, J/or special characters, words not found in a dictionary, etc.) Are accounts automatically locked-out after 5 (or less) consecutive failed login attempts? Is a locked-out account unusable for at least 30 minutes? Is there a secure process to communicate passwords to users? Are accounts prevented from reusing at least the previous 10 passwords? Are all accounts automatically disabled after 90 consecutive days of inactivity? Is there a forced password change after the initial login? Are all passwords required to change at least every 90 days? Are privileges granted and revoked based on the principle of least privilege needed? Is there a process to ensure granted access rights adjust to role changes and/or role termination? Are users automatically logged off after 30 minutes or less of inactivity? Is there a process to authenticate a user's identity for password and/or other account administration? Are users automatically logged off after 30 minutes or less of inactivity? Is there a process for allowing personnel to access workstations and/or servers that have client data when such access is required? (e.g., tor sign-in, visitor escort, identity authentication and verification protocols, etc.) Is remote access use IPSec or 128 | Yes Yes Yes No Yes Yes No No No Yes Yes Yes Yes No Yes | SSH with RSA keys |

| 1. Is the internet connection business-dase and built-plann? Yes = 2. Is access controlled bubbents accurate to allow only controlled authented and authorized access and o ensure data integrity? Yes = 3. Are all wieless LAN segments, or tabrevis controlled, a planet table access and o ensure data integrity? NA = 5. Is their a process to automatically detect and respond to suspicious activity on the network? Yes = 6. Is their a management process in place to identify, assess, test, and deploy appropriate security patches for network and security infrastructure oscillation of the prove infrastructure isolate or otherwise restrict access to sensitive network segments or applications (u.g., didatabet controls in the network infrastructure to isolate or otherwise restrict access to sensitive network segments or applications (u.g., didatabet controls in the infrastructure isolate or otherwise restrict access to sensitive network segments or applications (u.g., didatabet controls in the infrastructure isolate or otherwise restrict access to sensitive network segments or applications (u.g., didatabet controls in divises deployed to protect sensitive network segments or applications? NA NA 11. Is there bagging of the: a. System NA NA NA a. Application Are there bagging of the: NA NA NA a. Application A. Administrature devices agregated? NB NA NA A. Administrative response not sense to device device, prevent on otherwise network? Yes NA A. Administrat | Communications and Operations | | | | | | | | |
|---|---|-----|------------------------------------|--|--|--|--|--|--|
| 1 Process LAN segments secured to allow only controlled authenticated access on to ensure data integrity? Ves 4 Is the interral network segments accurde to allow only controlled, to prevent unauthorized access on to ensure data integrity? ViA 4 Is the interral network segments accurde to allow only controlled, to prevent unauthorized access and to ensure data integrity? ViA 5 The additional control of the respond to support of the network of a security patches for network and security? ViA 6 The interral network segments access to allow only controlled authentity access and to ensure data integrity? ViA 7 Are network and infrastruture security patches assessed as "ritical" deployed in less than 5 day? ViA 8 Is there loggin of the: Ves 9 Are there network-based intrusion detection and/or prevention devices deployed to protect sensitive network segments or applications (e.g., dedicated ecommerce infrastructure)? Ves 1 Is there loggin of the: Ves Ves 1 System Ves Ves 1 System Ves Ves 2 Are terre intrustry of the device deployed of the network? Ves 3 System Ves Ves 1 Is the network infrastructur | 1. Is the internet connection business-class and fault-tolerant? | Yes | | | | | | | |
| 4. Is the internal network segmented, or otherwise controlled, to prevent unauthorized access and to ensure data integrity? NA 6. Is there a monagement process in place to identify, assess, test, and deploy appropriate security patches for network and security infrastructure security patches assessed as "critical" deployed in less than 5 days? NA 7. Are network and infrastructure security patches assessed as "critical" deployed in less than 5 days? Na 8. Is hursian deployed in the network infrastructure to isolate or otherwise restrict access to sensitive network segments or applications (e.g., desicated e-commerce infrastructure)? Yes 10. Are there logical qortic: Yes a. System NA b. FliefFolder level access NA c. Applications G., desicated e-commerce infrastructure devices aggregated? 11. Is there logical qortic: NA a. System Na b. FliefFolder level access Na c. Application G. application d. Arminicative on keyn retwork and security infrastructure devices aggregated? No 13. Can security-related logs the mate available to the client if requested? If Yes, how leng is the log-relevation period? Yes 14. Is anti-virus aortivarie instancture to deted, prevent or otherwise hinder malicius code outhreaks? Yes 15. Are worelotate accomprovent security indicent responc | 2. Is access controlled between the internal network and the Internet by ICSA-certified, single-purposed firewalls? | Yes | SonicWALL TZ100 | | | | | | |
