Reference guide:

IoT service and support

Table of Contents

Finding your way quickly and easily

To get the most value out of your IoT services it is important that KPN IoT supports you 24/7. That is why our team is there for you whenever you need us.

This Reference Guide gives you and your colleagues a single overview of how KPN IoT can assist you operationally. This allows you to find your way quickly and easily in daily practice. For example; How do I contact the IoT Service Desk? How am I notified about scheduled maintenance? When will I receive a Root Cause Analysis?

If you have questions about commercial aspects or new developments for your IoT service, we are also available to assist you. For this you can always contact your KPN account manager and/or customer success manager.

KPN IoT actively updates this document to the latest developments within our service processes. This way you are always up to date of our working methods and what this means for you.

Have a question about our services? Contact the KPN IoT Service Desk

The KPN IoT Service Desk is available 24/7. The desk is staffed by a team of dedicated service agents who can help you in both Dutch and English. They will help you with all your service requests by calling on our various experts at KPN and/or our partners.

KPN IoT Service Desk contact information:

- KPN Service Portal for all your service requests
- e-mail: iotservicedesk@kpn.com
- Telephone: +31(0)88 1200 043

Our IoT Service Desk is 24x7 available.

During office hours

During office hours on Monday through Friday, 8:00 a.m. to 6:00 p.m. CET, we handle all service requests.

Outside office hours

Outside office hours, our stand-by team is available to assist you. This team only handles priority level 1 incidents or situations that need to be escalated to priority level 1. For all other service requests, you can submit a ticket. Please note that these are handled during regular office hours.

Holidays

Our stand-by team is also available during the holidays and will only handle priority level 1 incidents or situations that need to be escalated to priority level 1. This applies to the following holidays: New Year's Day (January 1), King's Day (April 27), Easter Sunday and Easter Monday, Ascension Day, both days of the Pentecost, Christmas day and Boxing Day (December 25 & 26).

4 types of service requests

In order to assist you efficiently and to your satisfaction, KPN bases its support service on the market standard ITIL. KPN IoT has 4 different types of service requests: Incident, Request for Change (RFC), Request for Information (RFI), and Complaint. You can submit these via the [KPN Service Portal]

Incident

Request for Information (RFI)

Request for Change (RFC)

Complaint

Incident

An incident is defined as an unplanned disruption or reduction in quality of service that is currently affecting you. Explainable downtime due to planned maintenance does not constitute an incident.

Initiating an incident ticket

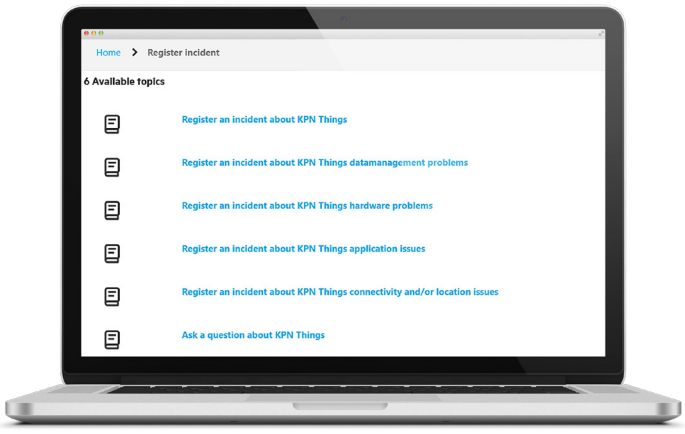
Within the KPN Service Portal, click on “Report Incident” (Register Incident). (This can be done either via the ‘tiles’ or via the vertical menu on the left side of the page).

1. Select a description that best describes your incident
You will see a list of options relevant to your portfolio.

Complete contact information

It is important that you enter your contact information as completely as possible. The easier it is for us to contact you, the faster we can work together to resolve your incident.

Select the option that best fits your specific incident by scrolling or using a search bar at the top right of the page. For example: M2M (Machine to Machine), Things, Lora or DSH (Data Services Hub).



