Information Security Regulations for Suppliers

Issued by:

Published by:

Celulosa Fabril S.A.

Pol. Malpica C/E Parcela 5

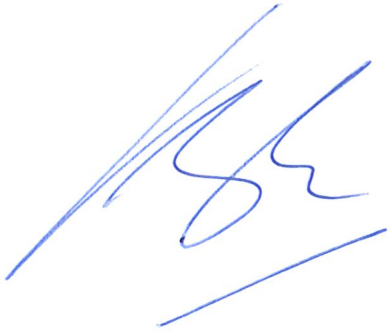
50.016 Zaragoza, España

Módulos Ribera Alta

Ctra. Nacional de Logroño, Km 27

50.639 Figueruelas, España

Version	Changes	Carried out by	Approved by	Date
A	Initial version of the document	Comité de Seguridad	Jorge Blanchard	01/09/2022



Índice

Índice **2**

1. Purpose 3
2. Scope 3
3. General guidelines 3
   - 3.1 Provision of the service 3
   - 3.2 Information confidentiality 4
   - 3.3 Intellectual property 5
   - 3.4 Exchange of information 5
   - 3.5 Appropriate use of resources 6
   - 3.6 Responsibilities of the user 7
   - 3.7 User equipment 8
   - 3.8 Hardware equipment management 8
4. Specific guidelines 9
   - 4.1 Scope of application 9
   - 4.2 Personnel selection procedure 10
   - 4.3 Security audit 11
   - 4.4 Incident reporting 11
   - 4.5 Physical security 11
   - 4.6 Asset management 12
   - 4.7 Security architecture 12
   - 4.8 System security 12
   - 4.9 Network security 14
   - 4.10 Traceability of use of systems 15
   - 4.11 Identity and access control and management 15
   - 4.12 Changes management 16
   - 4.13 Technical changes management 16
   - 4.14 Security in development 17
   - 4.15 Contingency management 17
5. Monitoring and control 18

1. Purpose

The purpose of this document is to establish the regulatory framework in relation to information security for CEFA/MRA's supplier organizations that access their information, information systems or resources, to protect their confidentiality, integrity, availability, authenticity and traceability.

To this end, the supplier organizations are responsible for informing their employees and subcontractors who provide services to CEFA/MRA.

2. Scope

All activities developed for CEFA/MRA by supplier organizations that access your information, information systems or resources.

Paragraph "3. General Guidelines" is applicable to any provider organization, regardless of the type of service provided.

Paragraph "4. Specific guidelines" is applicable exclusively to those provider organizations whose services provided correspond to the type of service indicated in each case, as indicated at the beginning of the aforementioned section.

3. General guidelines

3.1 Provision of the service

The supplier organizations may only carry out for CEFA/MRA those activities covered under the corresponding service provision contract.

The supplier organization will periodically provide CEFA/MRA with the list of people, profiles, functions, and responsibilities associated with the service provided, and will promptly inform of any change (registration, cancellation, replacement or change of functions or responsibilities) that occurs in said relationship.

In accordance with the provisions of the clauses associated with the contract for the provision of services, all external persons who carry out work for CEFA/MRA must comply with the safety regulations contained in this document. In case of non-compliance with any of these obligations, CEFA/MRA reserves the right of veto to the person who has committed the infringement, as well as the adoption of the sanctioning measures that are considered pertinent in relation to the supplier organization.

The provider organization must ensure that all its people have the appropriate training for the development of the service provided.

Any type of exchange of information that occurs between CEFA/MRA and the supplier organization will be understood to have been carried out within the framework established by the corresponding service provision contract, so that such information may not be used outside that framework or for other purposes.

IT Centralizes Global Efforts to Protect CEFA/MRA's Assets

Generically, assets include:

- Protected information, that is, information that allows the identification of natural and/or legal persons, and that relating to the configuration of information systems and communications networks.
- Partners for the processing of protected information (software, hardware, communications networks, information carriers, auxiliary equipment and facilities).

3.2 Information confidentiality

External persons who have access to CEFA/MRA information should consider that such information, by default, has the character of protected. Only information to which you have had access through the means of public dissemination of information provided for this purpose by CEFA/MRA may be considered as unprotected information

The disclosure, modification, destruction, or misuse of the information regardless of the medium in which it is located will be avoided.

