IRCT Anti-Torture Database Digital Security Guide

The purpose of this Digital Security Guide is to assist torture rehabilitation centres using the IRCT's Anti-Torture Database (ATD) in enhancing their digital security and ensuring the highest possible standards are followed to protect personal data.

This Digital Security Guide outlines three basic security steps to improve the secure use of the ATD:

1. **Secure Passwords**
2. **Secure Backups**
3. **Secure Devices**

The Digital Security Guide also covers additional steps that outline how:

- Information is secured when it is shared, transferred or deleted
- Computers that use the ATD are secured
- Steps are taken to ensure that other types of files are stored securely

---

1. *Passwords* are more secure, if

- They are long: it is recommended that passwords are longer than 12 characters
- They are complicated: they contain a mix of upper and lower-case letters, numbers and symbols
- They are changed periodically: every 3, 6, or 12 months
- They are individually assigned to each user or purpose
- They are easy to remember (or easily and securely accessed and stored)

A good practice for securing passwords (for teams) is the use of a password manager (like *keepassxc*). A master password is needed, and all other passwords will be secured and accessed through the password manager.

http://keepassxc.org/

2. *Backups* are more secure, if

- They are done frequently (according to your needs of how much time needed to recover the information without backups and how often the information is changed)
- They comprise at minimum the most important data (including data in the ATD)
- They consist of a backup on a separate external storage (USB or hard drive) inside the office and another backup kept outside the office in a different location to prevent loss of both in case of theft or fires etc…
- They are encrypted, and password protected so that the data cannot be read and accessed easily from another device

Secure backup options for Windows are *Cobian Backup* and the *Windows Backup and Restore*.

Cobian Backup: http://www.cobiansoft.com/cobianbackup.htm
Windows 7 and 8: https://support.microsoft.com/en-ca/help/17127/windows-back-up-restore
Windows 10: https://support.microsoft.com/en-us/help/17143/windows-10-back-up-your-files

3. *Devices* are more secure, if

- They are protected by passwords
- They are encrypted (Full Disk Encryption), so that the data on it is not accessible without the password and cannot be accessed by bypassing the password. Secure encryption options for Windows are *Bitlocker* or *Veracrypt*.
- They are kept securely in areas that are not accessible by clients or the public.

Veracrypt: https://www.veracrypt.fr/en/Home.html

Bitlocker: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview

Other applications

Certain applications may collect data on how you use your computer (usually for targeted advertising), including through cookies and location services. If you are using the ATD, please make sure:

- That, before using the ATD, you completely close other apps and programs, especially those that have direct access to the internet (like Facebook and Skype). Some programs run in the background and might collect user data or provide unsecure access to your device. Therefore, please make sure that you also completely shut down these background services. Don't forget to close the ATD before you start using other applications and programs.
- In general, if an application requests permission to see which other applications are running, make sure to completely close this application before using the ATD.

Example for Windows 10: how to close Skype securely: https://www.howtogeek.com/284864/how-to-stop-skype-from-running-in-the-background-on-windows-10/

Recording: Audio and Video Files

If you make audio or video recordings they have to, at minimum, be secured in the same way as the ATD [See section 3 above].

Secure deletion of files

Normal deletion via the Windows Recycle Bin only removes the name and location in the file system from the real file, meaning that it is easy to recover these deleted files. If you want to make sure that they are unrecoverable then you need to overwrite them. Our devices, including USB sticks, hard drives and smartphones, keep distributed copies every time we open, change and save the file. In order to completely eradicate the file, all empty space needs to be overwritten. Tools (on Windows) to do this are *Ccleaner* and *Bleachbit*.

Ccleaner: https://www.ccleaner.com/
Bleachbit: https://www.bleachbit.org

File transfer and sharing

If you share or transfer files or reports containing sensitive personal or confidential information from the ATD, please make sure that you follow the steps above to ensure they are stored and transferred securely and are subsequently securely deleted with an overwrite of the empty space [see the step above] when they are no longer needed.

Additional resources:

Digital security: https://securityinabox.org
https://ssd.eff.org/
https://www.digitaldefenders.org/digitalfirstaid/

Holistic security: https://holistic-security.tacticaltech.org/
http://integratedsecuritymanual.org/

Please remember! Your digital security is strongly linked with your emotional wellbeing and your physical security.