2. Answer all questions
It is important that you enter as much information as possible in the incident ticket so that we can provide you with the best possible service.

3. Click on ‘Submit’
Once your ticket has been successfully submitted, you will see a confirmation, including your ticket number. You (and any additional submitters you added) will also receive an e-mail confirmation of your report.

Priority levels

Depending on the consequences for the service, the incident is rated on a priority scale from 3 (Low) to 1 (High). The greater the impact and urgency, the higher the priority. Impact and urgency are determined by several variables that may be situation-specific, such as the number of connections and/or devices affected, and the impact on societal, financial, or security aspects. The agreed upon recovery time depends on the priority allocated. The higher the priority, the faster the incident must be addressed and resolved.

Call Servicedesk in case of P1

Every incident starts at priority level 3 by default. However, if an incident calls for a higher priority (e.g. level 1), we want to get in touch with you immediately so we can help you as quickly as possible. Therefore, in addition to reporting a ticket, you should also contact the IoT Service Desk by telephone. This way of working applies both within and outside office hours.

1. **Priority Level 1 (P1)**
Unforeseen unavailability of a managed service/customer production environment as a result of a disruption with a serious impact and high urgency.

2. **Priority Level 2 (P2)**
Important components or functions of the service are unavailable. This means that your service has been severely disrupted or impaired, resulting in severely reduced quality.

3. **Priority Level 3 (P3)**
Your IoT service is usable, but partially disrupted or impaired.

The table below specifies the recovery times for each priority level. If you find that the impact or urgency changes during the incident, the priority level may be revised. In this case, contact the IoT Service Desk via the ticket and preferably also by phone. If you wish to raise the priority to priority level 1, you must always contact the IoT Service Desk by phone.

	Recovery time	Servicewindow	Contact medium	Maximum initial response time
P1	< 8 hours	24/7	Ticket and telephone	Immediate when you call the Servicedesk in case of P1
P2	< 16 office hours	Office hours on business days (Monday through Friday, 8:00 a.m. to 6:00 p.m. CET).	Ticket	< 2 hours on business days during office hours (Monday through Friday, 8:00 a.m. to 6:00 p.m. CET).
P3	< 5 business days	Office hours on business days (Monday through Friday, 8:00 a.m. to 6:00 p.m. CET).	Ticket	

Contact with KPN during an incident

KPN takes full ownership and responsibility for solving issues and will do everything in its power to end the disruption. Our goal is to resolve the incident as quickly as possible with a permanent solution or, if that is not possible, a workaround.

We confirm receipt of the ticket via an automated e-mail. An IoT Service Desk agent will review the ticket and start the investigation. For a P3 or P2 incident the agent will contact you via the ticket and/or by telephone within 2 hours. Of course you can always call the Servicedesk within the 2 hours if you want to talk to KPN directly. In case of a P1 incident you must always call the Servicedesk so we can start immediately with our support.

To successfully resolve an incident in a timely manner, cooperation is key. To resolve the incident we may need your help in answering questions and/or a troubleshooting together. When, as a result of the investigation, the cause of the incident is known we will solve the incident.

We want to highlight two situations within incident management:

Issues at roaming partners

In case of an issue at a roaming partner, KPN also takes full ownership and responsibility for solving the roaming issue. We will do everything in our power to solve roaming related issues. The cooperation of the roaming partner(s) play a crucial role in the resolution of a roaming incident. As there are no SLA agreements regarding recovery times within the international roaming landscape we cannot always guarantee our resolution times.

Although we cannot guarantee resolution times due to the lack of SLAs with roaming operators we still work with the above mentioned priority levels (P1 / P2 / P3). The higher the priority, the faster the incident must be addressed and resolved.

Issues in customer domain

In case the analyses shows the cause of the incident lies in your domain we will also work together with you to solve the incident. Cooperation between KPN and your team is important to solve the incident as soon as possible.

