**DriveLock Support Specifications for Partner providing 1st Level Support**
Version: 08/2018

This agreement describes the services and obligations of a DriveLock Partner providing with 1st Level Support (partner FLS) to end customers.

Customers who are serviced by a partner FLS initiate support requests exclusively to them. The partner FLS is committed to providing these customers with technical support and the following support and services:

(a) Access to the partner FLS service desk.
(b) Contact to technical support staff to diagnose and resolve technical issues, as well as prioritization and escalation management services.
(c) Technical support staff must be DriveLock Basic or Advanced certified.

## Opening a support request at DriveLock

### *Processes and procedures*

DriveLock's Technical Support follows a multi-level model. On first contact, DriveLock collects, separates, prioritizes and analyzes all data on customer, contract, licenses and fault report. The customer undertakes to supply a full problem description including reproduction steps etc.

If the customer's communication stops without announcement, DriveLock sends a reminder after ten (10) workdays. After another five (5) workdays without reply, DriveLock closes the support incident.

A support request can be re-opened within fifteen (15) workdays after closure. Afterwards, the request expires and cannot be opened again.

If further work is necessary, a new support incident will be opened, and all necessary information must be submitted again.

If a support incident includes more than one fault, DriveLock will separate each fault and open additional support incidents. The DriveLock Policy requires one incident per fault.

### *Support Hours*

DriveLock's Technical Support is available 24/5, Monday thru Friday, Central European Time. On bank holidays, request for support are limited to high priority.

### *Remote Access*

The support staff of the partner FLS enables or coordinates remote access to the affected environment (as far as possible) with the end customer in the event of a high-priority failure. Remote access is via the TeamViewer software.

### *Escalation Process*

Escalation: If the partner FLS wants to prioritize a support incident, he/she communicates the critical situation to the DriveLock Support and describes the consequences on his/her business operation.

The DriveLock Support examines the information provided and decides if the escalation is accepted.
All support incidents are escalated true to the valid DriveLock standard business practice.

If the partner FLS realizes that DriveLock finds no solution in adequate time, they can escalate the incident to the Head of Support or his/her deputy.

### *Priority Definitions*

"**High"** Impact: company
Urgency: complete failure

A critical failure with no justifiable solution: immediately reduces the productive environment and fully disrupts the operation of the main number of terminal devices.

"**Medium**" Impact: workgroup
Urgency: malfunction

A failure with no justifiable solution: substantially limits the operation of several terminal devices or at least one vital function.

"**Low**" Impact: user
Urgency: partial failure

A failure with no justifiable solution: hardly limits the operation of few terminal devices or at least one vital function.

"**None**" Feature Requests

A request for the enhancing of components or functions.

***Initial Response***

DriveLock undertakes commercially justifiable efforts to reply to customer requests during normal business hours as follows:

| Priority | Initial Response |
|---|---|
| **High** | 60 minutes |
| **Medium** | 6 hours |
| **Low** | 24 hours |
| **None** | 48 hours |

For debugging, both DriveLock and the customer provide resources during the support hours mentioned.

**Note**: DriveLock is not liable for instant debugging. On missing the above-mentioned support level targets, DriveLock is liable neither financially, nor legally, nor otherwise.

***Web-Based Access***

Via the „My DriveLock Support" service desk, customers have 24x7x365 access to technical information

***Uploading Data***

Diagnostic data can be transferred to DriveLock with the Support Companion or directly attached to the Incident where the maximum size limit is 20 MB per attachment. Knowledge Article KBA00106 describes the collection of diagnostic data (tracing) and the transmission to DriveLock in detail.

Alternatively, the partner FLS may provide analysis data on an FTP server etc. for download.

***Creating Support Incidents***

High priority support incidents must be reported via telephone only.
Other support incidents must be reported via the "My DriveLock Support" service desk only.

(a) Telephone:

| | |
|---|---|
| Australia | 1800 931 758 |
| New Zealand | 0800 423 678 |
| Singapore | 800 492 23 91 |
| Austria | 0800 281 675 |
| Germany | 0180 437 48 35 |
| International | +49 (0) 89 546 3649 50 |
| Switzerland | 0800 564 685 |
| USA | 1 855 246 43 53 |

(b) Internet: „My DriveLock Support" service desk (registration required):

a. Go to *Support, select Report a New Incident*
b. In line *Quick Call*: Click on *"…"*
c. A list opens: Click on affected component
d. Fill out *Description* and add attachments. The description should be structured as follows:
e. Press *Submit*
f. The system automatically creates a support incident
g. DriveLock confirms the incident creation via e-mail referencing the Incident-ID in the subject line

(c) Email: Partner FLS using a Service Desk may open incidents at Drivelock, by prior arrangement, via email. The setup requires a unique identifier in the subject of the e-mail.

