DAILY AGREED PROCEDURES (DAP) BETWEEN CUSTOMER AND IOTSPOT B.V. PERTAINING TO THE IOTSPOT SERVICE LEVELS

Document version

Version	Author	E-mail address	Date
CONCEPT	Marnix Lankhorst	marnix@iotspot.co	01 March 2018
FINAL	Marnix Lankhorst	marnix@iotspot.co	17 September 2018
FINAL 1.1	Marnix Lankhorst	marnix@iotspot.co	01 December 2018
FINAL 2.0	Marnix Lankhorst	marnix@iotspot.co	01 October 2020
FINAL 2.1	Marnix Lankhorst	marnix@iotspot.co	19 May 2021

Distribution list

Name	Company	E-mail address	Telephone for P1 or P2

Confidentiality

This document contains iotspot confidential information and proprietary information and is solely supplied to allow you to agree upon daily operational procedures in regard to the delivery of iotspot services. This document (including any part thereof) contains business confidential information and may not be disclosed or transferred or shared with persons outside your organisation without prior written consent from a duly authorised iotspot representative. Use of the (content) of this document for other purposes than the intended purpose, could result in an unlawful act.

1 Table of Content

2 Introduction

2.1 Purpose

The Daily Agreed Procedures document (DAP) uniformly records all work agreements with respect to the procedures as agreed between Customer and iotspot pertaining to the Service Levels of iotspot (as defined in section 3). The goal is to have a clear mutual understanding of how the parties interact, to prevent miscommunication thus making the co-operation as efficient and effective as possible.

2.2 Validity and Status

The period in which this DAP is valid is identical to and follows the contract period. In case of contradicting statements between this DAP and the contract, the contract always supersedes the DAP. The DAP is not a contractual document, but it is a formal agreement on how the parties collaborate.

2.3 Updates and Document Ownership

Changes in the DAP are possible, as long as they do not contradict the contract and are accepted and agreed upon by both Customer and iotspot. Proposals for changes in this document are subject to the operational meeting between Customer and iotspot.

The DAP will be reviewed during the operational meeting and, if necessary, will be modified accordingly by iotspot's Service Manager who is also the document owner. Furthermore, any changes to the contract will always result in intermediate reviews of the DAP.

2.4 Operational meeting to assess Service Level and improve procedures

Customer and iotspot regularity assess the Service Level in their operational meeting. The operational meeting is held at minimum once a year with the objective to:

1. Assess the Service Level and agree the number and type of Incidents between parties;
2. Agree to the number of Service Level Credits that iotspot is eligible to Customer; following the Service Level assessment;
3. Review this document and agree to required updates; and
4. Make arrangement for any Service continuation and or extensions.

2.5 Contact Persons

For security reasons, Customer needs to provide iotspot with an e-mail address for Service notifications (a distribution list is recommended) and a list of names and phone numbers of their employees who have been appointed as contacts to the iotspot Service Desk. This detailed contact information is aggregated in Annex A.

2.6 Definition Reference Table

In this DAP, in addition to those terms set out elsewhere in this document, the terms and expressions in Table 1 apply.

Term / Expression	Meaning
“Change”	means an adjustment to the Service that is the Resolution of a Problem.
“Credit (or Service Level Credit)”	means the right of the Customer to use the Service for one day for free, as compensation for an Incident that degraded the Service Level. A Service Level Credit can be capitalised, upon renewal of the contract period and accounts to a price reduction of 1/365 part.
"Emergency Downtime"	means where iotspot is required to suspends the Service in an unforeseen and unplanned fashion, in accordance with iotspot terms and conditions.
"Escalation Management"	means handing over the necessary activities to a higher responsibility level when the current Incident Management level is likely to achieve the agreed results. An escalation will result in a higher level of management attention thus ensuring that every effort is made to achieve the shortest possible resolution to an Incident.
"Excusable Downtime"	means the time during which the Service is not Available due to Planned Maintenance or Emergency Downtime.
“Inventory in Consignment”	means inventory of iotspot hardware, owned by iotspot, that is provided to a third party, at no cost, in consignment for the purpose of the RMA process.
"Incident Management"	means the process and methodology employed to bring about the timely resolution of a recognized and recorded incident.

