## **CIS Critical Security Controls for Effective Cyber Defense Checklist**

 The Center for Internet Security (CIS) Controls are a set of security best practices that are used by organizations around the world. In 2016, the California Attorney General cited to the CIS Controls as a reference to reasonable security in the office’s 2016 Data Breach Report. This checklist may be used as a means of determining whether the dealership and its vendors have reasonable security measures in place.

|  |  |  |
| --- | --- | --- |
|  | YES | NO |
| 1. | Inventory of Authorized and Unauthorized Devices |  |  |
|  | YES | NO |
| 2. | Inventory of Authorized and Unauthorized Software |  |  |
|  | YES | NO |
| 3. | Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers |  |  |
|  | YES | NO |
| 4. | Continuous Vulnerability Assessment and Remediation |  |  |
|  | YES | NO |
| 5. | Controlled Use of Administrative Privileges |  |  |
|  | YES | NO |
| 6. | Maintenance, Monitoring, and Analysis of Audit Logs |  |  |
|  | YES | NO |
| 7. | Email and Web Browser Protections |  |  |
|  | YES | NO |
| 8. | Malware Defenses |  |  |
|  | YES | NO |
| 9. | Limitation and Control of Network Ports, Protocols, and Services |  |  |
|  | YES | NO |
| 10. | Data Recovery Capability |  |  |
|  | YES | NO |
| 11. | Secure Configurations for Network Devices such as Firewalls, Routers, and Switches |  |  |
|  | YES | NO |
| 12. | Boundary Defense |  |  |
|  | YES | NO |
| 13. | Data Protection |  |  |
|  | YES | NO |
| 14. | Controlled Access Based on the Need to Know |  |  |
|  | YES | NO |
| 15. | Wireless Access Control |  |  |
|  | YES | NO |
| 16. | Account Monitoring and Control |  |  |
|  | YES | NO |
| 17. | Security Skills Assessment and Appropriate Training to Fill Gaps |  |  |
|  | YES | NO |
| 18. | Application Software Security |  |  |
|  | YES | NO |
| 19. | Incident Response and Management |  |  |
|  | YES | NO |
| 20. | Penetration Tests and Red Team Exercises |  |  |