4th Season Consulting

Internal Security Assessment

<Vendor Name Here>

Click or tap to enter a date.

Internal Security Assessment

|  |  |  |
| --- | --- | --- |
| Question | Yes or No? | Comments |
| Policies and Procedures |
| Does the vendor have documented security policies and procedures that align with industry standards? | Choose an item. | Click or tap here to enter text. |
| Does the vendor review their policies and procedures annually at a minimum? | Choose an item. | Click or tap here to enter text. |
| Security Training and Awareness |
| Does the vendor have a process for training all workforce as required by state and federal regulations? | Choose an item. | Click or tap here to enter text. |
| Does the vendor conduct regular testing for compliance with security training through phishing campaigns or similar programs? | Choose an item. | Click or tap here to enter text. |
| Does the vendor require specialized training related to workforce member job description? | Choose an item. | Click or tap here to enter text. |
| Does the vendor require contingency training for appropriate workforce members? | Choose an item. | Click or tap here to enter text. |
| Does the vendor conduct regular awareness training for emerging threats? | Choose an item. | Click or tap here to enter text. |
| Does the vendor training include acceptable use of vendor assets? | Choose an item. | Click or tap here to enter text. |
| Patch Management |
| Does the vendor have a patch management process? | Choose an item. | Click or tap here to enter text. |
| Does the vendor identify different levels of importance for patches and maintain a different process accordingly? | Choose an item. | Click or tap here to enter text. |
| Does the vendor have a process for testing patches before distribution? | Choose an item. | Click or tap here to enter text. |
| Network Security Management |
| Does the vendor maintain a network diagram showing all appropriate assets? | Choose an item. | Click or tap here to enter text. |
| Does the vendor regularly review their network diagram? | Choose an item. | Click or tap here to enter text. |
| Does the vendor regularly conduct penetration testing, vulnerability assessments, and other industry-standard procedures? | Choose an item. | Click or tap here to enter text. |
| Does the vendor maintain a separate network for guest access? | Choose an item. | Click or tap here to enter text. |
| Does the vendor regulate all non-vendor-approved technology to the guest network, including personal devices belonging to workforce members? | Choose an item. | Click or tap here to enter text. |
| Does the vendor maintain separate environments for development, user acceptance, and production as appropriate? | Choose an item. | Click or tap here to enter text. |
| Does the vendor maintain a DMZ for internet-facing systems? | Choose an item. | Click or tap here to enter text. |
| Does the vendor have a change management process? | Choose an item. | Click or tap here to enter text. |
| Does the vendor enforce industry-standard encryption for network traffic as appropriate? | Choose an item. | Click or tap here to enter text. |
| Does the vendor have a mobile device policy for securing BYOD and personal assets? | Choose an item. | Click or tap here to enter text. |
| Does the vendor lock accounts after a certain number of invalid login attempts within a period of time? | Choose an item. | Click or tap here to enter text. |
| Facility and Environmental Security |
| Does the vendor define and label restricted areas? | Choose an item. | Click or tap here to enter text. |
| Does the vendor track access to restricted areas? | Choose an item. | Click or tap here to enter text. |
| Does the vendor train their workforce on processes and procedures for access to restricted areas? | Choose an item. | Click or tap here to enter text. |
| Does the vendor maintain a list of workforce personnel with access to restricted areas? | Choose an item. | Click or tap here to enter text. |
| Does the vendor require visitors to identify themselves and sign in at a central location? | Choose an item. | Click or tap here to enter text. |
| Does the vendor require their workforce to wear identification badges while in the office or other work environments? | Choose an item. | Click or tap here to enter text. |
| Does the vendor monitor restricted areas with video cameras? | Choose an item. | Click or tap here to enter text. |
| Does the vendor maintain video surveillance for a minimum of 14 days?  | Choose an item. | Click or tap here to enter text. |
| Does the vendor require key, badge, or other controls for restricted areas?  | Choose an item. | Click or tap here to enter text. |
| Does the vendor require visitors to wear a visitor badge, temporary name tag, or in some other way identify themselves from workforce? | Choose an item. | Click or tap here to enter text. |