The maximum reservation will be kept indefinitely and no protected information will be issued abroad, unless it is duly authorized.

The number of reports in paper format containing protected information will be minimized and kept in a safe place and out of the reach of third parties.

In the event that, for reasons directly related to the job, the employee of the supplier organization comes into possession of protected information contained in any type of support, he must understand that such possession is strictly temporary, with an obligation of secrecy and without this conferring any right of possession, ownership or copy over said information. Likewise, the employee must return the aforementioned media or supports, immediately after the completion of the tasks that have originated the temporary use of the same and, in any case, at the end of the relationship with CEFA/MRA of his company.

All these obligations will remain in force after the completion of the activities that external persons develop for CEFA/MRA

Failure to comply with these obligations may constitute an offence of disclosure of secrets.

To guarantee the security of personal data, the persons of the provider organization must observe the following rules of action, in addition to the considerations already mentioned:

- They will only be able to create files when it is necessary for the performance of their work. These temporary files will never be stored on local disk drives of the PC workstations of the users and must be destroyed when they are no longer useful for the purpose for which they were created.
- No personal data will be stored on the local disk drives of the PC workstations of the user.
- The exit of media and documents (including e-mails), outside the premises where this information is located, can only be authorized by CEFA/MRA and will be carried out according to the defined procedure.
- The media and documents must make it possible to identify the type of information they contain, be inventoried and stored in a place of restricted access to authorized persons.
- The transmission of specially protected personal data (e.g. Health), through telecommunications networks (e.g. Email) will be made by encrypting such data or using any

other mechanism that guarantees that the information is not intelligible or manipulated by third parties.

3.3 Intellectual property

Compliance with legal restrictions on the use of material protected by intellectual property regulations will be ensured.

Users may only use material authorized by CEFA/MRA for the development of their functions.

The use of computer programs without the corresponding license in CEFA/MRA's information systems is strictly prohibited.

Likewise, the use, reproduction, assignment, transformation or public communication of any type of work or invention protected by intellectual property without due written authorization is prohibited.

CEFA/MRA will only authorize the use of material produced by itself, or material authorized or supplied to it by its owner, in accordance with the agreed terms and conditions and the provisions of current regulations.

3.4 Exchange of information

No person shall conceal or manipulate his or her identity under any circumstances.

The distribution of information, whether in electronic or physical format, will be carried out through the resources determined in the contract for the provision of services for this purpose and for the exclusive purpose of facilitating the functions associated with said contract. CEFA/MRA reserves, depending on the risk identified, the implementation of control, registration and audit measures on these dissemination resources.

In relation to the exchange of information within the framework of the contract for the provision of services, the following activities shall be considered unauthorized:

- Transmission or receipt of material protected by copyright in violation of the Intellectual Protection Act.
- Transmission or receipt of all kinds of pornographic material, of a sexually explicit nature, racially discriminatory statements and any other kind of statement or message classifiable as offensive or illegal.
- Transfer of protected information to unauthorized third parties.
- Transmission or reception of non-business-related applications.
- Participation in Internet activities, such as newsgroups, games or others that are not directly related to the provision of the service.

All activities that may damage CEFA/MRA's image and reputation are prohibited on the Internet and elsewhere.

3.5 Appropriate use of resources

The supplier organization undertakes to periodically inform CEFA/MRA of the assets with which it provides the service.

The provider organization undertakes to use the resources available for the provision of the service in accordance with the conditions for which they were designed and implemented.

The resources that CEFA/MRA makes available to external persons, regardless of the type they are (computer, data, software, networks, communication systems, etc.), are available exclusively to fulfill the obligations and purpose of the operation for which they were provided. CEFA/MRA reserves the right to implement control and audit mechanisms that verify the appropriate use of these resources.

All equipment of the supplier organization that is connected to the CEFA/MRA production network will be of the approved brands and models. The supplier organisation shall make such equipment available to CEFA/MRA for the latter to coordinate the installation of the approved software and configure it appropriately.

Any file entered into the CEFA/MRA network or on any equipment connected to it through automated media, the Internet, email or any other means, must comply with the requirements established in these rules and, in particular, those referring to intellectual property, protection of personal data, and malware control.

