1. SCOPE

This General Information Security Policy of the Universitat Politècnica de València (UPV) is applicable to all head and management offices, as well as agencies and campuses, including both its employees and students, as well as entities and professionals hired under other modalities when specified in their contracts.

2. PROTECTION OF INFORMATION

The UPV expressly recognises the importance of information and information systems, as well as the need for its protection, as a strategic and vital asset, to the point of endangering the continuity of the entity, or at least inflict significant damage if there is an irreversible loss of certain data. In addition, regarding personal data, - as it is established in Spanish legislation - and in defence of the interests of students, teaching staff and employees, suppliers, and other potentially affected persons.

The accesses and uses of the information, therefore, will be in line with what is indicated in the current policy and regulations, rules, standards and procedures of the UPV that arise from the same.

Employees and students (and users in general) must be at least aware of a summary of the policy, rules, regulations, standards and procedures, and must also be aware of the Security Document in regard to personal data in those aspects in which it affects them. In practice there should be a segregation of functions and an independent review of the operations or transactions made when necessary, from the records, on who is responsible for what, when and where. In anticipation of errors, omissions, fraud or crimes, and trying to detect the possible existence of anomalies as soon as possible, the dissemination of information and security training will also be promoted among employees and collaborators. Each function will only be able to perform the tasks and access the necessary data that are required to fulfil its task, that is, the principle of the so-called "minimum privilege" will be observed to avoid unauthorised access. Some of the risks against which adequate and reasonable controls - preventive, detective and corrective - should be established are: errors and omissions, sabotage, vandalism, industrial espionage, breach of privacy and data traffic, actions of other unauthorised external agents, and any others that may influence that the information is not accurate or complete, that is; in full, or is not available within the time established. The necessary and adequate means shall be established for the protection of persons, data, programmes, equipment, facilities, documentation and other media containing information, and in general of any UPV assets.
In the event of severance of the employee or contractor, he must hand in keys, access cards, UPV material, equipment and any type of information, and his user access codes will be deleted or blocked; in the case of a disciplinary severance, and if there were any suspicions, it will be investigated whether such person has been able to obtain copies, in paper or other means, of classified information, or has introduced unauthorised variations to computer programmes.

3.- PERSONAL DATA PROTECTION

A manager responsible for each file or database with personal data will be designated internally, who will be the one who will promote the establishment of controls and measures to protect the data under his responsibility.

4.- RESPONSIBILITIES

The responsibility on information security falls under the corresponding Management of the UPV centre, department, area, institute, service or unit in each case, that will establish the appropriate means, which does not prevent each employee or user from assuming his part of the responsibility for the means used, according to the points indicated in this policy, in the rules that develop it and the complementary procedures. Those who perform Information Security functions and other related management functions, will be those in charge of security.

5.- MONITORING AND CONTROL

Risk assessments should be carried out periodically and, depending on the weaknesses identified, it will be determined whether it is necessary to develop plans for the implementation or reinforcement of controls. The security review, although this is a concern to all, will fall under functions more related to internal control in the centres and departments, and information security and its correspondents or collaborators (by centres, departments, by campus...), and internal audit (of information systems), notwithstanding that an audit of external information systems may be contracted; the periodicity of reviews in critical systems should not exceed one year.

This policy will be specified and developed in a set of standards as well as through rules, guidelines, regulations and procedures, as the case may be, and as technology develops or the information spreads to different platforms or centres.