FTC Safeguards Questionnaire Responses for Quality Assurance, Inc.

Contact

Primary Contact

Emily Rudh

Email

https://about.qaecrm.com/contact-us

Telephone

(218) 736-5247

16 CFR 314.4

Section (a) - General Requirements:

Have you designated Qualified Individual responsible for implementing and maintaining the information security program?

Yes.

Is there company executive oversight of the Qualified Individual?

Yes.

Section (b) - Information Security Program

Do you have a written information security program?

Yes.

Does your program include a risk assessment, which is performed on a regular, ongoing basis?

Yes.

Section (c) - Administrative Safeguards

Do you have measures in place to protect customer information from unauthorized access, use, or disclosure?

Yes.

Are these measures regularly reviewed and updated to reflect changes in technology or threats?

Yes.

Do you have change management procedures to execute changes in systems housing customer information?

Yes - we track changes through change requests and use IaC (Infrastructure As Code) wherever possible, which is also tracked in source control.

Do you regularly review the Information Security Program to ensure it is up-to-date?

Yes, annually or more frequently.

Do you monitor and detect any attempts to access customer information without authorization?

Yes.

Are customer information and records protected by encryption in transit and at rest?

Yes. We encrypt data at rest and at transit per our Information Security Program policies.

Are customer information and records protected by firewalls?

Yes. Our information systems containing customer information are behind a combination of routing and security groups.

Do you have a system in place to detect and respond to intrusions affecting customer information and records?

Yes. Monitoring and an incident response plan are in place.

Are customer information and records backed up and stored securely to prevent loss or unauthorized access?

Yes.

16 CFR 314.4 Section (d) - Security Assessments:

Do you have an information security program to ensure customer information is protected?

Yes.

Do you review the information security program and update it periodically to reflect changes in its business or risks to customer information?

Yes.

Do you conduct annual penetration testing of your information systems determined each given year based on relevant identified risks?

No. Penetration testing of our systems as a whole by is not performed on an annual basis due to the financial impacts of such an engagement. We engage with our industry expert partners on a

regular basis to penetration test new applications, or material changes to systems.

Do you perform vulnerability scanning on information systems containing customer information on a regular basis?

Yes.

16 CFR 314.4 Section (e) - Training and Management:

Do you provide training to employees regarding customer information protection?

Yes. We mandate employee cybersecurity training, per our Information Security Program.

16 CFR 314.4 Section (f) - Vendors

Do you have procedures in place to ensure service providers are protecting customer information?

Yes.

Do you have procedures in place to terminate relationships with service providers that fail to protect customer information?

Yes.

Do you have procedures in place for customer information to be returned or destroyed at the termination of the relationship with the service provider?

Yes.

16 CFR 314.4 Section (g) - Information Security Program Updates

Do you review your Information Security Program and update it periodically to reflect changes in its business or risks to customer information?

Yes.

Do you evaluate and adjust your information security program in light of any (including risk assessments) that may have a material impact on your information security program?

Yes.

16 CFR 314.4 Section (h) - Information Security Program Updates

Do you have incident response procedures in place to address any potential data breaches or unauthorized access to customer information?

Yes.

16 CFR 314.4 Section (i) - Reporting

Do you require your Qualified Individual to report in writing, regularly and at least annually to a senior officer responsible for your information security program

Yes.