Raising the priority

Based on impact and urgency the priority of an incident can be raised to a higher level. This can be at your or KPN's initiative and is always based on consultation via the ticket and/or by telephone.
To help you as quickly as possible always contact the IoT Service Desk by telephone if you want to increase the priority of a ticket.

Closing an incident

An incident is closed once the effects of the disruption have been eliminated. This may be because the root cause has been resolved or a workaround has been implemented. When closing the ticket, as much detail as possible is provided about the cause and resolution of the incident so that you can inform your own stakeholders and/or customers.

To ensure that the incident has been resolved to your satisfaction, we will check with you. If you have not been able to respond after 2 working days, you will receive a reminder. After 2 working days we will ask you again for confirmation. If you have not been able to respond by then, we will close the ticket.
If the incident persists or recurs, you can reopen the ticket within 5 business days or submit a new ticket after the fifth business day.

After resolving an incident, there may be a follow-up in some cases. A follow up can be after a P1 incident or a problem analysis or a Request for Information when the incident is closed:

Follow up after a P1 incident

The impact and urgency of a Priority Level 1 incident requires further actions after the incident has been resolved.
Per default, we approach the aftercare of a P1 incident in three steps. First, when closing the ticket, we will share as much detail as possible about the cause and resolution in the ticket itself. Second, we supply you with a Reason For Outage (RFO) within 3 working days. The RFO is a formal document with a short sum up of the cause of the incident, the impact and what has been done to solve the disruption. This document is suitable for sharing with your stakeholders. Finally, we will supply you with a Root Cause Analysis (RCA) within 10 to 20 working days. The RCA shows the outcome of a more thorough investigation on what caused the disruption, the timeline and actions taken during the incident, and mitigating actions that prevent the disruption from happening again.

Problem management

In some cases, at KPN IoT we see opportunities to prevent incidents in the future, resulting in a problem analysis being initiated. See the section Problem management within KPN for more information.

Request for Information (RFI)

Sometimes you can have questions after an incident has been closed (even though the impact has been removed). We would also be happy to assist you. In this situation, submit a Request for Information with reference to the incident ticket. Please see the chapter Request for Information (RFI).

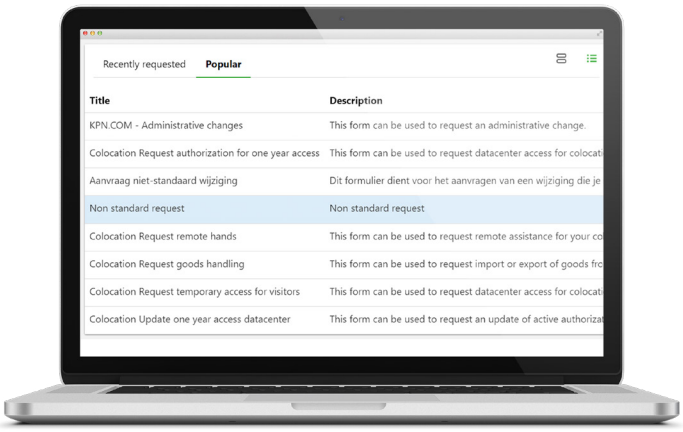
Request for Change (RFC)

A Request for Change (RFC) is defined as any addition or modification to, or removal of, your service. For example, a request for (or change to) an APN, a communication plan, or a rate plan.

