Service Handbook

Pod Group Customers

Table of Contents

Document History

Date	Name	Change	Version
October 2021	NOC	Draft Compilation	V 0.1
November 2021	NOC	1st Revision	V 0.2
August 2022	NOC	2nd Revision	V 0.3

Introduction

In July 2021, Giesecke+Devrient (G+D), a global security technology group headquartered in Munich, Germany, acquired Pod Group in order to expand its connectivity business portfolio.

By merging both companies, we intend to create even more efficiency and value for our customers and be able to bring better and more innovative solutions to market. One such change is the new support system providing 24/7 back up to our customers with individual technical support from a dedicated team of experts.

Tickets can be raised through eportal, support widget on Pod IoT Suite or over the phone.

This Service Handbook describes how our Support Services operate, based on ITIL best practices and processes.

This document shall be an appendix to the main Master Agreement established between Pod Customers and Pod Group

Service Operations

The objective of ITIL Service Operations is to ensure that IT services are delivered effectively and efficiently. Service Operations include the fulfilling of user requests, resolving service failures, fixing of problems, as well as carrying out routine operational tasks.

The NOC (Network Operations Center) team is responsible for operating and carrying out the activities and processes required to deliver the services within agreed SLA (Service Level Agreements) that include the following:

- Incident Management – Management of unplanned interruption or degradation in performance of a service. The Incident Management process aims to restore IT services to their defined service levels as quickly as possible

- Request Fulfillment – A request for information, standard change or access to a service

- Problem Management – Proactive and reactive problem management with the objective to prevent problems and incidents, eliminate repeating incidents, and minimize the impact of incidents that cannot be prevented

- Change Management – Enable beneficial changes - impacting or potentially impacting the services - to be made with minimum disruption of the service

- Event Management – Real-Time monitoring of events that occur through the IT infrastructure, connectivity infrastructure and the service layer to allow for normal operation and to detect and escalate exceptional conditions

- User Access Management – Management of providing the right access privileges to the right users

- IT Continuity Management – Ensures minimum agreed Service Levels can be provided, by reducing the risk from disaster events to an acceptable level and planning for the recovery of IT services and connectivity services running through our core.

Pod Group Support Services

How to contact the Service Desk

The Service Desk for this service is operated by our NOC (Network Operations Center) team and operational 24x7x365 i.e. 24 hours a day, 7 days a week, 365 days a year and can be accessed during the support hours specified in your SLA. Any incident requests received with Priority High will be handled as soon as they're acknowledged while the rest of the incidents with lower priorities will be handled during normal office hours.

*Please note the **outside business hours** there is a **specific process** for getting support. Please follow the steps described below.*

During business hours and for low priority incidences:-

The Service Desk is the Single Point of Contact (SPOC) for all customer communication on matters relating to the Operations Support including, but not limited to, incident reporting, registering tickets, related expert technical support and Change Management.

There are three ways to contact NOC:

1. Recommended method: through ePortal https://gdmsps-portal.gi-de.com/ePortal/

   Key users in your organization are able to access the ePortal ticketing platform, can log tickets, interact with the NOC team and follow up incidents from the platform.

   You will receive an email from Service Now with the new credentials. Username will be your email address.

   In case of any issues with receiving the email with your password you can email sm.noc.pod.l1@gi-de.com or call the support lines mentioned below.

   New users can be requested through a Service Request (SRQ).

2. Through the support widget on Pod IoT Suite.

3. For CRITICAL ISSUES that require **immediate** attention **ONLY**, you can call the NOC team using the numbers you can find on our website and by selecting 1-SUPPORT. Regional contact numbers are below:

- UK: +44 (0)1223 850 900

- USA: +1 415 7070 500
- Spain: +34 954 050 200
- Hong Kong: +852 5803 2400
- Mexico: +52 55 5350 2400

Outside business hours (P1 and P2 tickets only)

Out of working hours (weekends and business holidays), our team will concentrate on only P1 and P2 incidents (see the table below), so that we can focus on where support is most needed.
Please open a ticket on SNow (or the eportal) and **also**, it is **mandatory to call us** on any of the phone numbers above. The duty team will evaluate the incident and take appropriate steps to address it. Should the incident not be deemed high priority you will be informed and the ticket will be checked during normal office hours.

If the incident requires immediate action the duty team will initiate the support response.

Impact	Classification
High (P1)	A global problem that severely impacts **all** end-users and the ability to conduct business.
Medium (P2)	A serious issue that involves partial functionality loss, which impairs some or part of the Customer's operations affecting **multiple** end-users. This may include a roaming issue affecting devices roaming in a key region.
Low (P3)	A medium- to low-impact problem that affects an individual or a small number of end-users or involves partial functionality loss which impairs some operations but otherwise allows the Customer to continue to function normally.