All assets must be returned to CEFA/MRA, without undue delay, after the end of the contract. All personal computers to which CEFA/MRA has installed software will be taken to CEFA/MRA for formatting of the hard drive at the end of the service.

It is expressly forbidden:

- The use of resources provided by CEFA/MRA for activities unrelated to the purpose of the service.
- The connection to CEFA/MRA's production network of equipment and/or applications that are not specified as part of the software or standards of own computing resources.
- Introduce obscene, threatening, immoral or offensive content into CEFA/MRA's information systems or corporate network.
- Voluntarily introduce into CEFA/MRA's corporate network any type of malware (viruses, worms, Trojan horses, spyware, ransomware, ...), logical device, physical device, or any other type of sequence of orders that cause or are likely to cause any type of alteration or damage to computer resources. All persons with access to CEFA/MRA network will be required to use up-to-date anti-malware programs.
- Obtain without explicit authorization other rights or accesses other than those assigned to them by CEFA/MRA.
- Access without explicit authorization to restricted areas of CEFA/MRA's information systems
- Distort or falsify the logs of CEFA/MRA's information systems
- Decrypt without explicit authorization the keys, systems or encryption algorithms and any other security element that intervenes in CEFA/MRA's telematic processes
- Possess, develop or execute programs that could interfere with the work of other users, or damage or alter CEFA/MRA's computer resources
- Destroy, alter, disable or any other way of damaging data, programs or electronic documents with protected information (these acts may constitute a crime).
- Host protected information on the local disk drives of the user's PC workstations.

3.6 Responsibilities of the user

Service provider organizations shall ensure that all persons working for CEFA/MRA respect the following basic principles within their business:

- Each person with access to CEFA/MRA information is responsible for the activity carried out by their user identifier and everything derived from it. Therefore, it is essential that each person keeps under control the authentication systems associated with their user identifier, guaranteeing that the associated key is only known by the user himself, and should not be disclosed to the rest of the people under any circumstances.
- Users must not use any identifier of another user, even if they have the authorization of the owner.

  Users know and apply the existing requirements and procedures around the information handled.

Anyone with access to protected information should follow the following policies regarding password management:

- Select quality passwords, that is, difficult to guess by the rest of the users.
- Request the change of the password whenever there is a possible indication of knowledge on the part of other users.
- Change passwords at least once every 90 days and avoid reusing old passwords.
- Change default and temporary passwords at first login.
- Avoid including passwords in automated login processes (e.g. Those stored in browsers).
- Report any security incident related to your passwords such as loss, theft or indication of loss of confidentiality.

Anyone with access to protected information should ensure that equipment is protected when it is going to be neglected.

Anyone with access to protected information must respect at least the following clean desktop standards, in order to protect paper documents, computer media and portable storage devices and reduce the risks of unauthorized access, loss and damage to information, both during normal working hours and outside of it:

- Locked up paper documents and computer media when they are not being used, especially outside working hours.
- Block user sessions or turn off the PC when left unattended.
- Protect both the points of receipt and sending of information (postal mail, scanner and fax machines) and duplicate equipment (photocopier, fax and scanner). The reproduction or sending of information with this type of device will be under the responsibility of the user.
- Remove, without undue delay, any protected information once printed.
- Destroy protected information once it is not necessary.
- Persons with access to CEFA/MRA systems and/or information should never, without written authorization, perform tests to detect and/or exploit an alleged weakness, event or security incident.

- No person with access to CEFA/MRA systems and/or information will attempt without express written authorization by any means to violate the security system and authorizations. The capture of network traffic by users is prohibited, unless audit tasks authorized in writing are being carried out.

All persons who access the protected information must follow the following rules of action:

Protect protected information from unauthorized disclosure, modification, destruction, or misuse, whether accidental or not.

- Protect all information systems and telecommunications networks against unauthorized access or use, interruption of operations, destruction, misuse, or theft.
- Have the necessary authorization to obtain access to information systems and / or information.

3.7 User equipment

Service provider organizations shall ensure that all user-user computer equipment used to access protected information complies with the following standards:

- In the event of the user's inactivity, the equipment must be automatically blocked within a maximum period of 15 minutes.
- No user team will have tools that can transgress security systems and authorizations.
- User equipment will be maintained according to the manufacturer's specifications.
- All user computers will be adequately protected against malware:
  - Antimalware software should be installed and used on all personal computers to reduce the operational risk associated with viruses or other malicious software.
  - They will keep up to date with the latest security updates available.
  - Antimalware software must always be enabled and up to date.