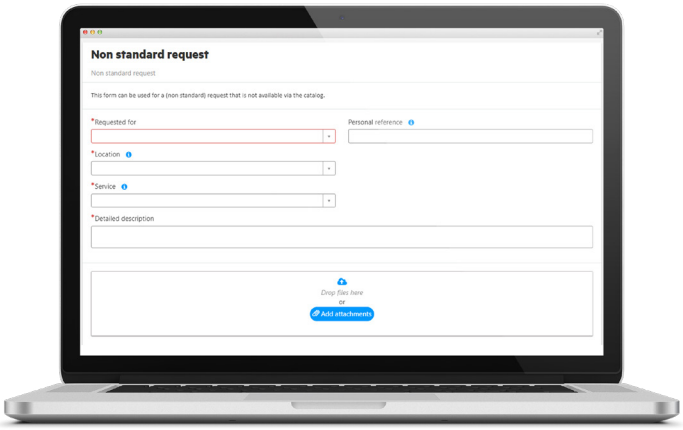
Initiating an RFC ticket

For you as a KPN IoT customer, there are two options: “Standard Request” and “Non-Standard Request”. When we offer your type of change as standard, you select it. Additionally, you may choose “Non-Standard Request” if we do not (yet) offer your exact improvement as standard.

Please note. Other options within the selection menu do not concern you as an IoT customer.



Select ‘Non-standard request’; the following window will appear:



It is important that you enter as much information as possible in the incident ticket so that we can provide you with the best possible service. Also add any attachments in the box provided.

Click on ‘Submit’

Once your request has been successfully submitted, you will see a confirmation, including your ticket number. You will then get an e-mail confirming your request.

Contact with KPN during an RFC

KPN is committed to providing you with the best possible support during your Request for Change. An IoT Service Desk employee will contact you within 2 hours, the maximum initial response time. The standard lead time for an RFC is a maximum of 5 working days. However, an RFC can also result in a project such as redesign, further investigation or business development which in general take more time. In this case KPN IoT will assess the request with you in terms of feasibility, alternative options, and potential costs. KPN IoT will communicate with you via the ticket and/or by phone about the status of the request and will contact you if there are any follow-up questions or if joint consultation is required. The potential costs and lead time of the RFC are dependent on the nature of the request and will be discussed with you.

Closing an RFC

The RFC will be closed once the request has been successfully implemented. If your request is not feasible, it will be closed after consultation with you.

Request for Information (RFI)

A Request for Information (RFI) is defined as any request for information about a service, product, invoice, closed incident, or past incident that does not currently impact your services. For example, if you have a question about the details of your invoice or need more information about a closed incident.

Incident versus RFI

To report an incident or inquire about an ongoing incident, always use the incident ticket (see the Incident section), not an RFI.

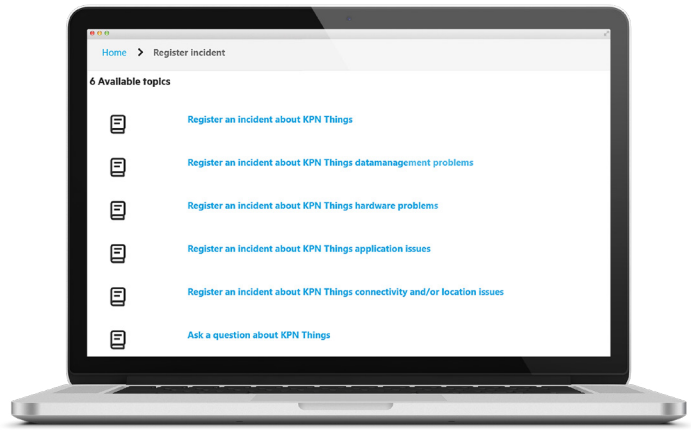
Initiating an RFI ticket

In the KPN Service Portal, click on 'Register incident' to submit an RFI.

1. Select the IoT service your question is about

You will see a list of options relevant to your portfolio.

Select the option that best suits your question: by scrolling or using a search term at the top right of the page. For example: M2M (Machine to Machine), Things, Lora or DSH (Data Services Hub). Then select the option"Ask a question about…".



2. Answer all questions

For us to be able to provide you with the best possible service, please make sure you are as specific as possible when formulating your question and/or explaining your request for assistance. If the RFI is about an invoice or a closed incident, also include the ticket number.

3. Click on 'Submit'

Once your request (RFI) has been successfully submitted, you will see a confirmation screen, including your ticket number. You (and any additional submitters you added) will also receive an e-mail confirmation of your report.