Access to ePortal

The Service Desk can only be accessed by the customer's technical and/or support staff who are authorized and registered in the ticketing system.

Our Customers must provide a list of authorized contacts – including the main contact - and may modify this list at any time, provided the NOC team is given notice of the changes in advance. The main contact will be responsible for the authorization of new contacts. All users of Pod IoT Suite have already been authorized and registered in the ticketing system.

Customers also have the ability to add a group email (Distribution List/DL) to the ePortal contact list. Key service users should continue to maintain their own ePortal credentials as account contacts.

The DL access will require two-step authentication. DL users have access to ticket creation and its associated actions (view/update). Change authorization remains the responsibility of our Customers selected key contact and/or the DL only. Change requests submitted by the DL must specify the name of the originator for acceptance. Customers are exclusively responsible for the maintenance of any DL list. Pod and G+D have no ability to monitor or maintain any DL members.

Note that you are **limited to five ePortal contacts** per contract with the exception of existing clients. For existing clients, as mentioned above, we have uploaded all their Pod IoT Suite users as ePortal contacts.

The initial setup is determined during the transition phase of the project. Once the service has gone live, the contact list can be modified by initiating a service request ticket (see section 3.2.2).

The NOC team distinguishes between “normal” contacts and “change management” related contacts. For every contact our Customers must indicate if:

- The contact is authorized to open tickets (ePortal authorization)
- The contact should receive automated emails from the ticketing tool and is able to update tickets by email

Please whitelist the following email address in advance: gdmsps.support@gi-de.com, as you will receive all the planned maintenance and incident notifications from that email address.

Ticket Types

This section outlines the different types of tickets that the NOC team uses to structure customer support requests. All SLAs (Incident, Service Request and Problem Management) are defined under the Service Level Agreement document.

Incident

An incident is an unplanned interruption or degradation of service. The Incident Management process aims to restore the service as quickly as possible, by minimizing the impact on the customer’s service.

Service Request

Service Request is the method for the customer to get standard services, general information, to deliver information or ask questions about the services. A typical Service Request can be related to the IT infrastructure (such as allowing a new IP address on the customer side to access ePortal), questions around the Pod IoT Suite platform, requests for information or user access management.

Problem Management

A problem is the unknown cause (root cause) of one or more incidents. Problem Management seeks to minimize the adverse impact of incidents by preventing incidents from happening. For incidents that have already occurred, Problem Management tries to prevent these incidents from happening again.

The Problem Management process can only be initiated by the NOC team.

The NOC team will create a Problem ticket ,when applicable, based on the diagnosis or solution of a concrete Incident ticket or as a result of the analysis of several incidents.

When a “high” impact Incident ticket is resolved, a Problem ticket is automatically opened for further investigation. When these high impact incidents are resolved, the underlying root cause is analyzed within the Problem Management process and concluded with the Root Cause Analysis (RCA), which is shown to our Customers via a Problem Report. Further steps are then decided based on the outcome.

Ticket Information

The customer must provide as much relevant information as possible to facilitate the immediate start of NOC team activities.

All tickets are logged and tracked in the ePortal Ticketing System, including incidents reported by telephone.

Tickets are identified by a unique ticket number (INCxxx, SRQxxx, PRBxxx, CHGxxx).

Updating Information on Tickets

Open tickets can be updated by our Customers at any time. There are two different ways to submit a ticket update, as follows:

Via ePortal:

- the preferred method is through the “additional info” field in ePortal

NOTE: (GDPR / private sensitive data should not be provided on this field, use “data privacy” fields instead)

Via e-mail (ticket updates only). Preconditions:

- User needs to be included on the authorized contact list

gdmsps.support@gi-de.com address needs to be included as a recipient of the email

- The subject of the email starts with +ticketID+ (the ticket ID between “+” signs)

Ticket Severity Classification

NOC team uses “impact” (refers to the potential impact on delivered services) as the basis for ticket severity classification.

Incident Severity Classification

Incidents can be categorized as “High” (P1), “Medium” (P2) or “Low” (P3) according to the following classification. In the case of an Incident with a “High” impact, we recommend that our Customers open a ticket via ePortal and call the G+D Service Desk / NOC to ensure proper and immediate attention.

Impact	Classification
High (P1)	A global problem that severely impacts all end-users and the ability to conduct business.
Medium (P2)	A serious issue that involves partial functionality loss, which impairs some or part of the Customer’s operations affecting multiple end-users. This may include a roaming issue affecting devices roaming in a key region.
Low (P3)	A medium- to low-impact problem that affects an individual or a small number of end-users or involves partial functionality loss which impairs some operations but otherwise allows the Customer to continue to function normally.

Before creating a ticket our Customers must carry out impact analysis and prioritise any incident into one of the categories listed in the table above.

At its election, the NOC team will make a similar priority designation regarding each incident. Determination of the final impact level is subject to reasonable discussion between the parties.