(d) When opening a support request by e-mail, the template stored in Knowledge Base article KBA00110 must be used.

(e) A collective account can be set up for support staff of a partner FLS. For the initial setup DriveLock requires the following information:

| | |
|---|---|
| Company name: | Partner ABC |
| Address: | Sonnenallee 1, 12345 Musterhausen |
| First name: | Support |
| Last name: | ABC |
| E-mail: | support@abc.com |
| Telephone: | +49 (0) 12 345 678 90 |

The request can be made by e-mail to helpdesk@drivelock.com or through an incident.

DriveLock confirms incoming support request. After the DriveLock confirmation, e-mail communication is possible (subject: #INC <number>, for example, # INC00001).

Knowledge Base article KBA00107 includes an example of a detailed documented incident report.

DriveLock confirms incident creation via email, you can respond to existing incidents via e-mail. (Subject is: #INC<Number>, i.e. #INC00001).

***KBA00107 Incident – Issue description***

In order to be able to solve support requests efficiently, the software support specialist needs relevant information about the problem at hand. To understand the context of a disturbance, e.g. answers to the following questions are helpful:

- Is it a new disorder or has it occurred before or always?
- Have any changes been made to the system?
- How many systems are affected?
- What distinguishes this system from those in which the fault does not occur?
- What effects does this disruption have on the user / company?
- What steps led to this disorder?
- How was DriveLock installed?
- Can the disorder be reproduced? If so, which steps are necessary?
- Which software versions were executed when the error occurred?
- Is the fault reproducible with the latest DriveLock version?
- Were error messages or other diagnostic information generated?
- etc. etc.

This information has to be handed over in a structured manner when opening a support request:

**# General Information**
...
**# Issue Description**
...
**# Issue details**
...
**# Environment details**
...
**# Steps to Reproduce**
...
**# Business Impact**
...
**# Issue Verification**
...

Here is an example of a detailed description of a DriveLock partner:

**# General Information**

| | |
|---|---|
| Customer: | Sample customer GmbH, Sonnenallee 1, D-01234 Musterstadt |
| Contact person: | first name, last name |
| E-Mail: | firstname.lastname@samplecustomer.de |
| Phone: | +49 12 345 678 |

**# Issue Description**
High CPU utilization (up to 100%) DriveLock Agent Service. When the problem occurs, the task manager displays a load of up to 100% of drivelock.exe (with 29,000 handles). Working on the system is therefore no longer possible. Once the DriveLock service is restarted everything is OK again. After 2-3 hours running time, the problem occurs again. As additional information the customer uses also Web Security.

**# Issue details**
The customer has now managed in the meantime by restarting the DriveLock service on all systems in a regular rhythm. Only then is it possible for users to work without restrictions.

Before upgrading to DriveLock version 7.7.10, versions 7.6.14, 7.6.16 were in use. As a test, some computers have version 7.6.18 installed. Reason for the updates were problems with the inheritance of the guidelines. After that, the problems with the high CPU utilization have occurred.

**# Environment details**
- MMC: 7.7.10.18786
- DCC: 7.7.10.18809
- DES: 7.7.10.18809
- DDB: SQL Express 2014 SP1
- Agent: 7.7.8.18786
- Microsoft Windows 7 Professional 6.1.7601 Service Pack 1 Build 7601

**# Steps to Reproduce**
Restart the PC. Wait about 2-3 hours until the CPU load increases again.

**# Business Impact**
Affected are all systems of the company.

**# Issue Verification**
A preliminary analysis (Event Logs, DriveLock settings, etc.) was performed without any indication of causes. Then tracing was activated which brought the following findings:

At the moment when the CPU load increases, the web security logfile (DlSvcWSec.log) will be flooded with entries. The log file finally reaches a size of 58GB and more. The system runs full of lack of space.

Due to the size of the logfile this can't be read anymore. A section of it is attached. The entries are always the same. In the meantime, a copy of the policy was created without active Web Security and assigned to these 3 PCs.

The problem has not occurred on these PCs so far.

Click here to open the Knowledge Base article in your web browser.