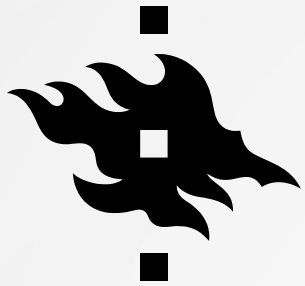




RDM ADVANCED

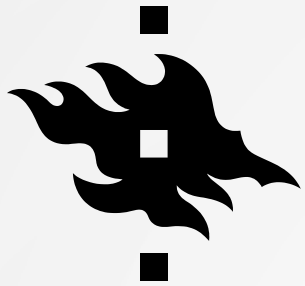
SENSITIVE DATA



SENSITIVE DATA CHECKLIST



- What makes your data sensitive?
- Have you assessed the risk level of your data?
- Can you pseudonymize or anonymize the data?
- What is the workflow with your data?
- What software do you process your data with?
- Who do you need to share your data with?
- From where do you work with your data?
- How long do you need to store your data?
- What happens to your data after the project is over?



BASIC RISK ASSESSMENT

Are you obliged by law or agreement to protect the data?

No

Yes

Can the data be freely published?

Would a potential data leak be harmful to individuals or organizations?

Yes

No

No

Yes

"Public"

"Internal"

"Confidential"

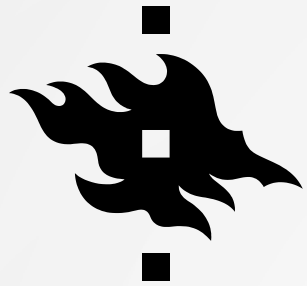
"Secret"



UH HOME AND GROUP FOLDER

- Can be used to store Public, Internal and Confidential data
- In other words, only low or medium risk sensitive data can be stored in home and group folders
- All sensitive data should be encrypted or pseudonymized when stored in home and group folders
- Access control, backup and version control are featured
- The most convenient solution when the data is not high risk and access can be limited to University of Helsinki user groups

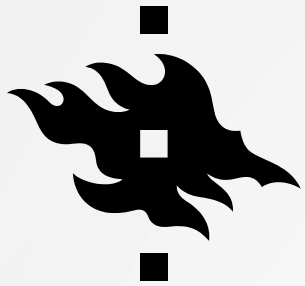




UMPIO

- A high security storage space & desktop in UH network
- Closed environment with no internet access
- For "Secret" data, in other words high risk sensitive data
- Accessed through a virtual desktop environment (VDI)
- Utilizes two-factor authentication
- Features are similar to UH personal and group storage
- Data is manually transferred from physical workstations to the secure storage space
- Some scientific software is available for processing data directly in the virtual desktop environment without downloading it to your local computer
- License upgrade is needed for students and non-employees being able to access the environment