| Set store a process to automatically detect and respond to suspicous activity on the networks? Set store a management process in place to identify, assess, test, and deploy appropriate security patches for network and security Indirective security patches assessed as childral deployed in less than 5 days? Set networks and infratructure security patches assessed as childral deployed in less than 5 days? Set networks and infratructure security patches assessed as childral deployed in less than 5 days? Set networks and infratructure security patches assessed as childral deployed in less than 5 days? Set the network and infratructure security patches assessed as childral deployed to protect sensitive network segments or applications? Set the network-based intrusion detection and/or prevention devices deployed to protect sensitive network segments or applications? Set the network-based intrusion detection and/or prevention devices deployed to protect sensitive network segments or applications? Set the network-based intrusion detection and/or prevention devices aggregated? Set the network-based intrusion devices aggregated? Set the network-based intrusion devices aggregated? Set the network-index days available to the client if requested? No Set the network-index days available to the client if requested? No Set the network infrastructure to devices aggregated? No No Set the network infrastructure to devices aggregated? No No Set the network infrastructure to devices aggregated? No No Set the network infrastructure of the network? Yes No No Set the network infrastructure to devices and responsibilities to minimize an incident? Yes No No Set the network infrastructure to define roles and responsibilities to minimize an incident? Yes No No | 3. Are all wireless LAN segments secured to allow only controlled authenticated and authorized access? | Yes | | | | | | | |
| S. Is there a management process in place to identify, assess, test, and deploy appropriate security patches for network and security infrastructure? Are network and infrastructure security patches assessed as "oritical" deployed in less than 5 days? S. Is there logical and physical controls in the network instantucture to isolate or otherwise restrict access to sensitive network segments or applications (e.g., dedicated e-commerce infrastructure)? Are there network-based intrusion detection and/or prevention devices deployed to protect sensitive network segments or applications? As place network-based intrusion detection and/or prevention devices deployed to protect sensitive network segments or applications? As place to entwork-based intrusion detection and/or prevention devices deployed to protect sensitive network segments or applications? Application Sign System Sign Sign Sign Application Applic | 4. Is the internal network segmented, or otherwise controlled, to prevent unauthorized access and to ensure data integrity? | N/A | | | | | | | |
| infrastructure? NA 7. Are network and infrastructure security patches assessed as "critical" deployed in less than 5 days? NA 8. Is Intrusion Prevention (IPS) installed and executing effectively? No 9. Are there network-based intrusion detection and/or prevention devices deployed to protect sensitive network segments or applications? Yes 10. Are there network-based intrusion detection and/or prevention devices deployed to protect sensitive network segments or applications? Yes 11. Is there network-based intrusion detection and/or prevention devices deployed to protect sensitive network segments or applications? No 2. Are there network-based intrusion detection and/or prevention devices deployed to protect sensitive network segments or applications? No 3. System No Ves 4. Administrative Privileged Usa Yes No 2. Are security-related logs to network and security infrastructure devices aggregated? No No 3. Can security-related logs to mean device infrastructure devices aggregated? No No 4. Is anti-vitus software signatures updated automatically? Yes No 5. Are workstain and security infrastructure to detect, prevent or otherwise inder medicious code outbreaks? Yes No 5. Are workstain and security indicant tesponse in place to define roles and responsibilities to minimize a | 5. Is there a process to automatically detect and respond to suspicious activity on the networks? | Yes | | | | | | | |