Particular care shall be taken to ensure the security of all mobile user computers containing or accessing it in any way:

- Verifying that they do not include more information than is strictly necessary.
- Ensuring that access controls are in place for such information.
- Minimizing access to such information in the presence of people outside the service provided.
- Transporting the equipment in covers, briefcases or similar equipment that incorporates the appropriate protection against environmental agents

3.8 Hardware equipment management

Service provider organizations shall ensure that all equipment provided by CEFA/MRA for the provision of services, regardless of the type of service, is properly managed. To do this, they must comply with the following rules:

- The supplier organization must maintain an up-to-date list of equipment provided by CEFA/MRA and users of such assets or associated responsible persons in case the assets are not for single-person use. Such a relationship may be required by CEFA/MRA.
- Whenever a supplier organization wants to reassign any CEFA/MRA equipment that contains protected information, it must return it temporarily so that the necessary secure erasure procedures can be carried out prior to its reassignment.
- In the event that a supplier organization wishes to proceed to unsubscribe from the list of CEFA/MRA equipment received by any of them, it must always return them, so that CEFA/MRA can treat said cancellation appropriately.
- In the event that a supplier organization ceases to provide the service, it must return to CEFA/MRA the entire list of equipment received, as established in the corresponding contracts for the provision of services. Only in the case of paper documents and computer media can the supplier organization proceed to their secure deletion, in which case it must notify CEFA/MRA of such deletion.

4. Specific guidelines

4.1 Scope of application

All supplier organisations must comply, in addition to the general rules, with the specific rules set out in this paragraph that correspond to them in each case, depending on the characteristics of the service provided to CEFA/MRA

The types of service contemplated are those indicated below.

- Place of execution of the service: Depending on the main place where the services are developed, two cases are distinguished:
    - CEFA/MRA: The supplier organization provides the service mainly from CEFA/MRA's own headquarters.
    - Remote: The supplier organization provides the service mainly from its own dependencies, although specific activities can be carried out at CEFA/MRA's headquarters.
- Ownership of the ICT infrastructures used: Depending on who owns the main ICT infrastructures (communications, user equipment, software) used to provide the service, two cases are distinguished:
    - CEFA/MRA
    - Producer organization.
- Level of access to CEFA/MRA systems: Depending on the level of access to CEFA/MRA information systems, three cases are distinguished:
    - With privileged access: The service provided requires privileged access to CEFA/MRA's information systems, with the capacity to manage these systems and/or the production data they process.
    - With user-level access: The service provided requires the use of CEFA/MRA's information systems, so that the people who provide the service have user accounts that allow them to access any of these systems with usual privileges.
    - No access: The service provided does not require the use of CEFA/MRA's information systems, so that the people who provide the service do not have user accounts in said systems.

Depending on each of the three categories in which each service is framed, the provider organization must comply, in addition to the general safety standards, the specific ones contained in the sections indicated in the following table:

	PLACE		*INFRASTRUCTURE*		*ACCESS*		
	CEFA/ MRA	*Remote*	*CEFA/MR A*	*Supplier organization*	*Privileged*	*Normal*	*No access*
selection of people	NO	NO	NO	NO	YES	NO	NO
security audit	NO	NO	NO	NO	YES	NO	NO
incident reporting	YES	YES	YES	NO	YES	YES	NO
physical security	NO	YES	NO	NO	NO	NO	NO
asset management	NO	NO	NO	YES	NO	NO	NO
security architecture	NO	NO	NO	YES	YES	YES	NO
security systems	NO	NO	NO	YES	NO	NO	NO
network security	NO	NO	NO	YES	NO	NO	NO
traceability of use of the systems	NO	NO	NO	YES	YES	NO	NO
identity and access control and management	NO	NO	NO	YES	NO	NO	NO
change management	NO	NO	NO	YES	YES	YES	NO
technical change management	NO	NO	NO	NO	YES	NO	NO
security in development	NO	NO	NO	NO	YES	YES	NO
Contingency management	NO	NO	NO	YES	NO	NO	NO

4.2 Personnel selection procedure

The supplier organization must verify the professional background of the persons assigned to the service, guaranteeing CEFA/MRA that in the past it has not been sanctioned for professional malpractice or has been involved in incidents related to the confidentiality of the information processed that have led to any type of sanction.

