Progressive Your Networking IT Partner COMPUTER SYSTEMS, Inc.

FTC SAFEGUARDS RULE

Checklist

1 CONDUCT A DATA INVENTORY

- [ ] Identify and document all sensitive customer information collected, stored, or transmitted by your company.

2 RISK ASSESSMENT

- [ ] Assess potential risks to the security, confidentiality and integrity of customer information.
- [ ] Identify vulnerabilities and potential threats to customer data.
- [ ] Evaluate the effectiveness of current safeguards.

3 WRITTEN INFORMATION SECURITY PROGRAM (WISP)

- [ ] Create a comprehensive WISP outlining the safeguards implemented to protect customer information.
- [ ] Designate an individual responsible for overseeing the program

4 EMPLOYEE ACCESS TRAINING

- [ ] Provide regular training to all employees on the importance of safeguarding customer information.
- [ ] Educate them on security best practices, including password management, data handling & identifying potential threats.

5 ACCESS CONTROLS

- [ ] Implement strict access controls to limit employee access to customer data based on job responsibilities.
- [ ] Utilize strong passwords, multi-factor authentication & regularly review & update access privileges.

6 DATA ENCRYPTION

- [ ] Encrypt customer data during storage and transmission, ensuring data remains secure from unauthorized access.

7 VENDOR MANAGEMENT

- [ ] Assess the security practices of third-party vendors that have access to customer information.
- [ ] Enter into written agreements with vendors, clearly outlining their obligations to protect customer data.

8 INCIDENT RESPONSE PLAN

- [ ] Develop an incident response plan to promptly & effectively respond to data breaches or security incidents.
- [ ] Define responsibilities & procedures for addressing breaches, notifying affected individuals & mitigating.

9 REGULAR MONITORING AND AUDITING

- [ ] Implement ongoing monitoring and auditing procedures to detect unauthorized access or suspicious activity.
- [ ] Regularly review logs, conduct vulnerability assessments & perform security audits.

10 SECURE DISPOSAL

- [ ] Establish procedures for securely disposing of customer information, including physical documents and digital media.
- [ ] Use methods such as shredding or secure data destruction to prevent unauthorized retrieval.

For help securing your data with encryption, auditing access controls, and maintaining complete control of your data at rest and in motion, **book a free assessment with Progressive Computer Systems.**

Progressive Your Networking IT Partner COMPUTER SYSTEMS, Inc.

(919) 929-3080 | PCSsales@pc-net.com

To view the full rule and learn more about The Federal Trade Commission's Safeguards Rule visit FTC.gov.