Cybersecurity Policy Waiver

Request Date: _____ Request By: _____

For Company: _____on SAAS Platform: ☐ eMRO ☐ eMobility ☐ Trax

☐ Permanent Waiver ☐ Temporary Waiver _____ to _____

Disclaimer

TRAX follows the AWS Security Best Practices. AWS services were designed with the assumption that certain policies, procedures, and controls are implemented by its customers to comply with SSAE16 SOC Audit Standards. In certain situations, the application of specific policies, procedures, and controls by the customer is necessary to achieve certain control objectives in accordance with SSAE 16. Below are those additional policies, procedures, and controls customers may need to implement in order to satisfy the control objectives for customers' specific use case that are requested to be waived.

AWS Best Practices & User Entity Complementary Controls to be waived:

Select 1 or more controls to be waived. It is not required for you to select all, just all that apply to your use case.

	TRAX RESPONSIBILITY as Per AWS Best Practices	Customer Feature/Service Being Waived
Secure Data Handling		
☐	Customers should use encrypted (TLS/SSL) connections for all of their interactions with AWS. Best practices include the use of TLS 1.2 with updated ciphers suites. Old or outdated cipher suites are often vulnerable to attacks. If you use them, the attacker may intercept or modify data in transit.	By waiving this control the company mentioned above would **not** like SSL/TLS configuration or would like to modify a set list of known secure ciphers for any of the connections on the platform selected above.
☐	Customers should appropriately configure and manage usage and implementation of available encryption options to meet customer requirements.	By waiving this control the company mentioned above requires encryption of but not limited to (Volume, Instance, Bucket or FTP) to be **disabled** on the platform selected above.
Cloud Networking Best Practices		
☐	Using Network Access Control Lists (NACLs) that allow stateless management of IP traffic. NACLs are agnostic of TCP and UDP sessions, but they allow granular control over IP protocols (for example GRE, IPSec ESP, ICMP), as well as control on a per-source/destination IP address and port for TCP and UDP. NACLs work in conjunction with security groups, and can allow or deny traffic even before it reaches the security group.	By waiving this control the company mentioned above requires IP Filtering to be **disabled** and allow **Public Access** on the platform selected above.
☐	Use IPSec or AWS Direct Connect for trusted connections to other sites. Use Virtual Gateway (VGW) where Amazon VPC-based resources require remote network connectivity.	By waiving this control the company mentioned above does **not** require direct VPN or AWS Direct connect access to instances or services hosted on AWS for the platform selected above.

_____

Authorized Signature **Date**

Customer hereby indicates it's aware of and approves this request to bypass standards in use by TRAX in safeguarding systems & data.
Customer hereby releases TRAX of any responsibility for any security breaches or network outages that may occur as a result of this waiver.

Contact us

TRAX Offices in United States, United Kingdom, Japan, Saudi Arabia
U.S. HEADQUARTERS 2601 S. BAYSHORE DR, SUITE 500, COCONUT GROVE, FL 33133

www.emro.com