**Cigna Information Security Summary of Controls Questionnaire**

Please check the box for your organization’s level of compliance with the following information security controls. If a control is not applicable, check N/A.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Does your company provide 24 x 7 x 365 Security Operations and Incident Response? | | | | |
| No  x☐ | Yes, partial  ☐ | Yes, full  ☐ | N/A  ☐ | **Comments:** |
| 1. Does your company have a Forensics and Incident Response Retainer Service? | | | | |
| No  ☐ | Yes, partial  x☐ | Yes, full  ☐ | N/A  ☐ | **Comments:** |
| 1. Does your company have a documented and continuously tested Incident Response plan? | | | | |
| No  ☐ | Yes, partial  ☐ | Yes, full  x☐ | N/A  ☐ | **Comments:** |
| 1. Does your company have an Intrusion Prevention and Detection System? | | | | |
| No  ☐ | Yes, partial  ☐ | Yes, full  x☐ | N/A  ☐ | **Comments:** |
| 1. Does your company have Network Access Controls? Please provide details. | | | | |
| No  ☐ | Yes, partial  ☐ | Yes, full  ☐ | N/A  x☐ | **Comments: We do not have an internal network.** |
| 1. Does your company have Web Content Filtering? Please provide brief details around the controls used. | | | | |
| No  ☐ | Yes, partial  ☐ | Yes, full  x☐ | N/A  ☐ | **Comments:** |
| 1. Does your company do Security Event Logging, Aggregation, and Alerting? Please provide brief details around the controls used. | | | | |
| No  ☐ | Yes, partial  ☐ | Yes, full  x☐ | N/A  ☐ | **Comments: Security event logging is done on the cleardata sFTP instances** |
| 1. Does your company have a comprehensive Data Loss Prevention (DLP) program for USB, Web, and email? Please provide brief details around the controls used. | | | | |
| No  ☐ | Yes, partial  ☐ | Yes, full  x☐ | N/A  ☐ | **Comments: We have EPP (Endpoint Protector) installed on all VCR end points which provides the following features 1) Content Filtering - Based on the predefined and company approved Content aware policy and also prevent browser plugins and ActiveX filters.**  **2) EPP Rule set - List of rules which disables USB, CD DVD RW, printer, file sharing, Bluetooth, PCMCIA devices etc..** |
| 1. Do you encrypt data in transit? Please provide brief details around the controls used. | | | | |
| No  ☐ | Yes, partial  ☐ | Yes, full  x☐ | N/A  ☐ | **Comments: https/sftp with SSL/TLS encryption** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Do you encrypt data at rest? Please provide brief details around the controls used. | | | | |
| No  ☐ | Yes, partial  ☐ | Yes, full  x☐ | N/A  ☐ | **Comments: Data at rest is encrypted with AES 128 bit with 256 bit key** |
| 1. Do you have data encryption on your endpoints? Please provide brief details around the controls used. | | | | |
| No  ☐ | Yes, partial  ☐ | Yes, full  x☐ | N/A  ☐ | **Comments: Yes, Disk level encryption using FileVault** |
| 1. Does your company use multifactor authentication (MFA) for remote user access into your corporate network? | | | | |
| No  ☐ | Yes, partial  ☐ | Yes, full  ☐ | N/A  x☐ | **Comments: We do not have an internal corporate network, we rely on services. Access to those services requires MFA.** |
| 1. Does your company use multifactor authentication (MFA) for corporate web mail access? | | | | |
| No  ☐ | Yes, partial  ☐ | Yes, full  x☐ | N/A  ☐ | **Comments:** |
| 1. Does your company use multifactor authentication (MFA) for privileged user activity? | | | | |
| No  ☐ | Yes, partial  ☐ | Yes, full  x☐ | N/A  ☐ | **Comments:** |
| 1. Does your company have SAML/Federation capabilities? Please provide brief details around the controls used. | | | | |
| No  x☐ | Yes, partial  ☐ | Yes, full  ☐ | N/A  ☐ | **Comments:** |
| 1. Does your company have CCTV surveillance of sensitive areas? | | | | |
| No  x☐ | Yes, partial  ☐ | Yes, full  ☐ | N/A  ☐ | **Comments: Data is stored in the compliant cloud environment. We have no access to those locations.** |
| 1. Has your company deployed physical security access controls? | | | | |
| No  ☐ | Yes, partial  ☐ | Yes, full  x☐ | N/A  ☐ | **Comments:** |
| 1. Does your company run periodic vulnerability scans? How often? | | | | |
| No  ☐ | Yes, partial  ☐ | Yes, full  x☐ | N/A  ☐ | **Comments: Quarterly** |
| 1. Does your company run periodic source code scans? How often? By whom? | | | | |
| No  x☐ | Yes, partial  ☐ | Yes, full  ☐ | N/A  ☐ | **Comments:** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Does your company have run periodic penetration testing? How often? By whom? | | | | |
| No  ☐ | Yes, partial  ☐ | Yes, full  x☐ | N/A  ☐ | **Comments: Yes, we engage third party vendors to do penetration testing annually.** |
| 1. Do your company’s Information Security policies and procedures align with industry accepted standards, e.g., NIST, ISO, etc.? | | | | |
| No  ☐ | Yes, partial  ☐ | Yes, full  x☐ | N/A  ☐ | **Comments:** |
| 1. Does your company have an Enterprise Risk Management (ERM) program? | | | | |
| No  ☐ | Yes, partial  ☐ | Yes, full  x☐ | N/A  ☐ | **Comments:** |