| 8. Is Intrusion Prevention (IPS) installed and executing effectively? No No 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 network-based intrusion detection and/or prevention devices deployed to protect sensitive network segments or application? No 2. System No Ves 3. Administrative Privileged Use No Ves 4. Administrative Privileged Use Yes No 5. Are where tools deployed within the network infrastructure devices aggregated? No Ves 13. Can security-related logs be made available to the client if requested? If Yes, how long is the log-retention period? Yes Pres 14. Is anti-virus oftware installed and executing on all workstations and server connected to the network? Yes Pres 15. Are where procedures for employees to report and respons to detect, prevent or otherwise hinder malicious code outbreaks? Yes Pres 16. Is there a computer security incident response process in place to define roles and responsibilities to minimize an incident's impact? Yes Yes 2. Will the | | N/A | | | | | | | |
| A 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)? Are there network-based intrusion detection and/or prevention devices deployed to protect sensitive network segments or applications? Yes NA < tense network-based intrusion detection and/or prevention devices deployed to protect sensitive network segments or applications? Yes NA < tense network-based intrusion detection and/or prevention devices deployed to protect sensitive network segments or applications? Application File/Folder level access Application Application Administrative Privileged Use Are security-related logs from key network and security infrastructure devices aggregated? Yes No NA No NA No NA No | 7. Are network and infrastructure security patches assessed as "critical" deployed in less than 5 days? | Yes | | | | | | | |
| 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 in logging of the: No Incommerce infrastructure)? a. System Yes Incommerce infrastructure)? b. File/Folder level access Yes Incommerce infrastructure)? c. Application Yes Incommerce infrastructure)? d. Administrative Privileged Use Yes Incommerce infrastructure)? 12. Are security-related logs from key network and security infrastructure devices aggregated? No Incommerce infrastructure)? 13. Can security-related logs be made available to the client if requested? If Yes, how long is the log-retention period? Yes Incommerce infrastructure)? 14. Is anti-irrus offware installed and exercuting on all workstations and servers connected to the network? Yes Incommerce 15. Are workstation and server virus anti-irrus offware signatures updated automatically? Yes Incommerce Yes 1. Is there tools deployed within the network infrastructure to deten, prevent or otherwise hinder malicious code outbreaks? Yes Incommerce 2. Are there procedures for employees to report and respond to (suspected) information security policy violations? Yes Incommerce 3. Will the clienthe notified immediately if an incident cozers of the asser | 8. Is Intrusion Prevention (IPS) installed and executing effectively? | No | | | | | | | |
| 11. Is there logging of the: NA * Leave Member 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 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 automaticult? Yes 16. Are there tools deployed within the network infrastructure to detect, prevent or otherwise hinder malicious code outbreaks? Yes 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 violations? Yes 3. Will the client be acking up to 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 and asprocessing location? No | | Yes | | | | | | | |
| a. System Yes b. File/Folder level access No c. Application No d. Administrative Privileged Use Yes 12. Are security-related logs from key network and security infrastructure devices aggregated? No 13. Can security-related logs to make available to the client if requested? If Yes, how long is the log-retention period? Yes 14. Is anti-virus software installed and executing on all workstations and server sions and server virus anti-virus software signatures updated automatically? Yes 15. Are workstation and server virus anti-virus software signatures updated automatically? Yes Image: Comparison of the computer security indicent response in place to define roles and responsibilities to minimize an incident's impact? Yes Image: Comparison of the computer security incident response to report and respond to (suspected) information security policy violations? Yes Image: Comparison of the comp | 10. Are there network-based intrusion detection and/or prevention devices deployed to protect sensitive network segments or applications? | Yes | | | | | | | |