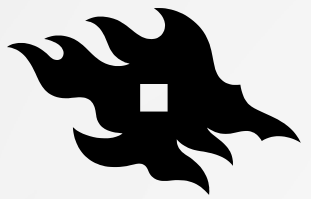




CSC SENSITIVE DATA SERVICES

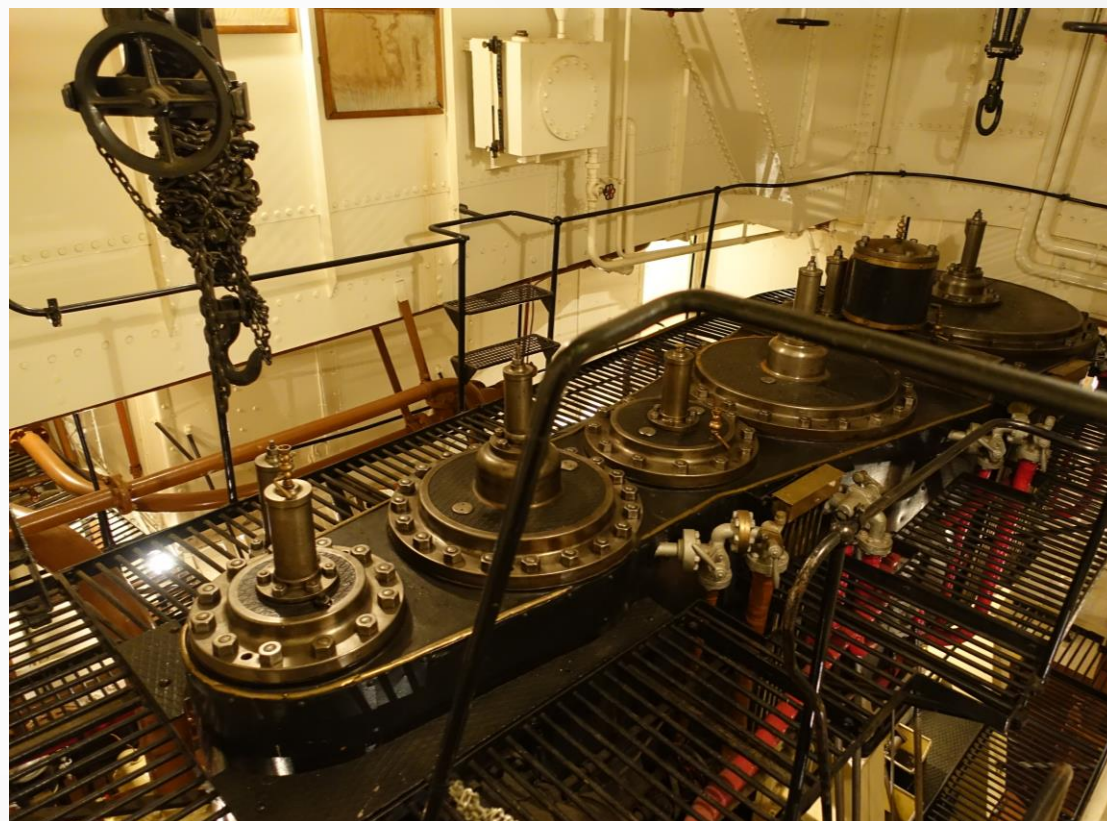


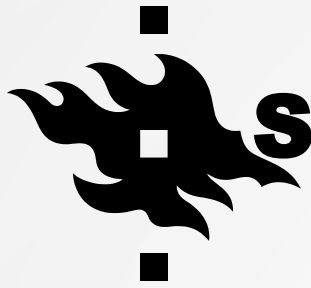
- CSC service for storing sensitive data
- SD Connect is a utility for storing and sharing data
- SD Desktop is a utility for processing the data uploaded with SD Connect
- Also available restricted version of Desktop for secondary use of social and health data (Findata)
- Ideal solution for working over organizational boundaries in Finland
- Data can be accessed from CSC HPC environment



SERVERS

- Physical and virtual UH servers can be used for processing sensitive data
- Physical UH servers can be placed in physically secure cabinets
- UH virtual servers in the "TL3"-cluster have enhanced security measures
- CSC provides ePouta –servers for sensitive data
- Virtual servers are preferred to physical ones for more fault tolerance and expandability





SECURE DATA COLLECTION & TRANSFER

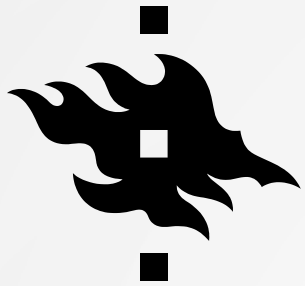
UH Services

- RedCap data collection tool
- Secure e-mail

CSC Services

- Funet Filesender with encryption
- SD Connect / Desktop
- Eduuni (for pseudonymized and small files)





SECONDARY USE OF HEALTH AND SOCIAL DATA

- Secondary use law is valid from May 2022
- New requirements for storing health and social data
- CSC SD environment is compatible with the law
- List of compatible services will be at Valvira [website](#)

