FAXcentric Security FAQ

Category	*Question*	*Response*
Access Control and Physical Security	How do you ensure that only authorized personnel have access to customer data?	We have a role-based access control system in place that ensures that only authorized personnel have access to customer data.
	Do you perform background checks on your employees before granting them access to customer data?	Yes, we perform background checks on all employees who have access to customer data as part of our hiring process.
	What physical security measures do you have in place to protect against unauthorized access to customer data?	We have a secure data center that is monitored 24/7, and we have implemented physical security controls such as access controls, surveillance cameras, and alarm systems to protect against unauthorized access.
Incident Management and Response	How do you monitor and detect potential security incidents?	We have a security information and event management (SIEM) system in place that monitors our network and systems for potential security incidents.
	How do you respond to and mitigate security incidents?	We have an incident response plan that outlines our procedures for responding to security incidents, and our security team is trained to respond to incidents promptly and effectively.
	Do you have a documented incident response plan?	Yes, we have a documented incident response plan that is reviewed and updated regularly.
Vulnerability Management and Third-Party Risk	How often do you perform vulnerability assessments and penetration testing?	We perform vulnerability assessments and penetration testing on a quarterly basis to identify and address potential security vulnerabilities.
	How do you manage and monitor third-party vendors and service providers that have access to customer data?	At this time, there are no third-party vendors with access to customer data, but if this ever changes in the future we would engage in a vendor risk management program that would include due diligence checks, contract reviews, and regular monitoring and assessment of third-party vendors and service providers.
Data Protection and Privacy	Do you have a data retention and destruction policy?	Yes, we have a data retention and destruction policy that outlines our procedures for retaining and securely disposing of customer data.
	How do you protect against data exfiltration and data loss?	We have implemented data loss prevention (DLP) controls and encryption to protect against data exfiltration and data loss.
	What controls do you have in place to prevent unauthorized modifications to customer data?	We have access controls and auditing mechanisms in place to prevent unauthorized modifications to customer data.
	How do you ensure that customer data is not disclosed to unauthorized parties or used for unauthorized purposes?	We have implemented access controls, encryption, and monitoring to ensure that customer data is not disclosed to unauthorized parties or used for unauthorized purposes.
	How do you handle requests from customers for access to or deletion of their data?	We have a documented process for handling customer requests for access to or deletion of their data. Customers submit requests via email.

FAXcentric Security FAQ

Category	*Question*	*Response*
Employee Training and Awareness	How do you ensure that your employees are trained and aware of your security policies and procedures?	We provide regular security training to our employees, including new hire training and ongoing training on an annual basis. Our training covers topics such as data protection, access controls, incident response, and compliance.
	How often do you conduct security awareness training for your employees?	We conduct security awareness training for our employees on an annual basis, and we also provide additional training as needed for specific topics or risks.
Risk Management	Do you perform regular risk assessments to identify potential security threats and vulnerabilities?	Yes, we perform regular risk assessments to identify potential security threats and vulnerabilities. Our risk assessments are conducted on an annual basis, and we also perform additional assessments as needed in response to specific risks or changes in our environment.
	How do you address identified security risks and vulnerabilities?	We have a documented process for addressing identified security risks and vulnerabilities. Our process includes prioritizing risks based on severity, developing mitigation plans, and tracking progress towards remediation.
IT Infrastructure and Service Availability	How do you ensure the confidentiality and integrity of data during transmission?	We use industry-standard encryption protocols to ensure the confidentiality and integrity of data during transmission. Our encryption protocols include TLS and SSL.
	How do you ensure the availability and reliability of your fax service?	We have geo-redundant systems and failover mechanisms in place to ensure the availability and reliability of our fax service. We also perform regular load testing and capacity planning to ensure that our systems can handle expected traffic.
	How do you handle system and service interruptions or outages?	We have a documented incident response plan that outlines our procedures for handling system and service interruptions or outages. Our plan includes procedures for communication with customers and stakeholders, escalation, and restoration of services.
	How do you ensure the security of your IT infrastructure and applications?	We have a layered security approach that includes access controls, network segmentation, intrusion detection and prevention, and regular security testing and monitoring.
	How do you protect against unauthorized access to your IT systems and networks?	We use a combination of access controls, firewalls, and intrusion detection and prevention systems to protect against unauthorized access to our IT systems and networks. We also perform regular vulnerability assessments and penetration testing to identify potential security gaps.
Continuous Improvement	How do you ensure that your security controls are effective and meet industry standards?	We perform regular audits and assessments of our security controls to ensure that they are effective and meet industry standards. We actively work to stay current on best practices and emerging threats.