RFI confirmation e-mail

The confirmation e-mail refers to an 'incident'. This is because the current service portal categorizes an RFI under the 'Incident' selection menu. However, your request will not be treated as an incident, but as a Request for Information (RFI).

Contact with KPN during an RFI

KPN is committed to providing you with the best possible RFI support. An IoT Service Desk employee will contact you within 2 hours, the maximum initial response time. If necessary, KPN IoT will communicate with you via the ticket and/or by phone if there are any follow-up questions or if joint consultation is required. The standard lead time for an RFI is a maximum of 5 working days. In exceptional cases the lead time might be longer if an RFI is more complex and needs further investigation and expertise. KPN IoT will always keep you informed about the progress of an RFI.

Closing an RFI

The RFI will be closed once your question has been answered; if KPN cannot provide you with the requested information, an explanation will be provided. We will notify you when the RFI is closed.

Complaint

You can submit a complaint if you are dissatisfied with KPN's procedures, e.g. with the way a process is handled, or with a KPN (IoT) employee.

Initiating a complaint

1. Select the 'Complaint' option

In the KPN Service Portal, click on 'Complaint' to report a complaint. You will find this in the vertical menu on the left side of the screen.

2. Answer all questions

For us to be able to provide you with the best possible service, please make sure you are as specific as possible when formulating your complaint. If the complaint is about a ticket, please state the ticket number.

3. Click on 'Submit'

Once your complaint has been submitted, you will see a confirmation screen, which includes the number associated with your complaint.

Contact with KPN during a complaint

KPN is committed to providing you with the best possible support and to taking action in response to your complaint. KPN IoT will contact you within a business day of receiving your complaint. We will do this via the ticket and/or by telephone to discuss the complaint with you and determine any follow-up action.

Closing a complaint

The complaint will be closed in joint consultation, after which you will also receive a confirmation by e-mail.

Problem management at KPN

A problem is defined as a cause or a possible cause of 1 or more incidents or a risk that may cause incidents in the future. Even after an incident has been resolved, the root cause, or problem, may still persist. KPN monitoring or analysis may also reveal a problem.

Initiating a problem

Problem management focuses on situations where it has become apparent that the root cause of a disruption has not yet been resolved. Problem management also focuses on mitigating or eliminating future risks. KPN IoT may decide to initiate a problem analysis based on this root cause.

Contact with KPN during a problem

At KPN IoT, the problem manager takes the lead in the analysis and resolution of the problem. The problem manager is responsible for issuing customer-specific updates as well as generic updates for several customers at the same time, and also organizes troubleshooting sessions with the customer and other forms of consultation as required.

Closing a problem

A problem is closed when a permanent solution has been implemented. If no permanent solution is available or feasible, actions will be taken to minimize the problem. Depending on the nature of the problem (customer-specific or generic), an appropriate way to finalize and close the problem will be considered.

Escalating

If a ticket is not being handled in the desired way and/or is not expected to be resolved within the specified time frame, it may be escalated to a higher level. The purpose of escalating is to engage people with more expertise or authorizations. The following 3 escalation levels can be implemented 24/7.

A ticket is escalated using the escalation matrix below. The most up-to-date version of the escalation matrix is always available on the IoT Service Portal. **Escalation always starts at level 1: the IoT Service Desk.** If an escalation fails to achieve the desired result, you can escalate to the next level, **Level 2: IoT Team Operations,** and finally to **Level 3: the VP Operations IoT.**

KPN IoT always strives to help you in the best way possible. During escalation, communication between you and KPN as well as actions to be taken will vary depending on the situation. Your contact person for each escalation level will discuss expectations with you. We will also discuss with you when it is appropriate and/or relevant to raise or downgrade the escalation level.