Term / Expression	Meaning
"Incident"	means a failure of the infrastructure that is acknowledged by iotspot to provide the Service in accordance with iotspot terms and service. An Incident is classified in one of four Priority Levels.
"Incident End Time"	means the point in time determined by iotspot and agreed by Customer that an Incident ends provided that the Incident has ended and provided Customer may not unreasonably withhold its agreement that an Incident has ended
"Incident Start Time"	means the point in time Customer notifies iotspot that an Incident is occurring.
“Local Timezone of Customer (LToC)”	means the time-zone of the Customer’s office location(s).
“Month”	means unless the context indicates that a full calendar month is intended, a continuous period until the same date in the following calendar month
"Planned Maintenance"	means where the Service is suspended in accordance with iotspot terms and conditions. Planned Maintenance is scheduled to be executed in a time window from Monday till Thursday from 00:00 – 07:00u LTZoC
"Priority Level 1 (P1) Incident"	means an Incident that causes a complete outage or significant failure or degradation in performance of the infrastructure resulting in decreasing the Availability of the Service of all production iotspots and downloaded/ distributed Mobile Apps and therefore Customer is not able to access or use the Service as intended, reproducible by iotspot and outside Excusable Downtime.
"Priority Level 2 (P2) Incident"	means an Incident that causes a significant failure or degradation in performance of the infrastructure resulting in decreasing the Availability of the Service of a significant amount (>40%) of production iotspots and downloaded/distributed Mobile Apps, reproducible by iotspot and outside Excusable Downtime.
"Priority Level 3 (P3) Incident"	means an Incident that causes a failure or degradation in performance of the infrastructure resulting in decreasing the Availability of the Service (>15% AND =<40%) of production iotspots and downloaded/distributed Mobile Apps, reproducible by iotspot and outside Excusable Downtime.
"Priority Level 4 (P4) Incident"	means an Incident that causes a minor failure or degradation in performance of the infrastructure resulting in decreasing the Availability of the Service of a small number (>3% AND =<15%) of localised production or testing iotspots and downloaded/distributed Mobile Apps, reproducible by iotspot and outside Excusable Downtime.
“Problem”	means the (root) cause of one or more Incidents
“Return Material Authorized (RMA)”	iotspot hardware that malfunctions and of which the malfunctioning is covered by the iotspot warranty and therefor is authorised to be returned to iotspot (in the context of this document to be replenished from the “Inventory in consignment”).
"Resolution Time"	means the time to restore the Service measured from Incident Start Time to Incident End Time for Priority Level 1 (P1), Priority Level 2 (P2), Priority Level 3 (P3) and Priority Level 4 (P4) Incidents.
"Response Time"	means the time to respond to a written (e-mail) ticket, or a telephone call when e-mail is not available, submitted to the iotspot Support Desk (support@iotspot.co).
“Response"	means an initial acknowledgement (phone or e-mail) of an Incident delivered by Customer to iotspot or a notification (phone or e-mail) from iotspot to Customer in the case that iotspot discovers an Incident in the iotspot infrastructure prior to notification from Customer.
"Service"	means all services provided in the territories by iotspot to Customer.
“Service Level”	means the level of Availability and Performance of the Service offered to Customer.
“Service Window”	means the time window in which support is provided to Customer by the execution of the Incident Management process of iotspot . The service window for Priority Level 1 (P1) and Priority Level 2 (P2) Incidents is 24x7. For Priority Level 3 (P3) and Priority Level 4 (P4) Incidents, the service window is defined from 08:00 till 18:00 LToC on Working Days

Term / Expression	Meaning
"Working Day"	Monday through Friday.

