

Security

Nothing is more important than the safety of our customers' data

In a SaaS solution security must be integrated on all levels: in the encryption, internet access, web server database, and most importantly – in the source code.

“Lack of security can have disastrous consequences for the company and its customers. TimeLog therefore works continuously on testing and improving the safety of our products.”



Christoffer Lanstorp
Manager, R&D
TimeLog A/S

Security of supply

TimeLog's solutions are hosted by Progressive IT, who are certified Microsoft ASP Channel Partner and specialised in hosting.

The connection from the data centre is duplicated by two independent suppliers, which results in nearly 100% effective uptime.

Encrypted access and firewalls

TimeLog Project is accessed via a 128 bit encrypted connection (HTTPS/SSL) delivered and managed by VeriSign. The level of encryption is comparable to that used by most online banking providers.

The SSL-encryption enables data sent between a registered user and TimeLog's systems to be encrypted, making it impossible to snatch up transferred information.

There are firewalls in front of all web servers, and between web and database servers.

Database backup

Each customer has his/her own database and codebase. A full backup of all data is made every night, which is moved to another physical location. All changes in the database are furthermore registered in a transaction log.

It is possible to order a security copy of the database, which can be delivered to your company by agreement.

Hardware duplication

To reduce the risk of hardware crashes the servers that hold TimeLog Project are duplicated, that is there are two hard disks, two network cards, and two power supplies.

Furthermore, the servers are dedicated; i.e. they only handle one function.



ISV/Software Solutions

TimeLog's products are built with Microsoft technologies.

Since 2007 TimeLog has been Microsoft Gold Certified Partner and Microsoft ISV/Software Solutions.

As part of the certification Microsoft has tested the security of TimeLog's products – and found no issues.

Increase IT-security through simple means

- Make a security policy, where the company revises the security level and communicate this policy to employees.
- Insecure passwords are the most prominent reason for lapses in security. In TimeLog Project it is possible to set up rules for how secure passwords have to be.
- Shut off access for previous employees – unfortunately, previous employees often represent a large threat to the IT-security.
- Avoid having a master password – and avoid using templates for passwords.
- Always keep anti-virus software updated.