In the event the parties are unable to agree on the appropriate impact level for an incident, at the election of our Customer, the NOC team shall proceed with the Customer's prioritization. However, the NOC team is entitled to an appropriate adjustment in its favour in the event that after resolution of the incident the priority level requested by our Customers is determined by the NOC team to have been incorrect.

Service Request Severity Classification

Service Requests can only be categorized with impact "Low".

Problem Severity Classification

As stated in section 3.2.3, Problem tickets can only be raised by NOC Team. The severity classification follows the same guidelines as for Incident tickets (section 3.4.1).

Ticket Response

Upon receipt of a ticket, NOC team will:

- Provide an acknowledgement notifying our customer's appropriate representative/s (pre-defined "contacts") by an automated email with a ticket reference and an update on the ticket status if available at that time.
- Provide updates on ticket status
- Request additional information or action needed on our customer's side in order to continue with ticket resolution ("Action required"). In this case, the ticket will show the status "On Hold" and the SLA clock will be stopped until the information has been provided or the required action undertaken by the customer.
- Provide resolution information. Once the ticket is resolved, an automated notification will advise our Customers accordingly.

  Our Customers have (3) days to confirm that the ticket has been resolved. If there is no answer within this time frame the ticket will be automatically closed. Tickets can not be reopened once they are closed.

All the ticket-related information is shown on ePortal. However, depending on certain conditions, the appropriate contacts will receive an automated email notification with ticket updates. The table below lists the various notifications types.

The subject line of these emails is built as follows:

G+D - <customer company name>/<contract ID>/<service type> - <ticket ID> - <ticket impact> - <keyword> - <environment> - <title of the ticket>

Notification (subject keyword)	Description of Notification	Applicable Ticket Types
	Notification is generated when the ticket has been created	INC/SRQ/PRB
UPDATE	Customer or G+D has updated the ticket	INC/SRQ
ACTION REQUIRED	Ticket is pending input or action from Customer. SLA clock is stopped until input is provided or the action executed	INC/SRQ
COMPLETED	Ticket has been resolved	INC/SRQ/PRB
CLOSED	Ticket has been closed	INC/SRQ/PRB
WITHDRAWN	Ticket has been withdrawn (cancelled)	INC/SRQ/PRB

Ticket Resolution and Closure

Incidents will be deemed to have been resolved upon either successful workaround or resolution of the problems identified in the report and/or upon agreement by both parties that the incident was not an incident or that the incident was not a responsibility of Pod Group.

Our Customers shall be deemed to have consented to incident closure unless the NOC team is notified to the contrary within three (3) business days after receipt of email notice from the NOC team that an incident has been resolved. All updates are done via the ePortal or by email.

“Problem reports” are provided as the Root Cause Analysis for all “High” impact incidents.

As a guideline this report will include the following:

- A high level summary of the incident
- An overview of the impact of the incident
- Details of root cause
- Proposed solution

Change Management

A Change is defined as the addition, modification or removal of anything that could affect the Service contracted by the customer.

The objective of the Change Management Process is to guarantee that all changes are applied in a controlled manner with minimum disruption to the service and following agreed processes between our Customers and Pod Group.

Changes may be requested by either party. However, only NOC team can create a Change Request (CHG) ticket. If our Customers require a change the process is initiated via a Service Request. Upon evaluation of this Service Request (SRQ) NOC team will create a Change Request and refer to the SRQ for additional information.

Changes out of scope of the contractual service require further evaluation by Pod Group and might result in additional cost to our Customers. In this case, approval from our Customers is needed to proceed with the Change Request.

Change Classification

G+D Change Management process supports three main change classifications: standard, emergency, and normal.

Standard Changes

A Standard Change is a low risk and low impact change that is pre-defined and pre-approved.

This change type follows a standard operating procedure and does not follow the conventional process flow. The purpose of pre-approved Standard Changes is to speed up the change process in a controlled way.

Emergency Changes

An Emergency Change is the highest priority change type that must be implemented as soon as possible. Emergency Changes may have to be deployed to resolve a major incident or implement a security patch. The aim is to keep emergency changes to a minimum.

Normal Changes

Normal Changes are all changes that require a full change management review by a Change Advisory Board (CAB). A Normal Change can be triggered and rejected by both parties.

Any change that is not a Standard Change or Emergency Change constitutes a Normal Change. The default notice period given before any change implementation start ("lead time") is 5 working days.

Patching

Pod Group takes every precaution to protect customer data and ensure services are up to date with the latest security patches from 3rd party vendors or the Pod Group IT team. Patching is subjected to formal change management procedures in all cases.

New patches are thoroughly tested in staging environments prior to being deployed in either customer pre-production or production environment. Once testing is complete, Pod Group will then schedule a date and time for the patch to be installed on the customer pre-production environments (if applicable). Only after successful testing in the pre-production environment will the patch be applied to the customer production environment.

