Daniel C. Oderbolz :: Head User Support :: Paul Scherrer Institut
Walter Morath :: IT Servicedesk :: Paul Scherrer Institut

PSI Tools for the management of scientific information

Lib4RI Course “Searching & Managing Scientific Information”
Information Security starts with you

- If you observe anything strange (Email, Software Behavior): http://i.psi.ch/i3x3
- In General: remain sceptical
  - Do not send Passwords over insecure channels
  - Treat Email like a Postcard – its not safe!
- Make sure to use only properly licensed Software

**Information security guidance**

**Passwords**
- Easy to remember, hard to guess
- Derive from a sentence (e.g. IItw@P.S.I!)
- Do not reuse PSI passwords for external services
- Use separate passwords for user and administrative accounts
- Store passwords safely (using e.g. Keepass from SW-Kiosk)

**Data protection**
- Avoid to expose personal or PSI data
- Choose a secure storage location for your data (Network Drives, DMS, SwitchDrive)
- Lock your monitor even on short absences
- Shut down your machine at the end of the day
- Use Standard-Systems if possible

**E-Mail**
- Be cautious, especially if the mail contains threats, bills or seems to offer a prize
- Do not open attachments from unknown senders
- Take extra care with these file types: *.zip, *.exe, *.com, *.pdf, *.scr
- Never answer to spam

**In case of an information security incident**
- If unsure, disconnect from network (unplug cable/disable wireless)
- Immediately call IT servicedesk (4800)
- Outside office hours: http://css.psi.ch
- Never pay ransom for your data!

**Surfing**
- Properly logout from online services
- Enter passwords on secure (https://) connections only

**Where do I find more information?**
- http://i.psi.ch/isee
- Follow the IT regulations (AW-95-6.6-01)

**Software**
- Only install software from the website of the software publisher
- Install available updates regularly
- Obtain valid licenses for your software products
On-Campus WLAN Access

PSI Users must use “corp” Network
(http://i.psi.ch/VdmV)

Non-PSI users: please use Eduroam or “guest” with their own VPN
From closed to open knowledge: Collaboration
Use the intranet Wiki for collaboration

“my own” Lab-Book

• PSI uses a Wiki to manage Intranet & Internet Content
  – https://intranet.psi.ch
• You already know the concept from Wikipedia
• Manual: http://i.psi.ch/7pyD
• Applications:
  – Electronic Lab-Book (full-text searchable, history function)
  – Lab & Group Documentation
  – Meeting Minutes
  – Simple Event Management (Beyond that: indico.psi.ch)

“our own” Wiki
The DMS lets you organize your documents
Documents are the essence of digital work

• However: collaboration is often messy
• DMS allows a way out of Email Ping-Pong
• Another strength is finding documents (full-text!)
• Access it: https://ecm.psi.ch
• Manual: http://i.psi.ch/wQHs
• Applications:
  • PSI-Internal collaboration on documents (non-concurrent)
  • PSI-Internal dissemination of documents
  • Example: https://ecm.psi.ch/share/page/site/phd-students/dashboard
Look & Feel
How to share data with external Collaborators?

- Consider AW-11-14-03 (http://i.psi.ch/lhm9).
  - As a rule of thumb, share only unclassified files

- Recommended System: Switch Drive (http://i.psi.ch/bWJH)
  - “Dropbox” for Swiss academic Institutions
  - Data can also be shared with non-academic partners

- Also possible: Datatrans (http://i.psi.ch/ZtG9)
  - Replacement for existing FTP Server

- To just send data once, use File Sender (http://i.psi.ch/uEN8)
Use central storage if possible

- Generally: **DO NOT STORE DATA ONLY LOCALLY** (no automatic backup)
- Use either Windows or AFS Drives
  
  [http://i.psi.ch/gLMS](http://i.psi.ch/gLMS)
Restore data on a Windows Share

• Restoring is easy (2 snapshots per day)
Installing Software on a Windows system

- With Windows 7, the SW Kiosk was introduced
- > 100 Packets available
- No admin permissions required!
VPN connections into PSI from the above date will only be available to registered users.
VPN Access can only be granted via an application process, which must also be approved by a line manager. The required SecurID-Token will be available via the Consumer Self Service Tool → css.psi.ch, under Request Fulfillment / IT Service Catalog.
Access to the ETH Web mail is still possible without VPN. VPN is required if you want to do E.g. Home Office and access the group or project drives or you want to take influence from home or on the road to systems at PSI.
For Home Office, we recommend the use of so-called soft tokens, they are easier to handle and less expensive. An app is running on your smartphone which generates the token (part of the password). The soft token app on your Smartphone works offline and need no network connection.
Contact IT Servicedesk

- Report incidents -> css.psi.ch
- Order IT Services -> css.psi.ch
My thanks go to

- The AIT Team
- You all