Note: This is a Public document, however it will be considered/ handled as confidential document after filling it with customer information.

Customer/Company Name		**Date**	dd/mm/yyyy
Reference Number	AAA/COMP-ver-ddmmyy	**Request Type**	New/Update

Company/Organization Name	
Technical Contact (Name, Position, Mobile)	
Telephone/e-mail	
Data Center Location	

Servers Information

Server #	**To be filled by Customer**		**To be filled by Data Center Team**	
	Package (Lite, Prof, Ent, Rk)	**Usage Type (Web, Email, Database, App)**	**Private IP**	**Public IP**
Server #1 *[Name]*				
Server #2 *[Name]*				
Server #3 *[Name]*				
Server #4 *[Name]*				
Server #5 *[Name]*				
Server #6 *[Name]*				

Security Policy*

Customer MUST fill-in a table for every server – (add/remove rows as required)

Existing Policy

Source IP	Destination IP	Dest. Port	Protocol (UDP/TCP)	Action (Permit/Deny)	Remarks
Any	*<Server IP>*	*Any*	*Any*	*Deny*	*Default Inbound: Deny All*
<Server IP>	*Any*	*Any*	*Any*	*Permit*	*Default Outbound: Permit all*

ADD – Policies to be added

Source IP	Destination IP	Dest. Port	Protocol (UDP/TCP)	Action (Permit/Deny)	Remarks

REMOVE – Policies to be removed

Source IP	Destination IP	Dest. Port	Protocol (UDP/TCP)	Action (Permit/Deny)	Remarks

Disclaimer

Although Etisalat takes all care to protect the Customer's hosted server(s), this policy does not represent by any means a guarantee against Customer server(s) being compromised. Etisalat's sole role is limited to implementing the above *stated security policy in accordance with the undertaking and responsibility of the Customer.*

*Conditions of Service:

- A security policy is implemented to all Etisalat customers.
- Customers subscribing to firewall service have the option to update the above policy as per their requirements.
- Customers subscribing to lite package (without firewall upgrade) are limited to a default security policy unless they upgrade their service package.
- The latest policy supplied by the customer in case of an update shall supersede all previous policies.
- In case of emergency/assistance, customer may contact Data Center Support team for follow-up on toll free number 8004181 (within UAE) or +971 4 8004181 (overseas customer).
- Security policy form to be filled by customer, should be mailed on support@dc.etisalat.ae for implementation you may log ticket in support portal (https://managedservices.etisalat.ae). To follow up you can check the status in the same ticket.

Policy Examples

Default Policy

Source IP	Destination IP	Dest. Port	Protocol (UDP/TCP)	Action (Permit/Deny)	Remarks
Any	<Server IP>	80	TCP	Permit	HTTP
Any	<Server IP>	443	TCP	Permit	HTTPS
Any	<Server IP>	20	TCP	Permit	FTP Data
Any	<Server IP>	21	TCP	Permit	FTP Control
Any	***<Server IP>***	***Any***	***Any***	***Deny***	***Default Inbound: Deny All***
<Server IP>	***Any***	***Any***	***Any***	***Permit***	***Default Outbound: Permit all***

Commonly Used Policies

Source IP	Destination IP	Dest. Port	Protocol (UDP/TCP)	Action (Permit/Deny)	Remarks
Any	<Server IP>	80	TCP	Permit	**Web:** HTTP
Any	<Server IP>	443	TCP	Permit	**Web:** HTTPS
Any	<Server IP>	25	TCP	Permit	**Email:** SMTP
Any	<Server IP>	110	TCP	Permit	**Email:** POP3
Any	<Server IP>	1433	TCP	Permit	**Database:** Microsoft SQL server
Any	<Server IP>	20	TCP	Permit	**Remote Access:** FTP Data
Any	<Server IP>	21	TCP	Permit	**Remote Access:** FTP Control
Any	<Server IP>	22	TCP	Permit	**Remote Access:** SSH
Any	<Server IP>	23	TCP	Permit	**Remote Access:** Telnet
Any	<Server IP>	5631	TCP	Permit	**Remote Access:** PC ANYWhere
Any	<Server IP>	3389	TCP	Permit	**Remote Access:** Microsoft Terminal Services
Any	***<Server IP>***	***Any***	***Any***	***Deny***	***Default Inbound: Deny All***
<Server IP>	***Any***	***Any***	***Any***	***Permit***	***Default Outbound: Permit all***

Definitions

Source IP	IP Address of the source where the traffic is coming from (usually “any”)
Destination IP	IP Address of the destination where the traffic is going to
Destination Port	Port number of the destination where the traffic is going to
Protocol:	TCP/IP Packet Type: UDP / TCP / ICMP
Action	Whether the traffic should be permitted or denied