Table 1 - Terms and Expressions

3 iotspot Service Level

3.1 iotspot service

iotspot B.V. provides non business critical 'Smart Workspace' services resulting in office (occupancy, utilisation and climate) information, by which Customer can:

1. Optimise the workspace, i.e. volume, layout, interior design and work-station offering of its offices;
2. Facilitate staff with workplace (desks & rooms) management and flexible working concepts like ABW and Agile working;
3. Improve the Facility Service to provide a more hospitable and cost efficient working environment; and
4. Detail out "Smart Building" concepts or coordinate FMIS, BMS and/or Office Domotics;

3.2 iotspot technology

The iotspot service uses both Software and Hardware to provide for:

1. Platform as a Service (PAAS), comprising of:
    1. iotspot(s), which is a Hardware device that identifies both desks and rooms physically in the office as well as virtually on the Internet;
    2. Smart sensors, which are Hardware devices that monitor and provide information about occupancy, utilisation and interior climate parameters;
    3. An internet (of things) communication infrastructure for the iotspot independent of the Customer's ICT infrastructure;
    4. A mobile App for users to interact with the iotspot(s), downloadable from the iOS and Android online stores;
    5. An Amazon WebServices Cloud Server infrastructure, to store and report on the workspace management transactions; and
    6. Remote and on site support infrastructure.
2. Software as a Service (SAAS), comprising of:
    1. A Web-based information dashboard;
    2. A Map view of the office layout, based on Google Maps technology and modified for in office application; and
    3. Web-based occupancy information displays.

3.3 iotspot Service Level

The Service Levels pertaining to PaaS and SaaS that iotspot B.V. promises to deliver and Customer can hold iotspot B.V. accountable for are:

1. Availability of PaaS and SaaS, outside Excusable Downtime is:
    1. 99,5% available for use between 06:00:00 to 20:00:00, 7 days a week and 365 days a year; and
    2. 99,0% available for use between 20:00:01 and 05:59:59, 7 days a week and 365 days a year; and
2. Quality of performance of PaaS during Availability, defined as number of Incidents during a Year:
    1. For Priority Level 1 (P1) Incident: None;
    2. For Priority Level 2 (P2) Incident: not more than 1
    3. For Priority Level 3 (P3) Incident: not more than 3; and
    4. For Priority Level 4 (P4) Incident: not more than 5.
3. Quality of performance of a SaaS component during Availability, defined as number of Incidents during a Year :

1. For Priority Level 1 (P1) Incident: not more than 1 per component;
2. For Priority Level 2 (P2) Incident: not more than 2 per component;
3. For Priority Level 3 (P3) Incident: not more than 4 per component; and
4. For Priority Level 4 (P4) Incident: not more than 7 per component.

3.4 Recording and reporting on Service Level;

Every 6 months iotspot will report the number and severity of the reported incidents to Customer. Based on this report, Customer and iotspot assess the actual Service Level and determine the need for and definition of mitigation plans and activities. If contractual consequences hinge on the Service Level, these will be discussed, implemented and properly executed.

4 iotspot Service Desk, Service Window and Contact Details

Customer may submit requests for iotspot to provide support services to address Incidents with the iotspot infrastructure. iotspot is prepared to do everything possible to resolve this as fast as possible. That is why our staff members at the iotspot Service Desk are ready to assist you, even outside office hours.

The preferred method of contact during office hours (from 08:00 – 18:00 Local time zone of Customer) is by e-mail (support@iotspot.co) and by phone (see the distribution list) directly to the Service Manager in case of a Priority 1 (P1) or Priority 2 (P2) Incident.

Outside the Service Window (18:00 – 08:00 Local time zone of Customer) our staff is happy to answer your queries and call in the appropriate experts immediately in the case of Priority Level 1 (P1) and Priority Level 2 (P2) Incident.

The person contacting iotspot needs to be available to explain and/or describe the Incident if further details are required to solve it. In this case iotspot will contact the Customer contact person. Timely resolution of an issue may require Customer to provide supporting evidence of the Incident.

5 Incident Management

5.1 Description

This process ensures the interaction in case of an Incident in delivery of the Service between Customer and iotspot. Communication takes place between Customer's Support Centre / Level Zero and iotspot's Service Desk (Annex A table 4).

