Service Level Agreement

Last update: 04-01-2023

Coachview

The heart of your
training organisation

Introduction

In this document you will find the service levels agreements about the Coachview service.

You can find more substantive information about the program on our website: Coachview.net

Coachview
Verlengde Velmolen 4b
5406 NT Uden
The Netherlands

Tel. +31 88 44 88 550

Info@coachview.net
www.coachview.net

Coachview is a product of InnoPhase BV, part of the Paragin Group.

Table of contents

1   Infrastructure

Coachview data centre

Coachview is hosted in a professional (ISO 9001, ISO 27001 and ISO 14001 certified) dedicated data centre. Power supply is guaranteed by deployment of UPS systems, secure power connections on three different phases per rack and a diesel generator. Air conditioning is double (redundant).
All servers and data are located in the Netherlands and are therefore subject to Dutch legislation.

Security

The DataCentre is physically and electronically secured with closed-circuit video (CCTV), alarm system and electronic keys. Outside office hours, a security company monitors the servers. A certified fire detection system is in place.

Not Planned downtime

For 'not planned downtime', we guarantee an availability of >= 99.8% per year (24 hours a day, 365 days a year). 'Not planned downtime' > 15 minutes during office hours, we communicate within 2 hours, including an indication of resolution time. Once resolved, we communicate a summary of the incident via email, including total duration of downtime. If "internal failures" in the application lead to incorrect processing of data and it is therefore necessary to restore an earlier backup of data, we include the lost time as 'not planned-downtime'. We monitor continuously to identify failures immediately.

Planned downtime

We do maintenance work and installing new releases outside office hours (Mon-Fri, holidays excluded) 08:30 - 17:00. We always announce such work in advance via the Coachview application, or e-mail.
'Planned downtime' does not count in the availability percentage.

Coachview

2   Backup

Coachview makes a daily system and data backup of the entire environment. Every 15 minutes, the transaction files are backed up on a failsafe backup server. This backup is only generated for own usage purposes: due to Coachview's multitenant setup, it is not possible to restore data from an individual customer or user.

3   Helpdesk

Availability

From 08:30 to 17:00 on working days, the helpdesk is available for users.

Reachability

The helpdesk is available via +31 88 44 88 555 or email helpdesk@coachview.net.

Response times

Are there critical and serious disruptions? If so, we issue a response within 30 minutes and start solving the disruption immediately. If the disruption is serious but work can continue, we will issue a response within 2 hours and resolve it within 4 hours. For other disruptions, we respond within 1 working day, including an indication of the resolution time.

4   Security

SSL connection

The connection over which we send data is encrypted via an SSL certificate (the lock shown in the browser).

Login

The application can be accessed using a username and password. We take several measures to ensure the security of the login account:

- after 5 incorrect passwords, we block the account for 20 minutes
- when checking the password, you do not know whether the account exists
- we store passwords in hashed form so that no one can retrieve them

Password policy

We have a relatively strict password policy to prevent weakness in the security structure. Our password requirements:

- 8-15 characters
- at least 1 lowercase letter
- at least 1 uppercase letter
- at least 1 digit
- at least 1 special character: !#€$%()*+,-./:;=?[\]^_{|}`~&"<>@'
- user and company data must not be used in the password. Think first name, company name and place of birth
- we do not allow simple words such as Welcome and combinations of letters
- the password is not identical to any of the 15 previous passwords
- the password must be changed every 60 days.

For the training portal, we recommend deploying Single-Sign-on (SSO), for example via your own ActiveDirectory, so that you can align the password policy with your own security.