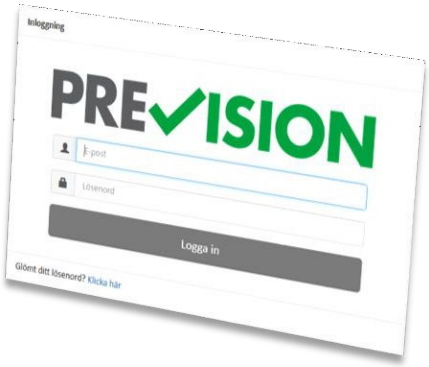
Bilaga

Security applied in PreVision



Presto PreVision is operated by IT provider Iver, a company with many years of experience and in-depth knowledge on operational safety as well as system development and management. The building blocks leading to our secure operating environment are presented below.

Data centre

Iver's main data centre has been designed in compliance with the international TIER3 standard, which guarantees 99.982% availability.
%. This means that the main components of the data centre must not be unavailable for more than 94 minutes per year. This is achieved by means of the market-leading, redundant systems for both power supplies and cooling.

Web operation

PreVision is a web application that runs in a virtual server environment. The environment can be rescaled to meet actual requirements. The virtual server environment is fully redundant to guarantee superior system availability. The Iver Service Desk monitors all components 24/7, every day of the year. Our Service Desk manages and rectifies any access issues during daytime hours, should these occur. In the evenings and at night, automatic notifications are sent to our emergency service, which immediately undertake troubleshooting and corrective actions.

Any access to PreVision, including data input and document upload and management, uses data encryption relying on SSL certificates.

Data storage

The PreVision system, including both databases and files, is hosted in a redundant Storage Area Network (SAN). Complete backups are made every 2 hours between 6:00 and 20:00. In addition, an extra backup is made every 24 hours and mirrored to an independent SAN site, approx. 100 km away. In case of a total breakdown, the system can be restarted and hence becomes operational on the secondary SAN site, where it can remain operational for a long time.

Protection against intrusion and tampering

PreVision is protected by a firewall that only accepts encrypted SSL data traffic. The firewall is connected to the Internet via optical fibre and features full protection against DDoS attacks. Any attacks are typically detected and remedied within a few seconds and, thus, will not affect user access to the system. As a matter of routine, the firewall is included in our normal maintenance and monitoring procedures.

Physical protection

The data centre is protected by intrusion alarms connected to security guards with emergency response. The entrance features camera surveillance to minimise the risk of intruders. Also all corridors outside the entrance are camera monitored. All visits to the data centre are logged at an individual level by person name, date and time of arrival and departure. The logs are checked monthly and kept for 12 months. Camera surveillance inside the data centre relies on motion detectors and IR technology. Recorded video footage is saved for a minimum of 30 days and checked by the Security Manager according to established routines.