5.2 Incident Response Time

In Table 2 the maximum Response Time per Incident Priority Level in the Incident Management process is defined.

Incident Priority Level	Maximum Response Time	Service Window	Reporting means
Priority Level 1 (P1)	180 clock minutes	24x7 support	Phone and e-mail
Priority Level 2 (P2)	300 clock minutes	24x7 support	Phone and e-mail
Priority Level 3 (P3)	1 Service Window Working days	08:00 – 18:00 LTZoC	e-mail
Priority Level 4 (P4)	2 Service Window Working days	08:00 – 18:00 LTZoC	e-mail

Table 2 - Response Times

Please note that Priority 1 (P1) and Priority 2 (P2) Incidents must be reported via the support e-mail (support@iotspot.co) and additionally by telephone to our Service Manager in order to guarantee the listed Response Time.

5.3 Interface

The Incident Management interface is defined in Table 3 below.

Incident Priority Level	Customer	iotspot
Priority Level 1 (P1)	Service Desk staff member	Service Manager
Priority Level 2 (P2)	Service Desk staff member	Service Manager

Incident Priority Level	Customer	iotspot
Priority Level 3 (P3)	Service Desk staff member	Service Desk staff member
Priority Level 4 (P4)	Service Desk staff member	Service Desk staff member

Table 3 – Incident Management Interface

5.4 Reporting an Incident

The Incident reporting and resolution process is defined as follows:

1. Incident is reported by iotspot or Customer, through e-mail and and/or by phone;
2. Priority and the reason of priority is indicated by Customer and defined by iotspot;
3. Customer data is collected and the Incident is registered by Customer and iotspot;
4. Incident reference numbers are exchanged between parties;
5. Analysis / diagnosis of the Incident is performed by iotspot;
6. Resolving / repairing the Incident is done by iotspot;
7. Testing is executed by iotspot;
8. Pre-closure is reported by iotspot; and
9. Final closure of the Incident in mutually agreed upon.

When reporting an Incident, the following information is required:

1. Description of the Incident – what does the Customer experience or see out of the ordinary?
2. Times, dates, locations, countries, addresses,….
3. Number of devices involved in the Incident;
4. In case of malfunctioning hardware devices, ID's of the devices involved;
5. In case of malfunctioning Mobile Apps, the phone types and Operating System versions;
6. Technical details of the location, if any;
7. Historical data of the Incident, if any

In the event of a disturbance that is not clearly attributable to either the Customer domain or the iotspot domain, both parties will work together to solve the Incident. After the Incident is resolved an evaluation can be initiated by iotspot or Customer to establish why the domain could not be established up front.

In case the Incident is in the Customer domain, iotspot provides best effort support to resolve this Incident.

5.5 Incident Resolution Time

In Table 4 the maximum Resolution Time per Incident Priority Level in the Incident Management process is defined.

Incident Priority Level	Maximum Resolution Time	Service Window	Reporting means
Priority Level 1 (P1)	18 clock hours	24x7 support	Phone and e-mail
Priority Level 2 (P2)	48 clock hours	24x7 support	Phone and e-mail
Priority Level 3 (P3)	4 Service Window Working days	08:00 – 18:00	e-mail
Priority Level 4 (P4)	6 Service Window Working days	08:00 – 18:00	e-mail

Table 4 - Resolution Times

For Priority Level 1 (P1) and Priority Level 2 (P2) Incidents the Resolution Time shall start immediately after Customer contacted the iotspot Service Desk reporting such an Incident (i.e. the Incident Start Time). Priority Level 1 (P1) and Priority Level 2 (P2) Incidents shall be reported by Customer by phone next to the notifying the Service Desk of the Incident by e-mail (support@iotspot.co).

Priority Level 3 (P3) and Priority Level 4 (P4) Incidents shall be handled within the Service Window. These Incidents shall be reported by Customer through e-mail (support@iotspot.co). For Incidents reported outside the Service Window (18:00 – 08:00 LToC) the Resolution Time shall be started at the start of the Service Window on the next Working Day.