| Identification and Authentication |
| Does the vendor assign each workforce member individual credentials? | Choose an item. | Click or tap here to enter text. |
| Does the vendor follow strong password best practices including minimum length; a mix of upper case, lower case, numbers, and special characters; and regular expiration or strong passphrases? | Choose an item. | Click or tap here to enter text. |
| Does the vendor log all access to systems, files, databases, hardware, and other assets? | Choose an item. | Click or tap here to enter text. |
| Does the vendor regularly review who has access to systems, files, databases, hardware, and other assets? | Choose an item. | Click or tap here to enter text. |
| Does the vendor require workforce members with administrator access to utilize a least-privileged account when administrator privileges are not needed? | Choose an item. | Click or tap here to enter text. |
| Are authentication mechanisms used, such as multi-factor authentication or strong passwords? | Choose an item. | Click or tap here to enter text. |
| Is data encrypted both at rest and in transit? | Choose an item. | Click or tap here to enter text. |
| Information Access Management |
| Does the vendor have a process for handling requests for access to vendor systems? | Choose an item. | Click or tap here to enter text. |
| Does the vendor perform background checks on all workforce members? | Choose an item. | Click or tap here to enter text. |
| Does the vendor ensure access to information is restricted to the principles of minimum necessary? | Choose an item. | Click or tap here to enter text. |
| Does the vendor have a process to lock accounts not accessed within a reasonable period of time? | Choose an item. | Click or tap here to enter text. |
| Does the vendor have a process for changing default credentials? | Choose an item. | Click or tap here to enter text. |
| Does the vendor have a privileged access management process? | Choose an item. | Click or tap here to enter text. |
| Does the vendor have a process for managing exceptions to standard procedures? | Choose an item. | Click or tap here to enter text. |
| Does the vendor identify different categories of their workforce by job function and apply policies accordingly? | Choose an item. | Click or tap here to enter text. |
| Risk Management |
| Does the vendor have a documented risk management program? | Choose an item. | Click or tap here to enter text. |
| Does the vendor have a risk management program that is regularly updated and aligned with industry standards? | Choose an item. | Click or tap here to enter text. |
| Does the vendor's contract include language that addresses security, data privacy, and data breach notification requirements? | Choose an item. | Click or tap here to enter text. |
| Does the vendor perform risk analysis of their IT infrastructure and identify potential vulnerabilities annually at a minimum? | Choose an item. | Click or tap here to enter text. |
| Does the vendor have tech errors and omissions insurance? | Choose an item. | Click or tap here to enter text. |
| Does the vendor have cyber insurance? | Choose an item. | Click or tap here to enter text. |
| Security Controls |
| Does the vendor have physical, technical, and administrative security controls in place? | Choose an item. | Click or tap here to enter text. |
| Does the vendor have access controls in place, and is access to data restricted based on roles and responsibilities? | Choose an item. | Click or tap here to enter text. |
| Does the vendor require workforce with administrator access to utilize a least-privileged account when administrator privileges are not needed? | Choose an item. | Click or tap here to enter text. |
| Does the vendor have data backup and recovery procedures in place? | Choose an item. | Click or tap here to enter text. |
| Is the vendor compliant with applicable regulations including HIPAA, HITECH, and other state or national privacy laws? | Choose an item. | Click or tap here to enter text. |
| Does the vendor have a process in place for monitoring their security posture? | Choose an item. | Click or tap here to enter text. |
| Does the vendor perform periodic audits to detect new security risks? | Choose an item. | Click or tap here to enter text. |
| Does the vendor undergo independent compliance audits at least annually (HITRUST, SOC, ISO, or similar)? | Choose an item. | Click or tap here to enter text. |
| Does the vendor provide evidence of independent compliance audits upon request? | Choose an item. | Click or tap here to enter text. |
| Third-Party Vendor Risk |
| Does the vendor use third-party service providers, and if so, do they have security controls in place? | Choose an item. | Click or tap here to enter text. |
| Does the vendor have a process for assessing third-party vendor security risks? | Choose an item. | Click or tap here to enter text. |