Security and data protection with use of SINTEF's SharePoint platform

SINTEF uses SharePoint Online for collaborative sharing of data both internally and externally. Documents, files and other data are stored on Microsoft's cloud platform, in data centres in Ireland and Netherlands. Data centres in the USA or other countries outside of the EU/EEA are not used.

Practicalities regarding collaborative sharing and login

Individuals with whom data will be shared will receive a link via e-mail to the shared project room or file.

Help with the initial login can be found at www.sintef.no/uno

- Users must log on with the same e-mail address they are invited with.
- Users do not need to have Office installed to work with documents stored on SINTEF's SharePoint platform. Documents can be opened with the Online version of SharePoint, which allows easy editing of documents directly from the browser.
- It is possible to work with others at the same time, on the same document.
- SharePoint Online uses a version history function that saves automatically new versions of the file worked on.
- If any files are deleted, they will still be available for 30 days in the trash folder, and they can be reinstated. For any further file restoration requirements, contact SINTEF for assistance with backup.

Data security

- Data is encryption protected when stored on SINTEF's servers.
- Encryption with the SSL/TLS protocol protects data transferred between used and SINTEF's SharePoint Online platform.
- Threat management, security monitoring and file- and data integrity prevents or registers any manipulation of data.

The 10 most important security and data protection functions with the Microsoft SharePoint platform

1. Microsoft limits physical access to the data centres to authorized personnel, and several layers of physical security are implemented, for example, biometric readers, motion sensors, 24-hour secured access, video monitoring and security breach alarms.
2. Microsoft actively encrypts data both when stored on the server and when transferred between a data centre and a user on the network.
3. Microsoft does not use customer data for commercial purposes.
4. Microsoft uses customer data only to perform the SharePoint Online service.
5. Microsoft routinely copies data for security.
6. Microsoft does not delete any data stored on an account at the end of the service agreement until after the user has had the possibility to transfer the data.
7. Microsoft hosts customer data regionally.
8. Microsoft uses "hard" passwords to increase the security of customers' data.
9. Microsoft allows the user to turn on and off functions affecting personal data security, as the user desires.
10. Microsoft is contractually obliged to follow the protocols listed above, through the data handling conditions in the licensing agreement.