Communication and escalation matrix

Level	KPN role	Name	Phone number
1	IoT Service Desk	Team Member	+31 (0)88 1200 043
2	IoT Team Operations	Team Member	+31 (0)88 1200 000, pin: 1261
3	VP Operations IoT	Richard van der Wel	+31 (0)6 4640 4963

Figure: KPN IoT escalation matrix

Maintenance by KPN and partners

KPN and its partners strive for the highest standards in terms of availability, reliability, and security for the IoT portfolio. Regular planned maintenance is performed to ensure that the services function optimally. Maintenance may be planned or it can take place on an ad-hoc basis. During maintenance, all or part of the service may be unavailable.

Since the IoT chain is largely redundant, in most cases there will be no noticeable impact on your service. In addition, efforts are made to keep the actual interruptions as short as possible. However, if certain maintenance activities on the network will have an impact on your service, we will provide you with as much information as possible.

We aim to give at least ten business days' notice of any work that may impact your service. In exceptional situations, work may need to take place on an ad-hoc basis. This means that it is not possible to announce the maintenance activities at least ten business days in advance. In such cases, KPN IoT will inform you as soon as possible.

Communication from KPN during generic disruptions

A generic disruption is a disruption to a component of the IoT portfolio that affects multiple customers at the same time. In order to keep you informed about the disruption, updates, and progress of the incident in a timely and efficient manner, KPN uses generic communications

Initiating generic communication

KPN initiates generic communication in the following cases:

- When a generic disruption is detected during proactive monitoring by KPN and its partners.
- When 1 or more customer-reported incidents indicate that a generic disruption is in progress.

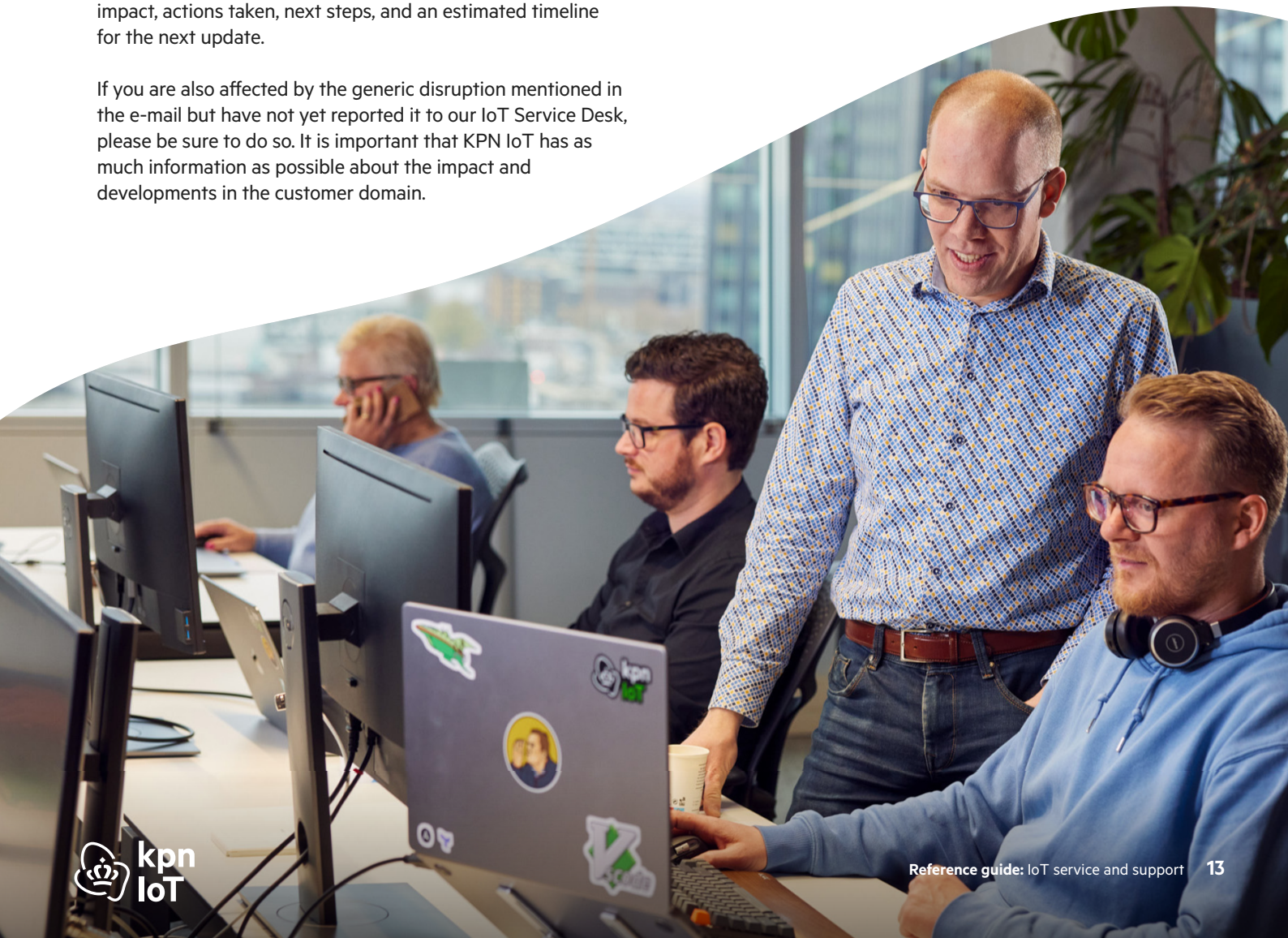
Contact with KPN during a generic disruption