| b. File/Folder level access No Image: Construction c. Application Yes Image: Construction 12. Are security-related logs form key network and security infrastructure devices aggregated? No Image: Construction 13. Can security-related logs form key network and security infrastructure devices aggregated? No Image: Construction 14. Is anti-virus software installed and executing on all workstations and servers connected to the network? Yes Image: Construction 15. Are workstation and server virus anti-virus software signatures updated automatically? Yes Image: Construction Yes 16. Are there tools deployed within the network infrastructure to detect, prevent or otherwise hinder malicious code outbreaks? Yes Image: Construction Yes 1. Is there a computer security incident response process in place to define roles and responsibilities to minimize an incident's impact? Yes Yes 2. Are there procedures for employees to report and respond to (suspected) information security violations? Yes Yes 3. Will the client be notified immediately if an incident occurs that may affect its data or services? Yes Image: Construction 2. Is there a comprehensive, documented and secure proces | 11. Is there logging of the: | N/A | <leave blank=""></leave> | | | | | | |
| C Application C Administrative Privileged Use C Are security-related logs to made available to the client if requested? If Yes, how long is the log-retention period? Yes C Are security-related logs be made available to the client if requested? If Yes, how long is the log-retention period? Yes C Are there tools deployed within the network infrastructure to detect, prevent or otherwise hinder malicious code outbreaks? Yes C Control Security incident response process in place to define roles and responsibilities to minimize an incident's impact? Are there procedures for employees to report and respond to (suspected) information security policy violations? Yes Ves C Control Contingency Planning Is client that 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? Is there a comprehensive, documented and secure process to handle all media on-site, off-site and during Are backup tapes encrypted? Are backup tapes encrypted? Are backup tapes encrypted? Are the primary and secondary site located in secure process to rate facilities? Are the primary and secondary site located in secure process or pare facilities? Are backup tapes encrypted? Are the primary and secondary site located in secure process in place to detat secure process in ViA No tapes No No | a. System | Yes | | | | | | | |
| d. Administrative Privileged Use Yes 12. Are security-related logs form key network and security infrastructure devices aggregated? No 13. Can security-related logs form key network and security infrastructure devices aggregated? No 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 16. Are there tools deployed within the network infrastructure to detect, prevent or otherwise hinder malicious code outbreaks? Yes 16. Are there procedures for employees to report and respons to (suspected) information security policy violations? Yes 2. Will the client be notified immediately if an incident occurs that may affect its data or service? Yes 16. Is there a comprehensive, documented and secure process to handle all media on-site, off-site and during No 3. Are backup tested periodically to taps available to be restored for at least seven years? No 4. Are the primary and secondary secondary recovery site for recovery and continuity? Yes 3. Are backup tapes savaliable to be restored for at least seven years? No 4. Are backup tapes savailable to be restored for at least seven years? <td>b. File/Folder level access</td> <td>No</td> <td></td> | b. File/Folder level access | No | | | | | | | |
| 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 immittie 14. Is anti-virus software installed and executing on all workstations and servers connected to the network? Yes immittie 15. Are workstation and server virus anti-virus software signatures updated automatically? Yes immittie 16. Are there tools deployed within the network infrastructure to detect, prevent or otherwise hinder malicious code outbreaks? Yes immittie 17. Is there a computer security incident response process in place to define roles and responsibilities to minimize an incident's impact? Yes immittie 18. Is there a computer security incident response process in place to define roles and responsibilities to minimize an incident's impact? Yes immittie 19. Is client data backed up to tape and stored offsite 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 immittie 1. Is client data backed up to tape and stored offsite 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 immittie 2. Is there a comprehensive, documented and ascure process to handl | c. Application | Yes | | | | | | | |
| 13. Can security-related logs be made available to the client if requested? If Yes, how long is the log-retention period? Yes 8 moniths 14. Is anti-virus software installed and executing on all workstations and servers connected to the network? Yes 1 15. Are workstation and server virus anti-virus software signatures updated automatically? Yes 1 16. Are there tools deployed within the network infrastructure to detect, prevent or otherwise hinder malicious code outbreaks? Yes 1 17. Is there a computer security incident response process in place to define roles and responsibilities to minimize an incident's impact? Yes 1 18. Is there a computer security incident response process in place to define roles and responsibilities to minimize an incident's impact? Yes 1 2. Are there procedures for employees to report and respond to (suspected) information security policy violations? Yes 1 3. Will the client be notified immediately if an incident occurs that may affect its data or services? Yes 1 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 No 2. Is there a comprehensive, documented and secure process to handle all media on-site, off-site and during N/A No No 3. A | | Yes | | | | | | | |
