IISPV
INSTITUT D'INVESTIGACIÓ SANITÀRIA PERE VIRGILI

DECALOGUE GOVERNING THE CONFIDENTIALITY OF INFORMATION WHILE TELEWORKING

All IISPV staff must respect the measures governing the security and confidentiality of information in accordance with current legislation and in a specific way in and the IISPV's Regulations Governing the Use of the Information and Communication Technologies (ICT).

In particular they must respect the regulations below:

1. Treat with maximum respect all confidential data, documents, methodologies, passwords, analyses, programs, documents and personal data that you become aware of as a result of participating in the processing of IISPV data.
2. Keep passwords and other security codes secret (it is important that you do not save passwords on your browser).
3. Use the personal data that the user can access exclusively for professional purposes and do not mix them with private data or files.
4. Use only the servers and other storage systems indicated by the IISPV to store information.
5. Should you ever download documents onto your computer, delete the temporary information from the downloads folders, recycle bin or any other similar folders that there may be in the computer's directories (for example, in "My documents").
6. Do not allow unauthorised people to access personal data or confidential information.
7. Turn off the connections to servers and websites or intranets with the option "Disconnect" or "Close session".
8. Keep all printed documents in a safe place while they are not being used and do not leave printed copies unattended on tables, printers, etc.
9. Do not destroy any printed information with personal or confidential data outside the IISPV. It is of the utmost importance that it is not thrown into recycling bins or reused as recycled paper at home. All documents with personal and confidential data must be destroyed in accordance with the instructions from the IISPV Archive.
10. Data can only be shared by using the storage systems provided by the IISPV or the collaborative tools that have been made available. Do not uses non-IISPV storage devices or send information to non-IISPV email addresses.