

Shared Responsibility Model

The security, availability, processing integrity, privacy, and confidentiality of the SPARK platform is built upon a shared responsibility model driven by a partnership between our team at Ignify Technologies, Inc, our customers, and our key vendors. While we, along with these vendors, take on many of the operational burdens inherent in a keeping a state-of-the-art technology platform secure, available, and resilient against disasters, our customer and their teams carry the accountability for who can access their dedicated SPARK environment, what information is captured there, and ensuring that it is accessed responsibly.

To help provide clarity in the shared responsibility model, we have provided an in-depth view of key areas within the SPARK environment

Physical Security

	IGNIFY	CUSTOMER	CLOUD PROVIDER
Implementing physical security controls to protect the data center and server infrastructure			✓

Infrastructure Security

	IGNIFY	CUSTOMER	CLOUD PROVIDER
Hardening the hypervisor (Host OS)			✓
Hardening the operating system (Guest OS)	✓		

Network Security

	IGNIFY	CUSTOMER	CLOUD PROVIDER
Implementing host-based firewalls	✓		
Implementing host-based intrusion detection system	✓		
Implementing host-based file integrity manager	✓		
Implementing host-based anti-virus	✓		
Conducting external network vulnerability scans	✓		
Conducting internal network vulnerability scans	✓		

Application Security

	IGNIFY	CUSTOMER	CLOUD PROVIDER
Securely designing and developing software	✓		
Securely host the SPARK application platform	✓		
Completing static code analysis for the SPARK platform	✓		
Conducting dynamic application scans for the SPARK platform	✓		
Responsible for providing application and product support	✓		

Data Security

	IGNIFY	CUSTOMER	CLOUD PROVIDER
Ownership of data stored in the SPARK platform		✓	
Administrator of data stored in the SPARK platform		✓	
Implementing encryption of data in motion and at rest	✓		✓
Protecting data in the databases	✓		
Secure deletion of data in the databases - during term of contract		✓	
Secure deletion of data in the databases - at contract termination	✓		
Defining records retention standards for SPARK platform		✓	
Enforcing records retention standards for SPARK platform		✓	
Implementing data loss prevention controls in the Ignify Technologies environment	✓		
Managing encryption keys for the SPARK platform	✓		
Responsible for responding to eDiscovery requests that include the SPARK platform		✓	

User Security

	IGNIFY	CUSTOMER	CLOUD PROVIDER
Requesting user access to the SPARK platform		✓	
Provisioning administrator level accounts to the SPARK platform	✓		
Provisioning non-administrator user accounts to the SPARK platform		✓	
Conduct periodic reviews of Ignify administrator accounts in the SPARK platform	✓		
Conducting periodic reviews of user access to the infrastructure of the SPARK platform	✓		
Conducting periodic reviews of user access to the client environment of the SPARK platform		✓	
User provisioning and de-provisioning in client environment of the SPARK platform		✓	
De-provisioning of client SPARK environment and users upon termination of contract	✓		
Defining and requesting password complexity and 2FA requirements in client SPARK environment.		✓	
Configuring password requirements in client SPARK environment.	✓		
Managing encryption keys for the SPARK platform	✓		✓

Integration Security

	IGNIFY	CUSTOMER	CLOUD PROVIDER
Responsible for setting up external integrations	✓		
Responsible for managing relationship with integration partners		✓	
Provisioning SPARK subdomains/environments for clients	✓		
API Key creation/ management		✓	
Integrating SPARK platform with Banking systems	✓	✓	

Resiliency

	IGNIFY	CUSTOMER	CLOUD PROVIDER
Responsible for detecting security events in the SPARK environment	✓		
Responsible to respond to infrastructure security incidents	✓		
Responsible to respond to application security incidents in the client SPARK environment		✓	
Implementing backup strategy for the SPARK platform	✓		
Implementing disaster recovery and high availability for the SPARK platform	✓		

Privacy and Data Protection

	IGNIFY	CUSTOMER	CLOUD PROVIDER
Compliance with CCPA and state data protection laws		✓	
Responding to consumer privacy rights requests		✓	

Compliance

	IGNIFY	CUSTOMER	CLOUD PROVIDER
Responsible for attesting the SPARK environment to SOC 2 standards	✓		
Responsible for delivering an annual security due diligence package	✓		
Responsible for conducting an annual penetration test	✓		
Responsible for	✓		