REGULATORY PROCEDURES

INTERNET OF THINGS (IoT)

Issue Date: 06 March 2019

tra.gov.ae

ص.ب. 26662، أبوظبــي، الإمــارات العربيــة المتحــدة   هاتـف   9999 626 2 971+ T
PO Box 26662, Abu Dhabi, United Arab Emirates   فاكس   8229 611 2 971+ F

Federal Authority | هيئـة إتحاديـة

IoT Regulatory Procedures, Version 1.

CONTENTS

1. Scope

1.1. This Regulatory Procedure is issued in conjunction with the TRA's IoT Regulatory Policy.

1.2. For definitions of terms used in this Procedure, refer to TRA's IoT Regulatory Policy.

1.3. This Regulatory Procedure covers the procedure for registration for an IoT Service; including M2M Services[1].

1.4. With advances in IoT development both globally and within the UAE, the TRA may update this Procedure and its associated Regulatory Policy on an as-needed basis.

2. Process for Registration of an IoT Service

2.1. Submission Procedure

2.1.1. An IoT service registration request may be submitted as soon as the IoT Service Provider has the information necessary to complete IoT Service Registration Request Form.

2.1.2. The IoT Service provider shall deliver to the TRA a completed IoT Service Registration Request Form and a covering letter.

2.1.3. Upon receipt of an IoT service registration request, the TRA may require the IoT service provider to submit additional information as determined by the TRA, in its discretion, to be necessary to review the request.

2.1.4. The TRA shall determine, at its discretion, whether to accept or reject the request submission.

2.2. Review Procedure

2.2.1. Upon receipt of an accepted IoT Service registration request, the TRA shall review the request and if required transfer the request to the IoT Advisory committee.

---

[1] As defined in the IoT Regulatory Policy

2.2.2. The IoT Advisory Committee shall provide recommendations on service conditions, if requested, for the IoT service registration request.

2.2.3. The TRA shall notify the IoT service provider with the decision regarding the IoT service registration request within (35) working days from the date of receipt of the request.

3. Compliance with Concurrent Obligations

3.1. It is the responsibility of the relevant Licensee and IoT Service Providers to ensure that before any IoT Service is introduced, it is in compliance with the TRA's entire Regulatory Framework as well as any conditions imposed by any other competent authority.

3.2. Under no circumstances shall an approval with respect to this Regulatory Procedure be construed as a waiver or excusal of any other relevant conditions or obligations.

4. Effective Date and Publication

This Regulatory Procedure shall take effect on the date of issue.

5. A List of Annexes

- Annex 1 – Service Registration Request Form
- Annex 2 – Guide for processing the Service Registration Request Form

Annex I – Service Registration Request Form

Service Registration Request Form (Version 1.0)	
1. Name of the company	
2. Company registration details	
3. Details of the company's ownership	
4. Details of the company contact person	
Name	
Designation	
Address	
Phone	
Fax	
Email	
5. Date of submission	
6. Name of the IoT service	
7. Industry vertical(s) where the IoT service would be used (e.g. healthcare, utilities etc.)	
8. What are the main use cases of the IoT service?	
9. Has the company provided this service in other countries? If yes, please provide details e.g. website, product/ service documentation etc.	
10. Please provide a detailed description of the IoT service including functionality and architecture.	
11. What is the target market for the service e.g. individuals, enterprises and/ or the government?	
12. Please provide the network connection diagram i.e. how will the devices/ equipment connect to the telecommunication network.	
13. What device(s) will be used for provisioning of the service? Do these devices have RTTE approval? If yes, please provide details of TRA RTTE approval.	
14. What is the reliability level of the service (in terms of failure rate)?	

15. What customer/consumer data will be collected in provisioning of the service?
16. How do these data sets get classified based on the classification indicated in the TRA IoT Regulatory Policy? (Secret, Sensitive, Confidential, Open)
17. Where will these data sets be stored? (In Country, Out of Country, Both)
18. Please indicate names of all the countries in case answer to the previous question is 'Out of Country'.
19. Where will these data sets get processed? (In Country, Out of Country, Both)
20. Please indicate names of all the countries in case answer to the previous question is 'Out of Country'.
21. What can be the extent of direct adverse impact on the user(s) in case of malfunctioning of the service?
22. What can be the extent of adverse impact on public safety/ convenience through disruption of public services in case of malfunctioning of the service?
23. Please indicate the information that will be shared with the user(s) towards informing them about various aspects of the service provisioning.

Annex 2 – Guide for processing the Service Registration Request Form

Form Item	Guidance
7. Industry vertical where the service belongs (e.g. healthcare, utilities etc.)	Services belonging to critical industry verticals such as healthcare, utilities, transportation etc. will have higher probability to be classified as Mission Critical *(refer to definition of Mission Criticality).* If the service can cause serious injury or death to even one individual, it will be Mission Critical.
13. What device(s) will be used for provisioning of the service?	This is not an input into assessment of Mission Criticality, however it is a good checkpoint to ensure that appropriate type approval has been received on the devices to be used in adherence to stipulations indicated within the IoT Regulatory Policy.
16. How do these data sets get classified based on the classification indicated in the TRA IoT Regulatory Policy? (Secret, Sensitive, Confidential, Open)	This is not an input into assessment of Mission Criticality, however it is a good checkpoint to ensure alignment between the type of data sets being used, their classification and their storage location, to ensure adherence to stipulations indicated within the IoT Regulatory Policy.
17. Where will these data sets be stored? (In Country, Out of Country, Both)	This is not an input into assessment of Mission Criticality, however it is a good checkpoint to ensure alignment between the type of data sets being used, their classification and their storage location, to ensure adherence to stipulations indicated within the IoT Regulatory Policy.
18. Please indicate names of all the countries in case answer to the previous question is 'Out of Country'.	It should be checked if the names of the countries indicated adhere to the stipulations of the IoT Regulatory Policy.
19. Where will these data sets get processed? (In Country, Out of Country, Both)	This is not an input into assessment of Mission Criticality, however it is a good checkpoint to ensure alignment between the type of data sets being used, their classification and their storage location, to ensure adherence to stipulations indicated within the IoT Regulatory Policy.
20. Please indicate names of all the countries in case answer to the previous question is 'Out of Country'.	It should be checked if the names of the countries indicated adhere to the stipulations of the IoT Regulatory Policy.

21. What can be the extent of direct adverse impact on the user(s) in case of malfunctioning of the service?	A high direct adverse impact will increase the probability of the service being classified as Mission Critical. If the service can cause serious injury or death to even one individual, it will be Mission Critical.
22. What can be the extent of adverse impact on public safety/ convenience through disruption of public services in case of malfunctioning of the service?	A high adverse impact will increase the probability of the service being classified as Mission Critical. If the service can cause inconvenience to >10000 individuals, it will be Mission Critical.
23. Please indicate the information that will be shared with the user(s) towards informing them about various aspects of the service provisioning.	This is not an input into assessment of Mission Criticality, however it is a good checkpoint to ensure that adequate information is being shared with the user(s) as stipulated in the IoT Regulatory Policy.