LORIOT EXTERNAL CODE

Version 0	12-9-2022	Approved by Information Security Officer & Quality Officer
Version 1	02-8-2023	Yearly review - Point 4.11 amended
Version 2	11-7-2024	Yearly review
Version 3	30-5-2025	Yearly review

Shared with: all stakeholders / LORIOT webpage

1. Purpose

The purpose of this document is to establish the information security policy framework for LORIOT AG (or any other LORIOT AG subsidiaries), hereinafter the “LORIOT” provider organisations accessing their information, information systems or resources, in order to protect their confidentiality, integrity and availability.

To this end, supplier organisations are responsible for informing their employees and subcontractors providing services to LORIOT.

2. Scope

All activities carried out for LORIOT by supplier organisations accessing its information, information systems or resources.

General guidelines’ is applicable to any provider organisation, regardless of the type of service provided.

Specific guidelines' is applicable only to those provider organisations whose services provided correspond to the type of service indicated in each case, as indicated at the beginning of that section.

3. General guidelines

3.1. Service provision

Supplier organisations may only perform for LORIOT those activities covered under the corresponding service provision contract.

The provider organisation shall periodically provide LORIOT with the list of persons, profiles, functions and responsibilities associated with the service provided, and shall promptly inform LORIOT of any change (registration, cancellation, substitution or change of functions or responsibilities) that may occur in this list.

In accordance with the provisions of the clauses associated with the contract for the provision of services, all external persons performing work for LORIOT must comply with the safety standards set out in this document. In case of non-compliance with any of these obligations, LORIOT reserves the right to veto the person who has committed the infraction, as well as the adoption of the sanctioning measures considered pertinent in relation to the provider organisation.

The provider organisation shall ensure that all its personnel have the appropriate training for the performance of the service provided.

Any exchange of information between LORIOT and the provider organisation shall be understood to have taken place within the framework established by the relevant service provision contract, so that such information may not be used outside this framework or for other purposes.

Systems centralises the global efforts to protect LORIOT's assets.

Generically, assets include:

- Protected information, i.e. information identifying natural and/or legal persons, and information concerning the configuration of information systems and communications networks.
- Those associated with the processing of protected information (software, hardware, communications networks, data carriers, auxiliary equipment and installations).

3.2. Confidentiality of information

External persons who have access to LORIOT information should consider that such information is, by default, protected information. Only information to which access has been obtained through the means of public dissemination of information provided for this purpose by LORIOT may be considered as unprotected information.

The disclosure, modification, destruction or misuse of information, whatever its medium, shall be prevented.

Maximum confidentiality shall be maintained indefinitely and no protected information shall be released to the outside world unless duly authorised.

The number of paper reports containing protected information shall be minimised and they shall be kept in a secure place out of reach of third parties.

In the event that, for reasons directly related to the job, the employee of the provider organisation comes into possession of protected information contained in any type of support, it must be understood that such possession is strictly temporary, with an obligation of secrecy and without this conferring any right of possession, ownership or copy of said information. Likewise, the employee must return the aforementioned media immediately upon completion of the tasks that have given rise to the temporary use of the same and, in any case, upon termination of the relationship with LORIOT of his or her company.

All these obligations shall continue after the termination of the outsiders' activities for LORIOT.

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

In order to ensure the security of personal data, persons within the provider organisation shall observe the following rules of conduct in addition to the above-mentioned considerations:

- They may only create files when necessary for the performance of their work. These temporary files shall never be saved on the local disk drives of users' PC workstations and shall be destroyed when they are no longer useful for the purpose for which they were created. No personal data shall be stored on the local disk drives of user PC workstations.
- The output of media and documents (including the sending of e-mails), outside the premises where such information is located, may only be authorised by LORIOT and shall be carried out in accordance with the defined procedure.
- The media and documents shall be capable of identifying the type of information they contain, shall be inventoried and stored in a place to which access is restricted to authorised persons.

- The transmission of specially protected personal data (e.g. health) through telecommunications networks (e.g. electronic mail) shall be carried out by encrypting such data or using any other mechanism that guarantees that the information cannot be intelligible or manipulated by third parties.

3.3. Intellectual property

Compliance with legal restrictions on the use of material protected by copyright law shall be ensured.

Users may only use material authorised by LORIOT for the performance of their duties.

The use of unlicensed software on LORIOT information systems is strictly prohibited.

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

LORIOT shall only authorise the use of material produced by itself, or material authorised or supplied to it by its owner, in accordance with the agreed terms and conditions and the provisions of the regulations in force.

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 by means of the resources determined in the service provision contract for such purpose and for the exclusive purpose of facilitating the functions associated with such contract. LORIOT reserves, depending on the identified risk, the implementation of control, registration and audit measures on these dissemination resources.