5.6 Progress of Incident

After an Incident with Priority Level 1 (P1) is reported, a progress report shall be provided by iotspot to Customer on a regular basis (i.e. about every 6 hours) via email. The progress update includes the diagnosis, the action(s) required and the expected time to repair the Incident. The minimum information is:

1. Both iotspot's and Customer's Incident reference numbers;
2. Description of the Incident;
3. Any actions that have been undertaken and necessary follow-up actions;
4. Indication of expected resolution/repair time;
5. Time for next status update;

If the agreed Resolution Time will be exceeded or the Incident is very urgent, the escalation process described in section 5 of this DAP is activated.

5.7 Closure of an Incident

At the moment of closure of a Priority Level 1 (P1) Incident, iotspot will provide an incident statement to Customer. After resolution and internal investigation of a Priority Level 1 (P1) Incident, a problem report is created describing the root cause of the Incident, the solution provided and structural corrective actions taken. This problem report is shared with Customer. The details shared in the incident statement and problem report are:.

1. Both iotspot's and Customer's Incident reference numbers;
2. Reporting if the Incident has been resolved temporarily or fully;
3. The actions that have been undertaken in order to resolve the Incident;
4. The time at which the Incident has been resolved;
5. Additional contents in a Problem report:
    1. Any follow-up actions in case the Incident was resolved temporarily (the Incident is classed as a Problem)
    2. The cause of the Incident, also known as 'reason for outage'

6 Escalation Management

6.1 Description

Escalation management concerns handing over the necessary activities to a higher responsibility level when the agreed Service Levels are likely to be exceeded. An escalation will result in a higher level of management attention thus ensuring that every effort is made to achieve the shortest possible solution to a Service disruption. Additionally, the escalation management procedure serves to inform both organisations about the scope of an Incident, the progress, the time needed to correct it and any emergency measures or actions that must be taken. The escalation management procedure applies to all aspects of the Service.

Customer is able to set the Incident priority when submitting an Incident using the Service Desk e-mail or phone. This priority is judged by the iotspot service desk staff member and if agreed used within iotspot based on the incident priorities as defined in Table 1. A limited number of employees of Customer shall be authorised to increase the priority of an Incident or increase the level of escalation. Customer and iotspot service employees engaged in the incident and escalation management process are defined in Annex A.

6.2 Interface and Escalation Times

In Table 5 below, the escalation time per Incident Priority Level in the escalation management process is defined.

Escalation level	Priority 1 (P1)	Priority 2 (P2)	Priority 3 (P3)	Priority 4 (P4)
0	N.A.	N.A.	N.A.	N.A.
1	6 hrs	16 hrs	2 Working days	3 Working days
2	12 hrs	32 hrs	3 Working days	5 Working days

Table 5 - Escalation Management Interface

6.3 Procedure

An escalation starts at the initiative of a Customer or the iotspot Service Desk staff and will always be taken up one step at a time in the schedule above in accordance with the requirements, impact and results. This is subject to the relevant counterparts informing each other before escalating to the next (responsibility) level. Each level will first escalate to its relevant counterparts before escalating to the own organisations' next level.

For a Priority Level 1 (P1) Incident the service manager is involved in the resolution process 4 hours after the Incident is reported to iotspot. After 8 hours, iotspot Operations manager is also involved.

After the resolution of an escalation, iotspot or Customer may call an evaluation meeting, where both parties will participate.

7 Problem Management

7.1 Description

Problem management is about the investigation of an unknown underlying cause of one or more Incidents. The problem management process allows iotspot and Customer to register and exchange relevant information about problems.

7.2 Interface

The Problem Management interface is Service Desk staff member of Customer to Service Desk staff member of iotspot.

7.3 Procedure

Based on the Incident analysis/diagnosis a Problem is identified. To resolve a Problem, iotspot or Customer defines a Request for Change that defines an adjustment of the Service and has the Priority Level of the associated Incidents it will structurally resolve.