The supplier organization must guarantee CEFA/MRA the possibility of immediate withdrawal of the persons assigned to the service of any person in relation to whom CEFA/MRA wishes to exercise the right of veto, in accordance with the conditions established in section "3.1. Provision of the service".

4.3 Security audit

The supplier organization must allow CEFA/MRA to carry out the requested security audits, collaborating with the audit team and providing all the evidence and records required.

The scope and depth of each audit will be expressly established by CEFA/MRA in each case. The audits will be carried out following the planning that is agreed in each case with the organization providing the service.

CEFA/MRA reserves the right to carry out additional extraordinary audits, provided that there are specific reasons that justify it.

4.4 Incident reporting

When a vulnerability, event and / or information security incident is detected, it must be notified immediately through the email box seguridad.info@cefa.es.

Any user can transfer through the aforementioned mailbox those events, suggestions, vulnerabilities, ... which may relate to the security of the information and the guidelines referred to in these rules of which it is aware.

Any incident that is detected and that affects or may affect the security of personal data (e.g., Loss of lists and / or computer supports, suspicions of improper use of access authorized by other people, recovery of data from backups, ...).

The aforementioned mailbox centralizes the collection, analysis and management of the notified incidents.

If the mailbox is not accessed, the communication channels established within the service itself must be used, so that it is the CEFA/MRA interlocutor who communicates the security incident.

4.5 Physical security

The headquarters must be closed and must have an access control system.

There will be some type of control of visits, at least in areas of public access and / or loading and unloading.

The headquarters shall have at least adequate fire detection and extinguishing systems and shall be constructed in such a way as to provide sufficient resistance to flooding.

If any type of backup is maintained, the systems that house and/or process such information must be located in a specially protected area, which includes at least the following security measures:

- The specially protected area must have an access control system independent of that of the headquarters.
- Access to specially protected areas will be limited to outsiders. This access will be assigned only when necessary and authorized, and always under the supervision of authorized persons.
- A record of all access by outsiders will be kept.

- Outsiders may not stay or carry out work in specially protected areas without supervision.
- The consumption of food or beverages in these specially protected areas will be prohibited.
- Systems located in these areas must have some type of protection against power failures.

4.6 Asset management

The provider organization shall have an up-to-date asset register in which the assets used for the provision of the service can be identified.

All assets used for the provision of the service must have a responsible person, who must ensure that these assets incorporate the minimum-security measures established by the provider organization, and that at least they must be those specified in these regulations.

The supplier organization shall notify CEFA/MRA of the withdrawal of the assets used for the provision of the service. If such asset contains another property of CEFA/MRA (hardware, software or other assets), it must be delivered to CEFA/MRA prior to carrying out the cancellation in order for CEFA/MRA to proceed with the withdrawal of the assets of its property.

Whenever an asset has contained protected information, the provider organization shall carry out asset write-offs by ensuring the secure deletion of such information, applying secure erasure functions, or physically destroying the asset, so that the information contained therein cannot be recoverable.

4.7 Security architecture

Whenever the service provider organization carries out application development and/or testing work for CEFA/MRA or with protected information, the environments with which such activities are carried out shall be isolated from each other and isolated from the production environments in which protected information is hosted or processed.

All access to information systems that host or process protected information must be protected, at least, by a firewall, which limits the ability to connect to them.

Information systems hosting or processing particularly sensitive information shall be isolated from the rest.

4.8 System security

Information systems hosting or processing protected information shall record the most significant events surrounding their operation. These activity logs will be covered by the backup regulations of the provider organization.

The clocks of the provider organization's systems that process or host protected information will be synchronized with each other and with the official time.

The organization providing the service shall ensure that the capacity of the information systems that store or process protected information is properly managed, avoiding potential shutdowns or malfunctions of such systems due to resource saturation.

Information systems that host or process protected information shall be adequately protected against malicious software, applying the following precautions:

- Systems will keep up to date with the latest security updates available, in the development, test and production environments.
- Anti-malware software should be installed and used on all servers and personal computers to reduce the risk associated with malware.
- Anti-malware software must always be enabled and up to date.