| 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 Yes 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 9. Lo 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 1. Is there a secure secondary recovery site for recovery and continuity? Na Na 3. Are backup tapes encrypted? Na Na Na 4. Are backup tapes encrypted? NA Na NA 5. Is there a secure secondary recovery and continuity? Yes NA Yes 6. Is there a secure secondary recovery and continuity? Yes NA | , | No | | | | | | | |
| 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 Yes 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 Yes 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 2. Is there a comprehensive, documented and secure process to handle all media on-site, off-site and during N/A 3. Are backup tapes encrypted? Yes 4. Are backup tapes encrypted? N/A 5. Are the primary and seccondary site located in secure, business-grade facilities? Yes 6. Is there a secure secondary recovery plan and prepared to execute it successfully? Yes 7 Are the primary and seccordary site located in secure, business | 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 | | | | | | |
| 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 | 14. Is anti-virus software installed and executing on all workstations and servers connected to the network? | Yes | | | | | | | |
| Incident Response and Notification to the Client Is there a computer security incident response process in place to define roles and responsibilities to minimize an incident's impact? Yes Are there procedures for employees to report and respond to (suspected) information security policy violations? Yes Secure Access, UPS, etc.) at least twenty miles away from the primary data processing location? Is there a comprehensive, documented and secure process to handle all media on-site, off-site and during Are backup tapes encrypted? Are backup tapes encrypted? Are backup tapes available to be restored for at least seven years? Is there a secure secondary recovery site for recovery and continuity? Yes Is the pinary and secondary site located in secure, business-grade facilities? Is the Disaster Recovery plan tested successfully with the results documented at least once per year? Are all of the employees aware of the Disaster Recovery plan and prepared to execute it successfully? Yes Nill client representative(s) be notified of a disaster declaration immediately? | 15. Are workstation and server virus anti-virus software signatures updated automatically? | Yes | | | | | | | |
| 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 Not 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 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? No 4. Are backup tapes encrypted? N/A 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 immediate | 16. Are there tools deployed within the network infrastructure to detect, prevent or otherwise hinder malicious code outbreaks? | Yes | | | | | | | |
| 2. Are there procedures for employees to report and respond to (suspected) information security policy violations? Ites 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? 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 No 3. Are backup tapes encrypted? Not harded up to tape available to be restored for at least seven years? 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 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? | Incident Response and Notification to the Client | | | | | | | | |
| 3. Will the client be notified immediately if an incident occurs that may affect its data or services? Yes 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? 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 backup tapes encrypted? Ni/A 5. Are client monthly backup tapes available to be restored for at least seven years? Ni/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 9. Are all of the employees for processing eDiscovery requests on behalf of your customers? If yes, please describe your process in Yes 10. Woy uhave a defined process for processing eDiscovery requests on behalf of your customers? If yes, plea | 1. Is there a computer security incident response process in place to define roles and responsibilities to minimize an incident's impact? | Yes | | | | | | | |
| Backup, Disaster Recovery, and Contingency Planning Not 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? 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 backup tapes encrypted? N/A 4. Are backup tapes available to be restored for at least seven years? N/A 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 9. Are all of the employees for processing eDiscovery requests on behalf of your customers? If yes, please describe your process in Yes 10. Do you have a defined process for processing eDiscovery requests on | 2. Are there procedures for employees to report and respond to (suspected) information security policy violations? | Yes | | | | | | | |