KPN understands that when you and your stakeholders are affected by a generic disruption, you need regular updates that are as detailed as possible. Customers who are affected or potentially affected will be notified by e-mail as soon as possible. These e-mails will include information about the impact, actions taken, next steps, and an estimated timeline for the next update.

If you are also affected by the generic disruption mentioned in the e-mail but have not yet reported it to our IoT Service Desk, please be sure to do so. It is important that KPN IoT has as much information as possible about the impact and developments in the customer domain.

Closing a generic disruption

KPN will inform you by e-mail as soon as the disruption has been resolved. Depending on the type of disruption and its impact, we will notify you of any follow-up steps, such as root cause analysis (for P1 incidents only). If you submitted a ticket to report the disruption, you will also receive notification in the ticket regarding the closure of the disruption.



Managing your profile to contact KPN and stay up to date

In order to be able to submit service requests to the IoT Service Desk and stay up to date on maintenance and generic disruptions, it is important that you and your colleagues have the right permissions.

KPN IoT is currently in the process of migrating to a single environment, the KPN Things Portal, which will be the new go-to place for all your questions and notifications. Until then, we will continue to use 2 environments:

1. **KPN Service Portal** for all your service requests (incidents, RFI, RFC, etc.)
2. **IoT Service Portal** for placing orders and staying up to date with news, maintenance, and general disruptions.

KPN Service Portal

Contacting the IoT Service Desk to report incidents or to request information (RFI) or changes (RFC).

To submit tickets for KPN IoT, you need a profile with the appropriate permissions.

To create a new profile or edit an existing one, please refer to the document 'Manage users for My KPN Business'. You will find this on the IoT Service Portal homepage under 'Shared documents'.

If you have any questions or need assistance in creating or editing a profile, please contact the IoT Service Desk. You can do this by submitting a ticket or by phone.

IoT Service Portal

Placing orders and forecasts, and staying up to date on news, maintenance, and generic disruptions.

To use the features of the IoT Service Portal, you need a profile with the appropriate permissions. To create a new profile or edit an existing one, refer to the document 'User Guide – IoT Service Portal'.
You will find this on the IoT Service Portal homepage under 'Shared documents'.

If you have any questions or need assistance in creating or editing a profile, please contact the IoT Service Desk. You can do this by submitting a ticket or by phone.

