PASSWORD POLICY OF THE UNIVERSITAT POLITÈCNICA DE VALÈNCIA

1.-PURPOSE AND SCOPE.

Passwords are a key aspect of the security of IT resources, it is the first line of protection for the user. A poorly chosen or protected password can result in a security breach for the entire organisation. Therefore, all Universitat Politècnica de València (UPV) users are responsible for ensuring the security of their passwords for the use of the various services offered to the university community through UPVnet.

The security provided by a password depends on whether it is always kept secret. All the guidelines provided by this policy are intended to maintain this key feature in the passwords of the UPV resources. The main goal of this policy is to set a standard for creating strong passwords, protecting those passwords, and changing them frequently.

The scope of this policy includes all those users of the services and IT resources of the Universitat Politècnica de València who have or are responsible for an account (or any other type of access that requires a password) in any of the systems of the Universitat Politècnica de València.

2.- GENERAL POLICY

All account passwords that give access to resources and services of the Universitat Politècnica de València should follow the following general guidelines:

- All system passwords (root, NT administrators, application management accounts, etc.) must be changed at least once every six months.

- All user passwords (UPVnet accounts, email accounts, Web service accounts, etc.) must be changed at least once every twelve months. However, it is recommended to change the password more frequently and also whenever the user suspects that the security of his password may have been compromised.

- User accounts with system privileges through their group membership by any other means must have passwords different from the other accounts owned by that user in the UPV services and resources.

- Passwords should not be included in email messages, or any other electronic communication means. Passwords should neither be communicated in telephone conversations.

- Wherever possible, passwords will be automatically generated with the features recommended in this policy and users will be notified their password have "expired" to force the user to change it in the first use they make of the account or service.

- The default passwords associated with new systems or applications must be changed before these systems start to run. Those "default" accounts that are not essential will also be deactivated.

- All system and user passwords for UPV resources and services must comply with the recommendations described in this policy.

Some services in which it is critical to keep the security of the password will be able to determine additional measures of protection of the same.
3. PASSWORD SELECTION AND CUSTODY

3.1. General recommendations for the selection of passwords

Passwords are used with multiple purposes at the Universidad Politécnica de Valencia, such as passwords for UPVnet user accounts, system passwords for UPV resources, Web services, email accounts, screen savers in user resources, remote device management, etc...

**Particular attention must be paid to the selection of secure passwords for authentication in all UPV resources and services.**

The security of this type of authentication is based on two premises:

1. The personal password is only known to the user.
2. The password is strong enough not to be decrypted.

To be considered "strong" (secure), the password must have the following characteristics:

Must be at least 15 characters long.

It must contain characters from three of the following four groups, and SHALL ALWAYS INCLUDE A SYMBOL:

1. Lower-case.
2. Upper-case.
3. Numbers (for example, 1, 2, 3).
4. Symbols (i.e., !, @, Ñ, =, etc.).

- It must not be or derive from a word of the dictionary or the jargon or of a dialect.
- It must not derive from the name of the user or any close relative.
- It must not derive from personal information (the telephone number, identification number, ID number, date of birth, etc...) of the user or of a close relative.

In addition, passwords in UPVnet must comply with the following recommendations:

- It cannot contain 3 or more consecutive characters of the UPVnet username or the full name of the person.
- It may not have any blank spaces.

Finally, if you plan to travel abroad or use non-Spanish keyboards, keep in mind that the symbols you use in your password may be in different places on the keyboard; for example, do not use letters such as 'ñ' if you travel frequently and do not know how to enter it in non-Spanish keyboards.

Passwords should never be stored in writing. Try to create passwords that can easily be remembered. One way to do this is to create a password based on a sentence which is easy to remember:

For example:

The sentence: 'Waiter, can I have some fish?'
It suggests the password: 'Waiter, can I have some fish?'

3.2. Password protection recommendations

Do not use the same password you use for UPV resources and service accounts in other non-UPV accounts (access to your personal service provider, access to your bank's services, etc.).
Whenever possible, do not use the same passwords in different UPV accounts and services. For example, use different passwords for your UPVnet user and for your email services.

Do not share UPV accounts and passwords with anyone, including administrators, secretaries, etc... All passwords should be treated as sensitive and confidential information.

Here is a list of things **NOT** to do regarding the password:

- Do not reveal your password over the phone to ANYONE, even if they speak to you on behalf of the IT service or a senior person in the organisation.
- Do not reveal the password in e-mail messages or through any other means of electronic communication.
- Never write down the password on paper and store it. Also, do not store passwords in computer files unless you encrypt them or use a security mechanism.
- Do not reveal your password to your superiors, or your employees.
- Do not talk about a password in front of other people.
- Do not reveal your password in any questionnaire or form, regardless of the trust it may inspire.
- Do not share the password with family members.
- Do not reveal the password to your peers when you go on vacation.
- Do not use the "Remember Password" feature in some applications (Outlook, Netscape, Internet Explorer).

If someone asks you for the password, refer him to this document or ask him to refer to the Information and Communication Systems Area (ASIC) of the UPV. If you suspect that an account or your password may have been compromised, notify the ASIC and change the passwords for all your accounts.

Change passwords with the recommended frequency for each type of account and service.

### 3.3.- Application development standards

The developers of computer applications for the environment of the Universitat Politècnica de València and who manage their own mechanisms of authentication through passwords, should ensure that their programmes contain the following precautions in terms of security regarding the selection and use of passwords:

- They must support authentication of individual users, not groups.
- They should not store passwords in clear text or in any easily reversible form.
- They must provide some kind of role mechanism, so that a user can take on the functions of another without having to know the password of the former.
- They must provide a mechanism to expire the passwords and force the users to change them.
- The number of consecutive unsuccessful log in access attempts should be limited.

### 4.- MEASURES TO BE APPLIED

Failure to comply with this Policy may compromise the security of the entire corporate network of the Universitat Politècnica de València.

The **University Information Technology Committee** shall be in charge of establishing the measures to be taken in case of breach of this policy, and once the consequences of such violation may have had on the IT resources and services of the UPV are known.

Notwithstanding the disciplinary, administrative, civil and/or criminal actions that may be applicable to the persons allegedly involved in such breach.