The provider organization will establish a backup regulation that guarantees the safeguarding of any data or information relevant to the service provided, on a weekly basis.

Whenever email is used in relation to the service provided, the provider organization must respect the following premises:

- The transmission via email of protected information will not be allowed unless the electronic communication is encrypted and the shipment is authorized in writing.
- The transmission via email of information containing specially protected personal data (e.g., Health), unless the electronic communication is encrypted and the shipment is authorized in writing.
- Whenever CEFA/MRA's email address is used for the provision of the service, at least the following principles must be respected:
- Email will be considered as another work tool provided for the exclusive purpose of the contracted service. This consideration will empower CEFA/MRA to implement control systems aimed at ensuring the protection and proper use of this resource. This power, however, shall be exercised while safeguarding the dignity of persons and their right to privacy.
- CEFA/MRA's email system should not be used to send fraudulent, obscene, threatening, or other similar messages.
- Users must not create, send, or forward advertising or pyramidal messages (messages that extend to multiple users).

Access to information systems hosting or processing protected information must always be done in an authenticated manner, at least by using a person identifier and an associated password.

Information systems that host or process protected information must have access control systems that limit access to such information exclusively to persons in the service.

Access sessions to information systems that host or process protected information should be automatically blocked after a certain amount of downtime of users.

Whenever software provided by CEFA/MRA is used, the following rules must be met:

- All persons accessing CEFA/MRA's information systems must use only the software versions provided and following their rules of use.
- Everyone is prohibited from installing illegal copies of any software.
- The use of software not validated by CEFA/MRA is prohibited.
- It is also forbidden to uninstall any of the programs installed by CEFA/MRA.

4.9 Network security

The networks through which the protected information circulates shall be adequately managed and controlled, ensuring that there is no uncontrolled access or connections whose risks are not properly managed by the providing organization.

The services available on the networks through which the protected information circulates should be limited as far as possible.

The networks that allow access to CEFA/MRA's ICT infrastructure must be adequately protected, and the following premises must be met:

- The access of remote users to the CEFA/MRA network will be subject to compliance with identification and prior authentication procedures, and validation of access.
- These connections will be made for a limited time and through the use of virtual private networks or dedicated lines.
- In these connections, no type of communications equipment (cards, modems, etc.) that allows uncontrolled alternative connections will be allowed.

Access to the networks through which the protected information circulates shall be limited.

All equipment connected to the networks through which the protected information circulates shall be appropriately identified so that network traffic can be identified.

Teleworking, considered as access to the corporate network from abroad, is regulated by the application of the following regulations:

- The use of equipment not controlled by CEFA/MRA for teleworking activities is not allowed.
- Criteria for authorizing teleworking will be established based on the needs of the job.
- The necessary measures will be established for the secure connection to the corporate network.
- Security monitoring and auditing systems will be established for established connections.
- The revocation of access rights and return of equipment after the end of the period of need for it will be controlled.

Whenever the Internet access provided by CEFA/MRA is used, the following regulations must also be respected:

- The Internet is a working tool. All activities on the Internet must be in relation to tasks and work activities. Users should not search for or visit sites that do not serve as support for CEFA/MRA's business objective or the fulfilment of their daily work.
- Access to the Internet from the corporate network will be restricted by means of control devices incorporated in it. The use of other means of connection must be previously validated and will be subject to the above considerations on the use of the Internet.
- Users must not use the name, symbol, logo or symbols similar to that of CEFA/MRA in any element of the Internet (email, Web pages, etc.) not justified by strictly work activities.
- The transfer of data to or from the Internet will only be permitted when it is related to business activities. The transfer of files not related to these activities (e.g., Downloading programs, multimedia files, ...) shall be prohibited:

4.10 Traceability of use of systems

Privileged accesses will be recorded, and these records will be kept in accordance with the Organization's backup regulations.

The activity of the systems used to carry out said privileged access will be recorded, keeping these records in accordance with the organization's backup regulations.

The errors and failures registered in the activity of the systems will be analysed, adopting the necessary measures for their correction.

4.11 Identity and access control and management

All users with access to an information system will have a single access authorization composed of a user id and password.

Users will be responsible for all activities related to the use of their authorized access.