Appendix

Definitions

2-2-2 Method	An IoT Service Desk workflow where a reminder is sent after 2 days if there has been no response from the customer. A second reminder is sent after 2 further business days. If there is still no response, the ticket is closed 2 business days after the final reminder. The ticket can be reopened within 5 business days.
Business day	Monday through Friday, excluding national holidays in the Netherlands. National holidays are: New Year's Day (January 1), King's Day (April 27), Easter Sunday and Easter Monday, Ascension Day, both days of the Pentecost, Christmas day and Boxing Day (December 25 & 26).
Complaint	You can submit a complaint if you are dissatisfied with KPN's procedures, e.g. with the way a process is handled, or with a KPN employee.
Contact medium	Method of communication; this may be via a KPN Service Portal and/or by phone.
Escalation	An activity initiated for the purpose of engaging people with more expertise or authorizations. If a ticket is not being handled in the desired way and/or is not expected to be resolved within the specified time frame, the customer may escalate the ticket to a higher level.
Escalation matrix	A matrix comprising 3 escalation levels where in case of an escalation you always start at Level 1: the IoT Service Desk. If an escalation fails to achieve the desired result, you can escalate to the next level, Level 2: IoT Team Operations, and finally to Level 3: the VP Operations IoT.
Explainable downtime	The time during which the service is not available or is only partially available due to planned maintenance or ad-hoc maintenance.
Generic disruption	A disruption to a component of the IoT portfolio that impacts multiple customers, after which generic communications are initiated for those customers.
Incident	An unplanned disruption or reduction in quality of service that is affecting you.
Incident End Time	The time determined by KPN and acknowledged by the customer at which an incident ends, provided that the incident has ended and assuming that the customer cannot withhold acknowledgement of the end of an incident on unreasonable grounds.
Incident Start Time	The time at which the customer notifies KPN that an incident has occurred.
IoT	IoT stands for Internet of Things and is the general name for all devices that are connected to other devices, servers, or other systems (or people).
ITIL	ITIL stands for Information Technology Infrastructure Library. It is a framework of best-practice processes for delivering IT services.
KPN Service Portal	The web portal through which you can report incidents, submit RFIs, RFCs, and complaints, and access further communication regarding these tickets.
Maximum initial response time	The maximum length of time between receiving a service request from a customer and contacting the customer directly either via a written ticket (e-mail) or by phone.

Planned maintenance	The period during which the service is suspended in accordance with the contractual terms and conditions.
Priority level 1 (P1) incident	An incident resulting in the unforeseen unavailability of a managed service/customer production environment as a result of a disruption with a serious impact and high urgency.
Priority level 2 (P2) incident	An incident that results in unavailability of important components or features of the service. This means that your service has been severely disrupted or impaired, resulting in severely reduced quality.
Priority level 3 (P3) incident	An incident where your IoT service is usable but partially disrupted or impaired.
Problem management	The process of identifying problems and minimizing or eliminating the impact of defined problems. A problem is defined as a cause or a possible cause of 1 or more incidents or a risk that may cause incidents in the future.
Recovery time	The time to restore the service, measured from Incident Start Time to Incident End Time for priority level 1 (P1), priority level 2 (P2) and priority level 3 (P3).
Request for Change (RFC)	Any addition or modification to, or removal of, your service. For example, a request for (or change to) an APN, a communication plan, or a rate plan.
Request for Information (RFI)	Any request for information about a service, product, invoice, closed incident, or past incident that does not affect your service at the time of the request.
Root Cause Analysis (RCA)	An analysis that determines the cause of a problem or incident and identifies corrective actions to prevent a recurrence.
Service window	The time window in which the customer receives support in the form of the Incident Management process carried out by KPN. The time window for incidents with priority level 1 (P1) is 24/7. For incidents with priority level 2 (P2) and priority level 3 (P3), a time window of 8:00 a.m. to 6:00 p.m. CET on business days applies.

kpn IoT

AD-20912/11-23/KRE-ENG