CORE COMPLIANCE & LEGAL SERVICES, INC.

## Cybersecurity Review Checklist

Please use the following cybersecurity review checklist for consideration in crafting your transactional, periodic, and forensic testing of your cybersecurity program. Please note that this checklist may need to be further customized to properly document cybersecurity risks and reviews that are specific to your Firm's business enterprise and compliance program. For more information on, or assistance with conducting cybersecurity testing or other compliance areas, please contact us at info@corecls.com, at (619) 278-0020, or visit us at www.corecls.com.

| | |
|---|---|
| ***Software*** | |
| Yes☐ No ☐ | Is the Firm's software inventory current? Has IT provided the CCO and/or ISO with the Firm's most current software inventory? |
| Yes☐ No ☐ | Was any new software installed on the Firm's Systems tested and vetted before installation? |
| Yes☐ No ☐ | Have software updates been deployed regularly? |
| Yes☐ No ☐ | Have security patches been deployed regularly? |
| Yes☐ No ☐ | Have any significant software errors compromised the security of the Firm's Systems? |
| Yes☐ No ☐ | Are redundancies and backups being performed regularly, are there any issues, and how quickly are those issues resolved? |
| ***Hardware*** | |
| Yes☐ No ☐ | Is the Firm's hardware inventory current? Has IT provided the CCO and/or ISO with the Firm's most current hardware inventory? |
| Yes☐ No ☐ | Was new hardware tested and vetted before installation? |
| Yes☐ No ☐ | Does the Firm's new hardware have up-to-date software installed on it? |
| Yes☐ No ☐ | Have all external non-Firm issued devices been approved by the CCO/ISO prior to use? |
| Yes☐ No ☐ | Have any significant hardware issues compromised the security of the Firm's Systems? |
| ***Data Mapping*** | |
| Yes☐ No ☐ | Is the Firm's data mapping current? Has IT provided the CCO and/or ISO with the Firm's most current data map? |
| Yes☐ No ☐ | Have there been any issues with the data transmission to and from the Firm? |

CORE COMPLIANCE & LEGAL SERVICES, INC.

| | |
|---|---|
| ***Incident Response*** | |
| Yes☐ No ☐ | Were identification, containment, eradication, and post-incident recovery procedures followed and documented during any cyber-incidents? |
| Yes☐ No ☐ | Were steps on communicating with clients and law enforcement about the incident followed? Were these interactions documented? |
| Yes☐ No ☐ | Were steps on breach notification procedures under state data privacy laws and/or provide identity theft protection services for clients followed? Were these steps documented? |
| Yes☐ No ☐ | Have steps for remedial actions that needed to be taken and were additional controls put into place? |
| Yes☐ No ☐ | Was testing of the Firm's incident response plan conducted as part of the Firm's overall BCP testing during the year? |
| Yes☐ No ☐ | Were additional controls and/or resources needed in order to ensure the incident response plan continues to work effectively? Were these controls/resources implemented? |
| ***Data Loss Prevention*** | |
| Yes☐ No ☐ | Were logs of all software updates, patch deployments to ensure that scheduled jobs occurred maintained for the period? |
| Yes☐ No ☐ | Were logs reviewed to determine if there were instances of data ex-filtration? How quickly were those issues resolved? Was documentation provided to the CCO and/or ISO? |
| Yes☐ No ☐ | Were there any instances of any hacking or malware attempts that occurred during the quarter that involved the loss of data containing client PII and was documentation provided to the CCO and/or ISO? |
| Yes☐ No ☐ | Were there any continuous issues with the deployment of software updates, and patch deployments during the year? |
| Yes☐ No ☐ | Were logs consistently reviewed and maintained to determine if there were instances of data ex-filtration? How quickly those issues were resolved; and was documentation provided to the CCO and/or ISO? |
| ***Systems Users Responsibilities*** | |
| Yes☐ No ☐ | Did new systems users received credentials and complete cybersecurity training during the year? |
| Yes☐ No ☐ | Was any non-business issued software or hardware installed by any systems users without permission from the CCO and/or CISO? |
| Yes☐ No ☐ | Were all mobile devices that are used by the Firm's employees for business logged by the Firm and verified for business use? |
| Yes☐ No ☐ | Did employees with remote access to the Firm's Systems have multi-factor authentication set-up? |
| Yes☐ No ☐ | Did systems users complete annual cybersecurity training? Was additional training provided to users who did not complete the training? |

CORE COMPLIANCE & LEGAL SERVICES, INC.

| | |
|---|---|
| ***Access Rights and Controls*** | |
| Yes☐<br>No ☐ | Have access rights and controls for any employees whose responsibilities have changed during the period been reviewed, approved, and documented by the CCO and/or ISO? |
| Yes☐<br>No ☐ | Have access rights and controls been revoked for any employees who were terminated or placed on leave? |
| ***Vendor Management*** | |
| Yes☐<br>No ☐ | Have the access rights and controls for any new and existing third-party service providers been reviewed? Has documentation been provided to the CCO and/or ISO? |
| Yes☐<br>No ☐ | Have all due diligence questionnaires completed for new and existing vendors contained supplemental documentation for cybersecurity risk assessments; policies and procedures; incident response plans; and, business continuity plans been provided to the Firm? |
| ***Penalties for Violations*** | |
| Yes☐<br>No ☐ | Were any and all violations of the Firm's cybersecurity policies and procedures for the period documented and were proper steps were taken to deliver reasonable penalties? |
| ***Annual Risk Assessment*** | |
| Yes☐<br>No ☐ | Was the annual cybersecurity risk assessment performed and were there any significant gaps in controls? |
| Yes☐<br>No ☐ | Were additional controls and/or resources needed as a result of the risk assessment? Were these controls/resources implemented? |