| 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 2. Is there a comprehensive, documented and secure process to handle all media on-site, off-site and during NA 3. Are backups tested periodically to ensure data can be recovered? Yes 4. Are backup tapes encrypted? NA 5. Are client monthly backup tapes available to be restored for at least seven years? NA 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 Image: Please provide contact details | 3. Will the client be notified immediately if an incident occurs that may affect its data or services? | Yes | | | | | | | |
| access, UPS, etc.) at least twenty miles away from the primary data processing location? No 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 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 eDiscovery - Access to Data Please provide contact details 1. Do you have a defined process for processing eDiscovery requests on behalf of your customers? If yes, please describe your process in Image: second | Backup, Disaster Recovery, and Contingency Planning | | | | | | | | |
| 2. Is there a comprehensive, documented and secure process to handle all media on-site, off-site and during 3. Are backups tested periodically to ensure data can be recovered? 4. Are backup tapes encrypted? 5. Are client monthly backup tapes available to be restored for at least seven years? 6. Is there a secure secondary recovery site for recovery and continuity? 7. Are the primary and secondary site located in secure, business-grade facilities? 8. Is the Disaster Recovery plan tested successfully with the results documented at least once per year? 9. Are all of the employees aware of the Disaster Recovery plan and prepared to execute it successfully? 1. Will client representative(s) be notified of a disaster declaration immediately? 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 | | No | Not backed up to tape, but to disk | | | | | | |
| 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 N/A 6. Is there a secure secondary recovery site for recovery and continuity? Yes Image: Control of the primary and secondary site located in secure, business-grade facilities? Yes Image: Control of the primary and secondary site located in secure, business-grade facilities? Yes Image: Control of the primary and secondary site located in secure, business-grade facilities? Yes Image: Control of the primary and secondary site located in secure, business-grade facilities? Yes Image: Control of the primary and secondary site located in secure, business-grade facilities? Yes Image: Control of the primary and secondary site located in secure, business-grade facilities? Yes Image: Control of the primary and secondary site located in secure, business-grade facilities? Yes Image: Control of the primary and secondary site located in secure, business-grade facilities? Yes Image: Control of the primer secondary site located in and prepared to execute it successfully? Yes Image: Control of the primer secondary | | | | | | | | | |
| 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 No tapes 6. Is there a secure secondary recovery site for recovery and continuity? Yes Yes 7. Are the primary and secondary site located in secure, business-grade facilities? Yes Yes 8. Is the Disaster Recovery plan tested successfully with the results documented at least once per year? Yes Yes 9. Are all of the employees aware of the Disaster Recovery plan and prepared to execute it successfully? Yes Yes 10. Will client representative(s) be notified of a disaster declaration immediately? Yes, please describe your process in Yes Pliscovery - 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 Image: Contact details | | | | | | | | | |
| 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 Image: Contact details | | | No tanes | | | | | | |
| 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 | | - | no tapes | | | | | | |
| 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 | | | | | | | | | |
| 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 eDiscovery - Access to Data Please provide contact details 1. Do you have a defined process for processing eDiscovery requests on behalf of your customers? If yes, please describe your process in Image: Contact details | | | | | | | | | |
| 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 | | | | | | | | | |
| 10. Will client representative(s) be notified of a disaster declaration immediately? Yes Please provide contact details eDiscovery - Access to Data . </td <td></td> <td></td> <td></td> | | | | | | | | | |
| 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 | | | | | | | | | |
| 1. Do you have a defined process for processing eDiscovery requests on behalf of your customers? If yes, please describe your process in | | Yes | | | | | | | |
| | | | | | | | | | |
| | | N/A | | | | | | | |