

Richtlinie zur Datensicherung und Archivierung an der Fachhochschule Technikum Wien

Diese Richtlinie soll drei Grundwerte der IT-Sicherheit und deren Maßnahmen zur Einhaltung dieser Grundwerte regeln. Dabei handelt es sich wie folgt um:

Verfügbarkeit: Dem/der BenutzerIn stehen Funktionen und Dienste zum geforderten Zeitpunkt zur Verfügung. Der Verlust der Integrität von Informationen kann bedeuten, dass diese unerlaubt verändert wurden oder Angaben zum/zur AutorIn verfälscht oder der Zeitpunkt der Erstellung manipuliert wurde.

Vertraulichkeit: Vertrauliche Informationen müssen vor unbefugter Benutzung geschützt werden.

Integrität: Die Daten sind vollständig und unverändert. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert wurden oder Angaben zum Autor verfälscht wurden oder der Zeitpunkt der Erstellung manipuliert wurde.

(1) Datensicherung

Um die Verfügbarkeit der benötigten Daten langfristig sicherzustellen, wird folgende Backup- und Archivierungsstrategie angewendet:

Die Datensicherung wird mithilfe eines Bandroboters (HP OpenView) durchgeführt. Der Softwareteil „HP OpenView Storage Data Protector Manager“ ist am Server „xanthype“ installiert.

Folgende Server sind derzeit in den periodischen Sicherungsplan inkludiert:

Server	Daten	Behaltdauer	Sicherungstyp
theseus	FHComplete - FASOnline	4 Wochen	1 x Full (Samstag) 4 x Inkremental
hades	Fileserver Fixangestellte	4 Wochen	1 x Full (Samstag) 4 x Inkremental
sirene / nestor	Fernlehre, Moodle CIS-Komponenten,	4 Wochen	1 x Full (Samstag) 4 x Inkremental
polyxena	Mailverzeichnisse zusätzliche Einschränkungen für Studierende: Mails > 6 Monate werden in der Mailbox gelöscht	3 Wochen	1 x Full (Samstag) 4 x Inkremental

antigone	WAWI	4 Wochen	1 x Full (Samstag) 4 x Inkremental
Server	Daten	Behaltdauer	Sicherungstyp
hydra	Verwaltungsserver (intern)	4 Wochen	1 x Full (Samstag) 4 x Inkremental
xanthype	Dataprotector Management, Netenforcer-Mgmt, SUS-Server	4 Wochen	1 x Full (Samstag) 4 x Inkremental

Zu jedem Monatsende wird ein Band gesondert beschriftet (Monat/Jahr) und aus dem Tageszyklus herausgenommen. Dadurch wird gewährleistet, dass Stichtagssicherung per Ende des Monats vorhandenbleiben. Dieses Band wird extern aufbewahrt.

Folgende Server werden nicht zentral gesichert:

fhe	Fileserver Home-Laufwerke Fixangestellte und LektorInnen
eid	Fileserver Studierendenshares, Lehre
ladon	Reverse Proxy
valar3	Reihungstest via DPT
valar	Dynamic Power Trainer
stud. Jahrgangsserver	Fileserver Studienjahrgang

(2) Datenarchivierung

Zum Zwecke der Datenarchivierung wird einmal pro Jahr (Ende August) eine Vollsicherung auf Band erstellt und diese wird in die Geschäftsführung in der Mariahilfer Straße ausgelagert.

Alle digitalisierten zeugnisrelevanten Daten, die außerhalb von FASOnline aufbewahrt werden, können bis 15.08. jedes Jahres in dem Verzeichnis [\\hades\admin\Datensicherung](#) von den zuständigen Instituten bzw. Studiengängen abgelegt werden und werden dadurch mit dieser Jahressicherung 7 Jahre aufbewahrt. Zusätzlich sind in diesem Verzeichnis auch die Softwareprogramme abgelegt, die für das Öffnen dieser Daten notwendig sind. (z.B. Office Version od. Adobe Acrobat Reader etc.)

Im Detail sind folgende Daten enthalten:

hades → Homeverzeichnis MitarbeiterInnen

Datensicherung → hades\admin\Datensicherung

polyxena → Mailboxen (Stichtagssicherung)

antigone → Sicherung WAWI Daten

sirene/nestor → Sicherung Lehrunterlagen Lehre/Fernlehre

theseus → Sicherung FASOnline DB

FASOnline → dumpfile zum Import in DB

Die Datensicherung wird 7 Jahre aufbewahrt. Die Bänder sind wie folgt zu beschriften:

Monat/Jahr – Erstellungsdatum, z.B: 08/2008 – 31.08.2008

Nicht inkludiert Daten, lokale Daten: Für die Sicherung von Daten, die auf zentralen Institutsservern, oder auf lokalen Platten der Arbeitsplatzrechner abgelegt werden, die nicht in der oben genannten Sicherungs- und Archivierungsstrategie enthalten sind, sind die jeweiligen BenutzerInnen/BetreiberInnen selbst verantwortlich, Datensicherungen durchzuführen.

Der nachfolgende Fragebogen zur Risikoanalyse soll das Bewusstsein der jeweiligen User schärfen und auch Lösungsvarianten anbieten.

Fragebogen zur Datensicherheit

Der nachfolgende Fragebogen soll Ihnen zur Selbsteinschätzung Ihres Risikopotentials dienen. Sofern Sie feststellen, dass Sie viele Fragen mit NEIN beantworten müssen, sollten Sie sich mit dem Service Desk der Infrastrukturabteilung in Verbindung setzen, um gemeinsam Ihre persönliche Datensicherheitsstrategie auszuarbeiten.

(1) Speichern Sie wichtige Daten auf Ihre lokale Festplatte, ohne zusätzlich eine Sicherung auf externen Medien abzulegen (C:\)?

☐ JA ☐ NEIN (weiter bei 2.3)

(2) Sichern Sie Ihre lokalen Daten auf externen Medien (CD, USB, ext. HDD, Netz)?

☐ JA ☐ NEIN (weiter bei 2.3)

(2.1) Wie oft sichern Sie die Daten?

- ☐ wöchentlich
- ☐ monatlich
- ☐ jährlich
- ☐ sonstige:

(2.2) Haben Sie schon einmal versucht, Daten wieder rückzusichern?

☐ JA ☐ NEIN

(2.3) Wissen Sie, wo Ihr Mailfile gespeichert wird (Outlook → pst-File, Thunderbird → Profilordner)?

☐ JA ☐ NEIN

(2.4) Sichern Sie Ihre lokale Maildatenbank (z.B. pst-Datei von Outlook)?

☐ JA ☐ NEIN

(2.5) Behalten Sie eine Kopie Ihrer Mails am Mailserver der FH Technikum Wien?

☐ JA ☐ NEIN

3. Verwenden Sie zur Ablage Ihrer Daten Netzwerklaufwerke, die in die Sicherung nicht einbezogen sind?

☐ JA ☐ NEIN

3.1 Wie heißen diese Netzlaufwerke, die Sie zur Datensicherung verwenden (Server, Freigabename)?

3.2 Duplizieren Sie diese Daten auf mehrere Stellen (lokal, Netzwerk etc.)?

☐ JA ☐ NEIN

Wichtige Zusatzinformationen

Interessante Backup-Programme für die lokale Datensicherung:

Maildaten sichern: <http://www.priotechs.com/>

lokale Datensicherung: <http://www.acronis.de/>
<http://www.usb-backup.de/>
<http://www.z-dbackup.de/datensicherung.html>
<http://deutsche-shareware.de/download/D2.htm>