

TELEWORKING POLICY

1. Purpose and scope of application

To regulate the provision of services via teleworking for ICN2 personnel.

2. Definition

The provision of services via teleworking is a form of work organisation whereby part of the working week is carried out remotely using information and communication technologies.

3. Regulatory framework

Based on Decree 77/2020, of 4 August, which regulates the provision of services via teleworking, and in accordance with Article 2.2 of the aforementioned decree, teleworking will be approved by the ICN2 Board of Trustees.

And, subsidiarily: Law 10/2021, of 9 July, on remote working.

4. Requirements for the provision of services via teleworking

- a) Having a job or undertaking activities that can be carried out remotely, i.e. in a non-face-to-face manner, given that the specific characteristics and the resources required to carry them out are in place. Accordingly, point 9 details the procedure for authorising the provision of services via teleworking.
- b) The Head of Department/Group Leader/Division Leader or, in their absence, the ICN2 Manager or Director certifies that the provision of the work or service will not be affected as a result of teleworking.
- c) Having sufficient and secure computer equipment and communications and Internet connectivity systems, with the characteristics defined by the IT department and under the conditions referred to in point 10 of this Policy.

5. Duration of authorisation

The teleworking agreement shall be established for a maximum period of one calendar year from date of approval, and may be extended by maximum periods of one year at a time.

6. Work schedule and hours

The working week will be distributed in such a way that services will be provided via teleworking for a maximum of two days a week. Face-to-face and teleworking hours can be combined on the same day.

Teleworking days will be regulated according to the schedule established in the annual work schedule, respecting breaks and rest periods between working days, in accordance with ICN2 Collective Bargaining Agreements and current legislation.

Physical presence at work may be required on teleworking days for duly justified service needs, with a minimum notice of 24 hours.

7. Recording hours worked

Employees shall record time spent teleworking, using the time recording system implemented by ICN2.

- Employees must specify "teleworking" as the reason in the time recording system, and all their working hours will be recorded as actual hours worked.
- If an employee exceptionally combines hours of work carried out at the workplace with hours of work carried out from home (on prior agreement with their manager), they must log the start and end times of the hours spent at the workplace and the start and end times of the hours worked from home.

8. Rights and obligations

Employees providing services via teleworking have the following rights and obligations:

- a) Identical rights and obligations to those of other ICN2 staff, without there being, for the reason of teleworking, any effect on remuneration or any difference with respect to training opportunities, professional promotion or any other right recognised for staff contracted by ICN2.
- b) Specific training and information on cybersecurity, personal data protection and occupational risk prevention prior to the start of teleworking.
- c) A requirement to participate in questionnaires or other teleworking evaluation instruments determined by the occupational risk prevention service.
- d) The right to digital disconnection and guaranteed respect for their rest time and personal privacy.
- e) The right to withdraw, at any time, from providing services via teleworking, given that teleworking is voluntary.

9. Procedure for authorising the provision of services via teleworking

To be able to apply for teleworking, employees must first meet the requirements outlined in point 4.

Interested persons must inform HR, with the approval of the Head of Department/Group Leader/Division Leader or, in their absence, the ICN2 Manager or Director, of their intention to provide teleworking services, taking into account that the maximum number of teleworking days per employee is 2 days a week.

HR shall respond within a maximum of 10 days with the agreement proposal to be signed by the parties.

The mutual agreement between the parties will enter into force upon signing the agreement.

10. Technological resources for the provision of services via teleworking

Any costs associated with teleworking shall be borne by the person providing the services via teleworking. Similarly, if personal equipment is used, the costs of technical assistance corresponding to the use of said equipment shall also be borne by the person providing services via teleworking.

Staff members authorised to provide services via teleworking must observe the recommendations for use and the security rules issued by ICN2 with regard to cybersecurity. They must meet the technical requirements and conditions for the use of technological resources in accordance with the instructions issued regarding the use of information and communications technologies (ICT).

Staff members authorised to provide services via teleworking shall use ICN2's portable computer equipment, if available. They shall also be responsible for the proper use and security of the equipment under the conditions established in the previous sections.

Authorised staff members shall connect to the Internet via a password-protected WiFi network, in accordance with the specific indications for guaranteeing an adequate level of security.

Authorised staff members must guarantee Internet connectivity, ensure that it is fully operational, and resolve any incidents with the operator as quickly as possible.

The IT department shall provide support in relation to the tools and resources made available to those authorised to telework.

If anyone does not have tools and resources provided by ICN2 and uses their own resources to provide services via teleworking, the IT department may provide limited technical support if necessary. Authorised persons shall ensure that ICN2 content and their own personal content are kept separate. They shall also have

separate access accounts to prevent third parties from accessing ICN2 content or software. Where possible, they shall use available network drives and avoid downloading ICN2 content locally.

11. Cases in which teleworking authorisation becomes void

Authorisation for the provision of services via teleworking may become void if expressly renounced by the authorised person.

Similarly, the authorisation to provide services via teleworking may be revoked by the person who authorised it, after the authorised person has been given a prior hearing, in the following cases:

- a) Owing to duly justified service needs.
- b) For serious breach of obligations regarding security, data protection or confidentiality, without prejudice to any disciplinary liability that may have been incurred.
- c) Owing to a negative evaluation of performance in providing services via teleworking.