Users must not use any authorized access of another user, even if they have the authorization of the owner.

Users must not disclose under any circumstances their identifier and / or password to another person, or keep it in writing in sight, or available to third parties.

The minimum length of the password must be 6 characters and must not contain the name, surname, or identifier of the user in it. It must be changed every 45 days or repeat at least the previous 8 passwords.

Likewise, they must have complexity and be difficult to guess, so they will be constituted by combination at least 3 of these 4 options in the first 8 characters:

- Capital letters
- Lowercase
- Numbers
- Special characters

We recommend that you use the following guidelines for selecting passwords:

- Do not use familiar words, or words that can be associated with oneself, for example, the name.
- The password must not refer to any recognizable concept, object, or idea. Therefore, you should avoid using significant dates, days of the week, months of the year, names of people, telephones, ...
- The key should be something virtually impossible to guess. But at the same time, it should be easily remembered by the user. A good example is to use the acronym of some phrase or expression.

The provider organization shall ensure that it is regularly found that only persons duly authorised to do so have access to the protected information.

In those cases in which CEFA/MRA's information systems are also accessed, the following regulations must also be considered:

- No user will receive an access identifier to CEFA/MRA's systems until they accept in writing the current security regulations.
- Users will have authorized access only to those data and resources that they need for the development of their functions.
- In case the system does not request it automatically, the user must change the provisional password assigned the first time he makes a valid access to the system.
- In the event that the system does not request it automatically, the user must change their password at least once every 90 days.
- Temporary authorized access will be configured for a short period of time. Once this period has expired, they will be deactivated from the systems.
- In relation to personal data, only the persons authorized to do so may grant, alter or cancel the authorized access to the data and resources, in accordance with the criteria established by the person responsible for the file.
- If a user suspects that their authorized access (user ID and password) is being used by another person, they must change their password and notify the incident in the email box seguridad.info@cefa.es.

4.12 Changes management

All changes to the ICT infrastructure must be controlled and authorized, ensuring that uncontrolled components are not part of it.

It must be verified that all the new components introduced in the ICT infrastructure of the provider organization used for the provision of the service function properly and fulfil the purposes for which they were incorporated.

4.13 Technical changes management

All changes that are made must be made following a formally established and documented procedure, which ensures that the appropriate steps are followed to make the change.

The change management procedure should ensure that changes to the ICT infrastructure are minimised, limiting themselves to those that are strictly essential.

All changes should be tested prior to deployment in the production environment to verify that there are no adverse or unforeseen spillover effects on the operation and security of the ICT infrastructure.

The supplier organizations must scan and mitigate the technical vulnerabilities presented by the infrastructures used for the provision of the service, informing CEFA/MRA of all those associated with the critical components.

4.14 Security in development

The entire outsourced software development process will be controlled and supervised by CEFA/MRA

Mechanisms for identification, authentication, access control, auditing and integrity will be incorporated throughout the life cycle of design, development, implementation and operation of the software.

The specifications of the software must expressly contain the security requirements to be covered in each case.

The software to be developed should incorporate input data validations that verify that the data is correct and appropriate and that prevents the introduction of executable code.

The internal processes developed by the applications must incorporate all the necessary validations to ensure that no corruption of the information occurs.

Whenever necessary, authentication and integrity control functions should be incorporated into the communications between the different components of the applications.

The output information offered by the applications must be limited, ensuring that only the relevant and necessary information is offered.

Access to the source code of the applications must be limited to the people of the service.

Actual data shall only be used in the test environment when it has been appropriately dissociated or provided that it can be ensured that the security measures applied are equivalent to those in the production environment.

During the tests of the applications, it will be verified that there are no uncontrolled information gaps, and that only the planned information is offered through the established channels.

Only software that has been expressly approved will be transferred to the production environment.

In relation to Web services, the management of the OWASP Top 10 will be considered.

4.15 Contingency management

The service must have a plan that allows its provision even in case of contingencies.

The above plan should be developed based on the events capable of causing interruptions in the service and their probability of occurrence.

The supplier organization shall be able to demonstrate the viability of the existing contingency plan.

5. Monitoring and control

In order to ensure the correct use of the aforementioned resources, through the formal and technical mechanisms deemed appropriate, CEFA/MRA will check, either periodically or when for specific security or service reasons it is convenient.