MOTOROLA SOLUTIONS

SaaS Shared Responsibility Model

The purpose of this document is to raise awareness of the shared responsibilities around security and compliance between Motorola Solutions Inc. (MSI) and our customers, as it relates to Software as a Service (SaaS) cloud-based solutions. SaaS solutions bring many advantages to our customers, including easier deployments, lower overhead, opportunity for cost savings, and potentially better security as compared to on-premises solutions.

Below are explanations of the eight categories called out in the shared responsibility graphic. The graphic illustrates which categories are the responsibility of the customer, the responsibility of MSI, or are shared between both the customer and MSI. Ultimately, our goal is to better inform our customers to maximize the utility and security of our suite of SaaS solutions.

MSI SaaS solutions are hosted within well established and trusted Cloud Service Providers (CSP) for the Platform (PaaS) and Infrastructure as a Service (IaaS) layers. The combination of MSI and CSP services provides a comprehensive set of both physical and information security controls intended to support our customers' mission critical and business critical needs.

Responsibility	**On-Premises Solutions**	**Software as a Service (SaaS)**
Data classification and accountability	Customer	Customer
Governance of customer policies	Customer	Customer
Proper configuration of the application	Customer	Customer
Identity and access management	Customer	Shared
Endpoint protection	Customer	Shared
Application level controls	Customer	MSI
Platform security	Customer	MSI
Infrastructure security	Customer	MSI

Customer Responsibilities

Each section below provides further details on the responsibilities depicted on the above chart.

Data classification and accountability

Customers are responsible for classifying the data they upload, store, and process, and also ensuring any authorized personnel that access the data are adequately trained around the protection of the customer's data. Customers are responsible for the accuracy of the data entered, and how they share data with third parties. Customers are also responsible for compliance with any applicable laws, regulations or standards that affect the customer, its users, and their devices.

Governance of customer policies

Customers have the responsibility to ensure they have proper cybersecurity and data protection policies in place and to monitor compliance with such policies.

Proper configuration of the application

Customers are responsible for properly configuring SaaS applications to ensure adherence to their specific security and compliance needs. For example:

- Protection of user passwords
- Proper user account management within the MSI provided application suite for their users

Shared Responsibilities

Identity and access management

Motorola Solutions will provide the customer with an application to provision and deprovision users, manage their access entitlements, and audit their actions.

Customers have a responsibility to ensure that they only give their authorized employees the proper access, regularly conduct audits on their entitlements and actions, and deprovision their employees when they should no longer have access.

Endpoint protection

Customers have a responsibility to ensure all customer owned and managed systems accessing the SaaS service are managed and maintained to a high standard of security. Depending on the offering, MSI may provide the capabilities for our customers to manage endpoint devices.

MSI Responsibilities

Application level controls

For SaaS offerings, MSI provides the application suite, along with the controls that accompany it. MSI creates SaaS applications utilizing industry best practices and provides patching and maintenance of the applications as needed.

Trained professionals provide 24/7 security monitoring for the application suite and supporting elements of the cloud service. MSI also provides the customer with capabilities and guidance for access control to the SaaS applications.

Platform security

For SaaS offerings, MSI provides complete 'Platform security' for all operating systems (OSs) used within the solution, including the services and controls that accompany it. For example:

- OS Configuration and Hardening
- OS Security Patching
- Server Security, including Anti-Virus and Anti-Malware capabilities with Security Log Monitoring

Infrastructure security

For SaaS offerings, MSI and the Cloud Service Provider for the PaaS and IaaS layers provide the complete 'Infrastructure security' for all hardware within the solution, along with the services and controls that accompany it to protect the full lifecycle of customer data in our control.