Any Service Change with respect to a Problem will be implemented according to the process, defined below:

1. A Request for Change (RFC) is agreed to by the Service Manager, ensuring all required information is validated with Customer;
2. The designated RFC is shared with all customers of iotspot as to validate the scope of the Problem and the impact on the Service;
3. Based on the scope and the impact, the Service Manager and Operations Manager of iotspot decide if a RFC is executed as a Minor or Major Release item, where:
    1. A Major Service Release is at the end of a period of 3 Calendar Months; and
    2. A Minor Service Release is at the end of a period of 4 Calendar Weeks;
4. The Service Manager determines the planning of the implementation and delivery of the RFC and communicates this to Customer;
5. The RFC is delivered and implemented in the Beta test environment at least a week before final delivery, where it is completes a pre-arranged testing and acceptance procedure (agreed in consultation with Customer);
6. Upon acceptance by the iotspot QA manager and Operations Manager, the RFC is released to Production at the planned date;

7.4 Request for Change Lead Times

The lead time of a RFC depends upon the Priority Level of the associated Incidents:

1. Priority 1 (P1) with minor scope/impact - before or with the second upcoming Minor Release;
2. Priority 1 (P1) with major scope/impact - before or with the second upcoming Major Release;
3. Priority 2 (P2) with minor scope/impact - before or with the third upcoming Minor Release;
4. Priority 2 (P2) with major scope/impact - before or with the third upcoming Major Release;
5. Priority 3 (P3) or Priority 4 (P4) irrespective of scope/impact - when iotspot sees fit.

7.5 Completion of a RFC

After competition of a RFC the below minimum of information is shared with Customer:

1. Both iotspot's and Customer's Change reference numbers;
2. A request to iotspot to start up the acceptance procedure;

3. All relevant information concerning the current PaaS and SaaS infrastructure resulting from the Service Change that is carried out; and
4. A test report, if applicable.

8 Request for information Management (RFI)

8.1 Description

During the contract the need for (more) information may occur. This request for information (RFI) management process describes the way to get this information on time. RFI's can be ad hoc questions about the Service, or a request for a report. In case such a question becomes structural and results in the need for the regular delivery of the information an agreement needs to be made between the Customer and the Service Manager of iotspot (e.g. to agree to take the report as a requirement for a next release).

8.2 Interface

The Information Management interface is Service Desk staff member of Customer to Service Desk staff member of iotspot.

8.3 Procedure

A RFI is accepted by iotspot when is it submitted through the support e-mail and validated by the Service Desk in consultation with the Service Manager. The acceptance of an RFI requires a clean order check, which will generally be completed within two (2) Working Days. If the check cannot be completed within four (4) Working Days, iotspot will provide Customer the cause for delay. When the RFI is classified as clean, and it acknowledged as a RFI, iotspot will confirm the change through e-mail to the requestor.

In case an RFI will result in a change than the change management process in Section 7 applies.

8.4 Request for Information Lead Times

The lead time of a RFI depends upon the impact of the request:

1. Minor impact, will lead to a response time of 2 Working Days; and
2. Major impact, will lead to a response time that is determined in consultation with Customer;

8.5 Planning

Processing times for major RFI's are not pre-defined, but will be within reason and in accordance with the magnitude of the required activities. iotspot will inform Customer about the planning. Committed dates can only be changed in consultation with both parties. The information below is shared when a RFI planning is provided:

1. Customer's RFI reference number;
2. iotspot's RFI reference number;
3. The planned start date of the work; and
4. The planned end date of the work.

8.6 Implementation and Acceptance

iotspot coordinates the execution of the RFI. After completion of the RFI, feedback is offered to Customer for acceptance. If the RFI is not answered to Customer's satisfaction the result will not be accepted; any follow-up action will be decided in consultation.

9 The special case of a Hardware related Incident and/or Problem; RMA

9.1 Description

The iotspot Platform as a Service partially comprises of Hardware devices, i.e. the iotspot and sensor devices as described in section 3.2. This chapter specifies the Incident, Escalation, Problem and RFI management processes in the special cases that the process management subject is either one of iotspot's Hardware.