12. Provision of occasional services via teleworking

The provision of occasional services via teleworking may be authorised in the following exceptional cases:

- a) When, by reason of a service outside the usual place of work, travel is inefficient; in which case the remaining working day may be completed on a teleworking basis.

For the purposes of guaranteeing the correct provision of services. This must be communicated immediately, using the most appropriate means (telephone, e-mail, etc.), to the direct person in charge, who may authorise the provision of services via teleworking.

- b) Where an agreement exists between the person in charge and the authorised person which, owing to the service needs, specific and concrete tasks arise for which teleworking is more appropriate and effective.

In this case, the provision of services via teleworking needs to have been foreseen and authorised by the person directly responsible for the person concerned and always be of an exceptional and non-periodic nature.

- c) When a person, following surgery or hospitalisation, provided that they have been medically discharged, or in any other extraordinary situation, is unable to travel to work to provide services in person, they may voluntarily request to provide services via teleworking, agreeing on the duration of this temporary situation.

These situations must be recorded by the authorised person using the time recording system.

13. Data protection and information security

The authorised persons shall comply with data protection and information security regulations, including the confidentiality agreement.

The security measures in place for accessing ICN2 data when teleworking must guarantee, in any case, a level of security equivalent to that when accessing the data at the work centre. The credentials and validation processes will be the same as those used when at the work centre. The software programs used shall be those approved by the IT department.

The authorised persons shall adopt the necessary technical and organisational measures to maintain the confidentiality of the information in their charge, preventing disclosure or access to this information by third parties. To maintain this confidentiality, other persons must be prevented from listening in on conversations concerning work-related matters.

Employees shall comply with everything included in the confidentiality obligation and in the applicable personal data protection regulations, and shall take the necessary measures to prevent any unauthorised person from accessing confidential or protected data, under the same conditions as in the performance of their duties in person. The services accessed by employees will be centralised and integrated with all company validation and permission systems.

Efforts should be made to telework from appropriately protected environments, safe from view and access by others with whom they share the remote workplace. Printing or handling paper-based information should be avoided wherever possible. Where appropriate, this documentation should be safeguarded to prevent it from being accessed by third parties, thus compromising its confidentiality.

Similarly, employees who are teleworking must adopt the necessary measures to preserve their own privacy, by not disclosing details of their private life or that which might affect their personal or family intimacy, especially when connecting remotely and during teleconferences. Failure to comply with this recommendation means that ICN2 cannot guarantee employees' privacy expectation.

Teleworkers shall notify ICN2 of any incidents in the place of work, or problems with the resources made available to them, that could compromise the security of the information processed or safeguarded, as well as any technical difficulties that impede the normal performance of remote work or that do not allow the implementation of the agreed security measures.

14. Occupational risk prevention

With regard to prevention, Article 16 of Spanish Royal Decree-Law 28/2020 stipulates that remote workers have the right to adequate health and safety protection, as does Decree 77/2020, of 4 August; and the provisions of Law 31/1995, of 8 November, on the Occupational Risk Prevention (ORP), and its implementing regulations, apply in all cases.

Teleworking, or telecommuting, allows employees to work in an alternative location to the workplace or ICN2's facilities using new communications technologies.

The risk assessment and planning of preventive activity shall include the typical risks associated with this type of working, with special attention given to psychosocial, ergonomic and organisational factors.

ICN2 shall obtain all information regarding risks through an appropriate methodology, which in this case will be an online questionnaire. This questionnaire will facilitate data collection and verification of the working conditions, allowing additional information to be added such as photos of the place of work, characteristics of the furniture, resources available, etc. The questionnaire will then be evaluated by a competent technician and a risk assessment will be generated and corrective measures proposed if necessary. Once the review has been completed, a report will be issued along with a risk sheet with prevention information for the employee.

Where appropriate, the risk assessment shall only cover the area designated for the provision of services, and shall not include other areas of the home or place chosen for carrying out remote work.

If, in order to obtain the necessary information, the Prevention Department needs to visit the workspace, a written report justifying the visit will be drawn up and given to the employee.

This visit will always require the employee's permission if it is their home or that of a third party. If permission is not obtained, the Institute's preventive activity will be carried out solely on the basis of the risks identified through the information gathered via the questionnaire.

With regard to health surveillance, training and information on occupational risk prevention, maternity and breastfeeding protection and other related issues, the current procedures for ICN2 personnel apply.

15. Approval of the policy

This policy was approved by the ICN2 Board of Trustees, in Bellaterra, on 9 December 2021.

Prof. Pablo Jesús Ordejón Rontomé

ICN2 Director

02869535D Firmado
PABLO digitalmente por
JESUS 02869535D PABLO
ORDEJON (R: JESUS ORDEJON
G63277776) (R: G63277776)
Fecha: 2022.01.18
10:20:25 +01'00'

Lluís Bellafont Álvaro

ICN2 General Manager

38499132F Digitally signed by
LUIS 38499132F LUIS
BELLAFONT (R: BELLAFONT (R:
G63277776) G63277776)
Date: 2022.01.18
11:42:51 +01'00'