Specific guidelines for IT security and personal data protection in telework

Employees who are working remotely must guarantee the confidentiality and security of the data and information that they use and have access to, and prevent them being altered, lost, processed, accessed without permission or improperly used by all possible means.

Teleworkers must comply with the UPC's information security policy and the UPC Data Protection Manual.

With regard to **computer security and telework**, follow the instructions you will find by clicking on this link: https://serveistic.upc.edu/ca/eines-teletreball/documentacio/guia-teletreball#section-1.

With regard to **personal data protection and telework**, follow the instructions below, in addition to those in the UPC Data Protection Manual:

- Personal data must be processed using the systems and services that the University provides to employees who are working remotely: https://serveistic.upc.edu/ca/treballa-en-remot. Personal data must not be processed in cloud services with which the UPC does not have a contract. Otherwise, the traceability of the personal data is lost, there are no guarantees as to how the data will be processed and the data are jeopardised.

- Documents containing personal data must not be shared using remote work tools (e.g. G Suite Drive) with users outside the upc.edu domain without express permission.

- Personal data must not be sent from a non-UPC e-mail account.

- Employees who are teleworking are responsible for their own work space and must therefore take appropriate measures to prevent unauthorised access to confidential information. Teleworkers must exercise the utmost caution regarding such information for an indefinite period of time and may not disclose or use data, documents, methodologies, keys, analyses, programs, studies or any other information belonging to the UPC, on paper or in electronic format, directly or through third parties or entities. They must act to prevent access to personal data or confidential information by unauthorised persons.

- Teleworkers have a personal, non-transferable password to access files containing personal data. The password is confidential, therefore:

    - They must not disclose it to anyone without the express permission of the head of the unit.
    - They should memorise it and never write it down.

  - They must change it if it has been compromised.
  - They must contact the University's IT services if they cannot remember it. (It is important not to store passwords in your web browser.)

- Employees must use the personal data that they have access to only and exclusively for the intended purposes corresponding to their work and never mix them with private data or files.

- Temporary information must be deleted from download folders and the recycle bin or similar folders that may be in computer directories such as My Documents in the exceptional event that documents have been downloaded locally.

- Connections to servers and websites or intranets must be closed by using the exit or log-out option.

- Employees must prevent unauthorised persons from accessing documents containing personal data on screen and on paper while they are away from their desk. Computers must be screen-locked, and paper-based information must be securely stored.

- Paper documents containing personal or confidential data must not be destroyed outside the University. It is very important not to place them in recycling bins and not to reuse them at home. Documents with personal and confidential data must be disposed of in accordance with the instructions of the UPC Archive.

The staff should notify any IT security or personal data protection incident to the ATIC customer service -- atic@upc.edu -- and will follow their instructions, which could include blocking or disconnecting the device's network.

24 March 2020