9.2 No changes to the general set-up of the management processes

In case of a Hardware related Incident, Escalation, Problem or RFI, the general process steps and timing thereof are consistent with those described in the sections 5, 6, 7 and 8. However, there is an additional sub-proces for Incident management, which is the Return Material Authorisation(RMA) process.

9.3 The Return Material Authorisation (RMA) process

For resolution of a Hardware related incident the following process is defined.

9.3.1 Hardware Inventory In Consignment

The Service Desk receives iotspot Hardware Inventory In Consignment at a quantity of 2,5% of the number of iotspot or sensor devices that are active at a designated office location.

In addition to this 'replacement inventory' the Service Desk is provided with a 'support & maintenance' application for smart devices. This App, allows for NFC access to (re)configure the iotspot devices.

9.3.2 Replacement of Hardware

In case of an Incident, the Service Desk will be informed by e-mail if it is required to replace a Hardware device for malfunctioning reasons. If that is the case the Service Desk can replace the malfunctioning device with one from the replacement inventory and (re)configure the PaaS accordingly. The malfunctioning Hardware device is taken into the Inventory In Consignment for 'authorisation assessment'.

9.3.3 Return authorisation

In month 5 and 11 of the contractual calendar, iotspot will assess if the hardware replacement is authorised:

1. The reason for malfunctioning, i,e, the Incident is due to a Problem within iotspot's PaaS and thus is an Authorised Return; or
2. The reason for malfunctioning of the Hardware, i.e. the Incident, is due to inappropriate (re)placement, use or misuse by staff or visitors and thus is not an Authorised Return in which case the replacement item will be invoiced in month 6 or 12 of the contractual calendar.

9.3.4 Replenishment

The replacement inventory is replenished to the 2,5% level after every return authorisation assessment.

9.4 Interface

The RMA Management interface is defined in Table 6 below.

RMA process step	Customer	iotspot
Inventory consignment	Service Desk staff member	Service Desk staff member
Replacement of Hardware	Service Desk staff member	Service Desk staff member
Return authorisation	Service Manager	Service Manager
Replenishment	Service Desk staff member	Service Desk staff member

Table 6 - The RMA Management interface

10 Planned Maintenance

10.1 Description

Planned Maintenance is the delivery of hard- and software releases of the iotspot Service and is categorised as Excusable Downtime.

10.2 Interface

The Planned Maintenance interface is Service Desk staff member of Customer to Service Desk staff member of iotspot.

10.3 Procedure

Releases resulting in downtime with impact on the Service, are announced ten (10) Working Days in advance to Customer. Planned Maintenance is scheduled to be executed in a time window from Monday till Thursday from 00:00 – 06:00u LToC. Commercially reasonable effort is invested to limit service outages duration caused by planned maintenance. If relevant, a test report will be offered by the party responsible for the release.

May 19th, 2021

Annex A - DAP information chart

A1. Customer information and contact details in relation to this DAP

This section details the Customer information and contact details of the staff that are responsible and accountable for the execution of the Daily Agreed Procedures.

Customer Information	
Legal Entity name	
Country	
Streetname	
Street number	
Postal Code	
City	
Contact person contract management	
Contact person for implementation	

Escalation level	Customer Role	Contact person	E-mail	Phone nr.
0				
1				
2				

A2. iotspot information and contact details in relation to this DAP

This section details the Customer information and contact details of the staff that are responsible and accountable for the execution of the Daily Agreed Procedures.

Customer Information	
Legal Entity name	iotspot B.V.
Country	The Netherlands
Streetname	Veemarktkade
Street number	8
Postal Code	5222 AE
City	s-Hertogenbosch
Contact person contract management	Marnix Lankhorst
Contact person for service implementation	Martijn Kors

Escalation level	iotspot Role	Contact person	E-mail	Phone nr.
0	Service Desk		support@iotspot.co	
1	Service Manager	Jules Eekelaar	jules@iotspot.co	
2	Operations Manager	Martijn Kors	martijn@iotspot.co	