Maintenance Windows

"Maintenance Window", refers to agreed slots in which Pod Group executes planned (normal) changes that "may" impact the services provided to our customers (refer to section 3.7.1 for additional details on Change Classifications).

Notifications

The NOC team will notify customers about changes impacting the contracted services through a "maintenance window" notification.

NOC team distinguishes here two main scenarios, depending on the impact and risk of the change:

No impact, low risk changes: these are handled as internal tickets and will be performed during regular working hours on the location in which the changes take place. Patching is the perfect example of these kind of changes

1. No impact but high risk changes and changes which do have an impact on the contracted service will be always notified to the affected customers taking into account the lead time included on the SLA

The “maintenance window” notification includes following information:

- Reason for change
- Benefit from the change
- Implementation window
- Outage window, when possible
- Impacted service or use case

Upon completion of change execution, our Customers will be informed via email about its outcome.

Our Customers must also notify Pod Group of any relevant change executed on their side that could have an impact on the services through a Service Request ticket.

Challenges to Change Notifications

In scenarios where, for technical or business reasons, planned changes cannot be accommodated by either party, the change notification must be challenged within 2 business days of being received.

The change may then be rescheduled or a meeting arranged to agree the implementation at mutual consent, except in cases in which the object of the change is a shared component where Pod Group, for security, operational or business related reasons, needs to execute it within a given time schedule.

Service Level Agreement

Please refer to annex 1 for additional SLA details. The ePortal guide is provided along with the contact credentials (sent individually).

Professional Services Escalation Matrix

Level/Role	Name	Phone
Level 0: NOC team	**NOC team**	UK: +44 (0)1223 850 900 USA: +1 415 7070 500 Spain: +34 954 050 200 Hong Kong: +852 5803 2400 Mexico: +52 55 5350 2400
Level 1: Cloud or DC Manager/Engineer Support Team Lead	**EMEA:** Martin Poncelas **APAC:** Sunny Mak **North America:** Milena Isidore Resk **Latam:** Pamela Montes	UK: +44 (0)1223 850 900 USA: +1 415 7070 500 Spain: +34 954 050 200 Hong Kong: +852 5803 2400 Mexico: +52 55 5350 2400

Annexes

Annex 1. Service Level Agreement

Incident SLA Milestones

Milestone	Description	Impact High (P1)	Impact Medium (P2)	Impact Low (P3)
SLA Start date and time - Event start (M0)	The timestamp at which the incident was detected, reported through the Event Management system and documented in the Ticketing System.This only applies for working days with the exception of public holidays.			
Acknowledgement date and time	The maximum time allotted between the point an incident is internally detected to the point the Customer is provided the report of the detected incident or the timeframe within which the Noc team acknowledges receipt of an Incident notification. This only applies for working days with the exception of public holidays.			
Acknowledgment time		Within 1 hour	Within 2 hours	Within 3 hours

Problem SLA Milestones

Milestone	Description	Impact High (P1)	Impact Medium (P2)	Impact Low (P3)
RCA Time	The timeframe within which a root cause analysis (RCA) will be provided. RCA is provided through internal problem management and starts at Event end. **Only for services running through Pod Group core.**			
RCA time		5 d	10 d	15 d

Note: All times are from time of SLA Start Date and Time.

Annex 2. Service Availability

The contracted Managed Services are operated 24 x 7 x 365. For the contracted period, the Service Availability, expressed as a percentage of the total hours during a calendar month, shall be delivered according to contracted service levels and calculated as defined in the SLA. This only applied to Pod Group Services running through its core.

The Service Availability shall be calculated by applying the following formula:

Av = [(TSH – TSD) / TSH)] x 100

Where:

Av = Availability in %, expressed as a two decimal number (i.e. 99.71%, choose availability based on contractual SLA)

TSH = Total Service Hours, which is the number of hours in the reporting period minus the total planned and approved downtime as well as downtime caused by ad hoc emergency changes (expressed in hours using one decimal), e.g. (31 x 24 – 0.5)*

* Example with 31 days per month x 24 hours per day – 0.5 hours (30 minutes) as the approved downtime

TSD = Total Service Downtime, which is the number of hours (expressed as a number with one decimal) in the last reporting period where the service was unavailable.

The service is considered available at any time except when an Incident Ticket with the Impact “High” has been logged and acknowledged in the ticketing system.

Pod Group will use reasonable endeavours to ensure that service uptime is equal to or greater than 99% for any given Invoice Period.

The calculation of the Service Availability excludes all Maintenance Windows, planned outages documented within the change management process and any downtime due to causes not in responsibility of Pod Group such as downtime caused by changes requested or approved by Customer, acts or omissions of the Customer, incidents on 3rd parties, natural disasters or any other Force Majeure.