

University of Applied Sciences Technikum Wien

Data back-up and archiving guidelines

These guidelines are intended to govern three basic values with respect to IT security and indicate measures for complying with these basic values. These are:

Availability: Users have access to functions and services when required. A compromise to the integrity of information can mean that it has been modified without authorisation or information regarding the author has been falsified or the time of generation has been manipulated.

Confidentiality: Confidential information must be protected against unauthorised access.

Integrity: The data is complete and unaltered. Therefore, a compromise to the integrity of information can mean that it has been modified without authorisation or information regarding the author has been falsified or the time of generation has been manipulated.

(1) Availability

The following backup and archiving strategy is to be used to ensure the long-term availability of the requisite data:

The data is backed up with the assistance of a tape robot (HP OpenView) The "HP OpenView Storage Data Protector Manager" is installed on the "xanthype" server.

The following servers are currently included in the periodic back up plan:

Server	Data	Retention period	Back up type
theseus	FHComplete - FASOnline	4 weeks	1 x Full (Saturday) 4 x Incremental
hades	Fileserver Fixangestellte [permanent staff]	4 weeks	1 x Full (Saturday) 4 x Incremental
sirene / nestor	Fernlehre [distance learning], Moodle CIS components	4 weeks	1 x Full (Saturday) 4 x Incremental
polyxena	E-Mail lists Additional restrictions for students: E-mails deleted > 6 months in the mailbox	3 weeks	1 x Full (Saturday) 4 x Incremental

antigone	WAWI	4 weeks	1 x Full (Saturday) 4 x Incremental
Server	Data	Retention period	Back up type
hydra	Administration server (internal)	4 weeks	1 x Full (Saturday) 4 x Incremental
xanthype	Data protector management, Netenforcer management, SUS Server	4 weeks	1 x Full (Saturday) 4 x Incremental

At the end of each month one tape is labelled with a unique title (month/year) and removed from the daily cycle. This ensures that the end of period data is backed up at the end of the month. This tape is stored externally.

The following servers are not backed up centrally:

fhe	Fileserver permanent staff and lecturers home drives
eid	Fileserver Student shares, tuition
ladon	Reverse Proxy
valar3	Entrance examination via DTP
valar	Dynamic Power Trainer
stud. year server	Fileserver academic year

(2) Data archiving

Once a year (end of August) a complete backup is created on tape for data archiving purposes and stored externally in the Mariahilferstrasse executive management office.

All digitalised degree-relevant data stored outside FASOnline can be downloaded into the [\\hades\admin\Datensicherung](#) folder until the 15/08 each year by the relevant departments/degree courses managers, which means that they will be retained for seven years as a result of this annual backup. This folder also contains the software programs required to open these data. (E.g. Office version or Adobe Acrobat Reader etc.)

The following data are contained:

hades → Home folders employees

Data storage → [hades\admin\Datensicherung](#) [i.e. [hades\admin\backup](#)]

polyxena → Mail boxes (end of period backup)

antigone → WAWI data backup

sirene/nestor → Teaching documents Teaching/Distance education

theseus → FASOnline DB backup

FASOnline → dumpfile for import into DB

The backup is stored for 7 years. The tapes are to be labelled as follows: Month/Year Date created e.g.: 08/2008 – 31.08.2008

Data not included, local data: Each of the users/operators are responsible for backing up their own data when data is saved on central department servers or on local workstation drives which are not included in the aforementioned backup and archiving strategy.

The enclosed risk analysis questionnaire is intended to increase the awareness of users in each case and also offer various solutions.

Data security questionnaire

The following questionnaire is intended to help you assess your risk potential yourself. If you find that you have to answer many questions (red) you should contact the service desk in the infrastructure section in order to develop your own personal data security strategy with their assistance.

(1) Do you save important data on your local hard drive, without backing it up on external media (C:\)?

☐ YES ☐ NO (go to 2.3)

(2) Do you back up your local data on external media (CD, USB, ext. HDD, network)?

☐ YES ☐ NO (go to 2.3)

(2.1) How often do you back up your data?

- ☐ weekly
- ☐ monthly
- ☐ annually
- ☐ others:

(2.2) Have you ever tried to restore data?

☐ YES ☐ NO

(2.3) Do you know where your mail file is stored (Outlook → pst file, Thunderbird → Profile folder)?

☐ YES ☐ NO

(2.4) Do you save your local mail database (e.g. pst file in Outlook)?

☐ YES ☐ NO

(2.5) Do you keep a copy of your e-mails on the UAS Technikum Wien mail server?

☐ YES ☐ NO

3. Do you use network drives to store your data that are not included in the backup?

☐ YES ☐ NO

3.1 What are the names of the network drives you use to store data (Server, share name)?

3.2 Do you duplicate these data in several places (locally, network etc.)?

☐ YES ☐ NO

Important additional information

Existing backup programs for local data security:

Mail data backup: <http://www.priotecs.com/>

Local data back up: <http://www.acronis.de/>
<http://www.usb-backup.de/>
<http://www.z-dbackup.de/datensicherung.html>
<http://deutsche-shareware.de/download/D2.htm>