VITENSKAPELIG HØYSKOLE
Norwegian School of Theology, Religion and Society

Utdrag fra Rutiner for lagring av forskningsdata ved MF vitenskapelig høyskole («Lagringsguiden»)

(For english, see below.)

Lagring av data på privat utstyr og maskiner

Du kan benytte privat utstyr underveis i oppgaver og forskningsarbeid når disse kriteriene er oppfylt:

- du følger MFs rutiner for bruk av privat utstyr, og
- du gjennomfører en ROS-analyse der du tar stilling til om dataene må krypteres.

Skal du behandle særlige personopplysninger skal dataene som hovedregel krypteres.
Rådfør deg med veileder når du vurderer om kriteriene ovenfor gjelder din oppgave.

Rutiner og sikkerhetstiltak du kommer fram til må forevises IT-leder eller forskerstøtte.

Rutiner for bruk av privat utstyr

1. Ingen andre brukere bør bruke datamaskinen, familie og venner må i tilfelle ha egne kontoer.
2. Minimere risikoen for at maskinen blir stjålet, mistet, gjenglemt el. (vurdér kensingtonlås, låst skap/safe e.l.)
3. Du må ha god kunnskap om maskinen:
   - Du bør ikke ha installert programmer du ikke trenger/bruker
   - Du vet hvilke backup og synkoniseringsløsninger du bruker, slik at eventuelt ukryptert materiale ikke ligger i mapper som synkes til Adobe, Google Music, Apple iTunes/iCloud, eller backupløsninger fra Get, Elkjøp el.

4. Følg vanlig praksis for god datasikkerhet (se også nettvettreglene på nettvett.no)
   - Automatisk sikkerhetsoppdatering må være slått på
   - Antivirusprogram må være installert, oppdatert og aktivt
   - Aktivere skjermlås og innlogging med passord
   - Bruk gode, unike passord
   - Ha gjerne kryptert harddisk (se eget punkt om kryptering)
   - Vis sunn skepsis til lenker i epost og på nettsider
   - Utvis forsiktighet ved bruk av ukjente trådløse nettverk

Gjennomfør gjerne en risiko- og sårbarhetsanalyse (ROS-analyse), og ta kontakt med IT-avdelingen for å avklare mer detaljerte spørsmål om datasikkerhet.

Se MFs nettsider for detaljert informasjon om datahåndteringsplan, fysisk sikring og kryptering.

Gjengitt fra MFs nettsider (pr. 4. september 2020):
https://www.mf.no/forskningogphd/forskning-ved-mf/dokumenter-forskningen/rutiner-lagring-av-forskningsdata

Storing data on private devices and machines
You may use private devices when working with theses and research if the following two criteria are fulfilled:

- you adhere to MF's routines for the use of private devices
- you conduct a Security and Risk Analysis (SRA) where you decide on whether or not you need to encrypt the data.

If processing personal data, the data should as s rule be encrypted.
Consult your advisor when considering whether the above criteria apply to to your thesis.

Routines and security measures that you arrive at must be cleared by MF's IT director or research adviser.

Routines for the use of private devices

1. No other users should use the computer. If they do, family and friends must have separate accounts.
2. Minimize the risk of the machine being stolen, lost, forgotten and so forth (consider using a kensington lock, locked cabinet/safe etc.).
3. You must have good knowledge of the machine:
   - You should not have installed programs that you don't need/use.
   - You know which back-up and synchronizing solutions you use so that unencrypted material is not found in folders that are synched to Adobe, Google Music, Apple iTunes/iCloud, or back-up plans from Get, Elkjøp etc.

4. Follow standard practices for sound computer security (see also general internet safety tips)
   - Automatic security updates must be activated.
   - Anti-virus programs must be installed, up-to-date and activated.
   - Activate screen locks and login with password.
   - Use good, unique passwords.
   - Have an encrypted hard disk if possible (see elsewhere on encryption)
   - A healthy scepticism regarding links in e-mails and on web sites.
   - Caution when using unfamiliar wireless networks.

We encourage you to conduct a security and risk analysis (SRA) of your project. Please do not hesitate to contact the IT department to reach clarity on more detailed questions about computer security.

See our web pages for information about data management plans, physical security and encryption.

Excerpt from mf.no (04. September 2020):
https://www.mf.no/en/standard-procedures-storage-research-data