Data Security Questionnaire

AutoLeadstar Inc. d/b/a Fullpath

Updated: March 2023

Physical & Administrative Questions

1. Does your company have a written information security program? YES

CIS V8 – 17, NIST CSF - PR.IP-9; ISO 27001:2013 - 5.2; A.5; PCI DSS V4 - 10.1; SOC2 TSP SECTION 100 - CC5.3; CC9.1;

2. Does your company perform physical, administrative, and electronic risk assessments relating to information safeguards at least annually? YES

CIS V8 - 7.1-7.2; NIST CSF - ID.RA-1; ISO 27001:2013 - 6; 8.2; 9; PCI DSS V4 - 6.3; 11.3; SOC2 TSP SECTION 100 - CC3;

3. Does your company perform training on security awareness for all employees at least annually? YES

CIS V8 - 14.2 - 14.7; NIST CSF - PR.AT-1; ISO 27001:2013 - 7.3; A.7.2.2; PCI DSS V4 - 12.6; SOC2 TSP SECTION 100 - CC1.4;

4. Does your company have a cybersecurity insurance policy that covers data breaches affecting customer personal information that you collect, receive, store, or process on our behalf? YES

5. Does your company have a process and/or policy that limits the ability to request and access files (whether stored physically or electronically) containing customer personal information to only authorized individuals with a need-to-know basis? YES

CIS V8 - 6.8; NIST CSF - PR.AC-4; ISO 27001:2013 - A.9.2; PCI DSS V4 - 7; SOC2 TSP SECTION 100 - CC6.3;

6. Does your company provide a mechanism for the secure destruction and disposal of documents containing customer personal information, such as locked shredding bins? YES

CIS V8 - 3.5; NIST CSF - PR.DS-3; PR.IP-6; ISO 27001:2013 - A.8.3.2; A.11.2.7; A.18.1.3; PCI DSS V4 - 9.4.6; 9.4.7; SOC2 TSP SECTION 100 - C1.2; CC6.5;

7. Does your company ask that each of your service providers and sub-processors sign a data processing agreement that complies with applicable state and federal data privacy laws? YES

CIS V8 - 15.4; NIST CSF - ID.SC-3; ISO 27001:2013 - 4.2; A.15; PCI DSS V4 - 12.8.2; SOC2 TSP SECTION 100 - CC9.2;

8. Does your company use and share only fictitious or test data (not real customer information) for training, development, or testing purposes? YES

CIS V8 - 3.1; NIST CSF - PR.AC-4; ISO 27001:2013 - A.14.3; PCI DSS V4 - 6.5.5; SOC2 TSP SECTION 100 - C1.1;

9. Has your company experienced a data breach affecting customer personal information in the past 12 months? NO

Electronic & Technical Questions

1. Does your company have endpoint detection and response (EDR) software installed on all endpoint devices that is continuously monitored and managed? YES

CIS V8 - 13.7; NIST CSF - DE.CM-1; ISO 27001:2013 - A.12.4; A.12.2.1; PCI DSS V4 - 12.10.5; SOC2 TSP SECTION 100 - CC7.2;

2. Does your company perform automated backups of sensitive data or critical enterprise assets that are either stored offline or on segregated systems? YES

CIS V8 - 11; NIST CSF - PR.IP-4; PR.PT-5; ISO 27001:2013 - A.12.3; PCI DSS V4 - 9.4.1; SOC2 TSP SECTION 100 - A1.2; CC6.4;

3. Does your company conduct social engineering and phishing simulations? YES

CIS V8 - 14.2; NIST CSF - PR.AT-1; ISO 27001:2013 - 7.3; A.7.2.2; PCI DSS V4 - 12.6.3.1; SOC2 TSP SECTION 100 - CC2.2;

4. Has your company performed a penetration test in the last 12 months? YES. We perform at least annual testing every January.

CIS V8 - 18; NIST CSF - PR.IP-7; ISO 27001:2013 - A.12.6.1; PCI DSS V4 - 11.4; SOC2 TSP SECTION 100 - CC3.2;

5. Does your company regularly run internal and external vulnerability scans? YES. We perform at least annual testing every January.

CIS V8 - 7.5 - 7.7; NIST CSF - DE.CM-8; ISO 27001:2013 - A.12.6; PCI DSS V4 - 6.3.1; SOC2 TSP SECTION 100 - CC7.1;

6. Does your company store network user credentials securely by ensuring such credentials are not stored in plain, readable text or in a vulnerable format? YES

CIS V8 - 3.11; NIST CSF - PR.DS-1; ISO 27001:2013 - A.10; PCI DSS V4 - 8.3.2; SOC2 TSP SECTION 100 - CC6.1;

7. Does your company grant administrator privileges to your network and applications on a least-access, role-based, and need-to-know basis? YES

; CIS V8 - 6.8; NIST CSF - PR.AC-4; ISO 27001:2013 - A.9.1; A.9.2; PCI DSS V4 - 7; 9; SOC2 TSP SECTION 100 - CC6.1; CC6.3;

8. Does your company regularly update and patch third-party software (e.g., antivirus, firewalls) and test your network to ensure that such updates and patches have been successfully installed on all applicable devices? YES

CIS V8 - 7.3 - 7.4; NIST CSF - ID.RA-1; ISO 27001:2013 - A.12.2; PCI DSS V4 - 6.3.3; SOC2 TSP SECTION 100 - CC7.1;

Software Services

1. Does your company offer software or applications as part of its services? This includes, but is not limited to, software-as-a-service tools, online web portals, desktop or server software, or mobile applications. YES

2. Does the software or application your company offers support multi-factor authentication, such as SMS or email tokens? YES

CIS V8 - 6.3; NIST CSF - PR.AC-7; ISO 27001:2013 - A.9.4.2; PCI DSS V4 - 8.4; SOC2 TSP SECTION 100 - CC6.1; CC6.6;

3. Does the software or application your company offers require the use of complex and unique passwords (alpha-numeric and non-dictionary words) for all systems containing customer personal information? YES

CIS V8 - 5.2; NIST CSF - PR.AC-1; ISO 27001:2013 - A.9.4.3; PCI DSS V4 - 8.3; SOC2 TSP SECTION 100 - CC6.1;

4. Does the software or application your company offers protect against brute-force attacks by suspending or disabling user credentials after a certain number of unsuccessful login attempts? YES

CIS V8 - 4.10; NIST CSF - PR.AC-1; ISO 27001:2013 - A.9.4.2; PCI DSS V4 - 11.4.2; 11.4.3; SOC2 TSP SECTION 100 - CC6.1; CC6.6;

5. Does the software or application your company offers use properly configured and industry-tested methods of encryption to keep customer personal information secure in transit and at rest? YES

CIS V8 - 3.10 - 3.11; NIST CSF - PR.DS-1; PR.DS-2; ISO 27001:2013 - A.10; PCI DSS V4 - 3.5.1; 4.2.1; SOC2 TSP SECTION 100 - CC6.1; CC6.7;

6. Does your company (1) employ engineers trained in secure coding, (2) test for common vulnerabilities, (3) follow platform and OS guidelines for security, and (4) verify that privacy and security features work as intended? YES

CIS V8 - 16; NIST CSF - PR.IP-1; PR.IP-2; ISO 27001:2013 - A.14.2; PCI DSS V4 - 6.2.1; 6.2.4; SOC2 TSP SECTION 100 - CC1.4;