In relation to the exchange of information within the framework of the service provision contract, the following activities shall be considered as unauthorised:

- Transmission or reception of copyrighted material in violation of the Copyright Act.
- Transmission or receipt of any kind of pornographic material, sexually explicit material, racially discriminatory statements and any other statement or message that could be classified as offensive or illegal.
- Transfer of protected information to unauthorised third parties.
- Transmission or reception of non-business related applications.
- Participation in Internet activities such as newsgroups, games or other activities not directly related to the provision of the service.

All activities that may damage the image and reputation of LORIOT are prohibited on the Internet and elsewhere.

3.5. Appropriate use of resources

The provider organisation undertakes to periodically inform LORIOT of the assets with which it provides the service.

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

The resources that LORIOT makes available to external parties, regardless of their type (IT, data, software, networks, communication systems, etc.), are available exclusively to fulfil the obligations and purpose of the operation for which they were provided. LORIOT reserves the right to implement control and audit mechanisms to verify the appropriate use of these resources.

All equipment of the supplier organisation connected to the LORIOT production network shall be of approved makes and models. The supplier organisation shall make such equipment available to LORIOT to coordinate the installation of the approved software and configure it appropriately.

Any file introduced in the LORIOT network or in any equipment connected to it through automated media, Internet, electronic mail or any other means, must comply with the requirements established in these rules and, in particular, those referring to intellectual property, personal data protection and malware control.

All assets shall be returned to LORIOT without undue delay after the end of the contract. All personal computers on which LORIOT has installed software shall be taken to LORIOT to have the hard disk formatted at the end of the service.

It is expressly prohibited:

- The use of resources provided by LORIOT for activities not related to the purpose of the service.
- The connection to the LORIOT production network of equipment and/or applications that are not specified as part of the software or standards of the company's own IT resources.
- Introducing obscene, threatening, immoral or offensive content into LORIOT's information systems or corporate network.
- Voluntarily introducing into the corporate network of LORIOT any type of malware (virus, worms, Trojans, spyware, ransomware, ...), logical device, physical device or any other type of sequence of commands that cause or are likely to cause any type of alteration or damage to computer resources. All persons with access to the LORIOT network shall be obliged to use up-to-date anti-malware software.
- Obtain without explicit authorisation rights or access other than those assigned to them by LORIOT.
- Accessing restricted areas of LORIOT information systems without explicit authorisation.
- Distort or falsify the log records of LORIOT's information systems.
- Decrypting without explicit authorisation the encryption keys, systems or algorithms and any other security elements involved in LORIOT telematic processes.
- Possess , develop or run programs that could interfere with the work of other users, or damage or alter the computer resources of LORIOT.

- Destroying, altering, disabling or otherwise damaging electronic data, programs or documents containing protected information (these acts may constitute a criminal offence).
- Store protected information on the local disk drives of the user PC workstations.

3.6. User responsibilities

Service provider organisations shall ensure that all persons performing work for LORIOT respect the following basic principles within their activity:

- Each person with access to LORIOT information is responsible for the activity carried out by his or her user ID and all that derives from it. Therefore, it is essential that each person maintains control of the authentication systems associated with their user identifier, ensuring that the associated password is only known by the user and must not be disclosed to others under any circumstances.
- Users shall not use any identifier belonging to another user, even if they have the owner's authorisation.
- Users are aware of and apply existing requirements and procedures regarding the information handled.

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

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

Anyone with access to protected information must ensure that equipment is protected when it is to be left unattended.

Anyone with access to protected information should adhere to at least the following clean desk rules, in order to protect paper documents, computer media and portable storage devices and to reduce the risks of unauthorised access, loss and damage to information, both during and outside normal working hours:

- Lock up paper documents and IT equipment when they are not in use, especially outside working hours.
- Block user sessions or shut down the PC when left unattended.
- Protect both the points for receiving and sending information (postal mail, scanner and fax machines) and the duplication equipment (photocopier, fax and scanner). The reproduction or sending of information with this type of device is the responsibility of the user.
- Remove, without undue delay, any protected information once printed.
- Destroy protected information once it is no longer needed.

- Persons with access to LORIOT systems and/or information shall never, without written authorisation, conduct tests to detect and/or exploit a suspected security weakness or incident.
- No person with access to LORIOT systems and/or information shall, without express written authorisation, attempt by any means to breach the security system and authorisations. The capture of network traffic by users is prohibited, except in the case of auditing tasks authorised in writing.

All persons accessing protected information must follow the following rules of conduct:

- Protect protected information from unauthorised disclosure, modification, destruction or misuse, whether accidental or not.
- Protect all information systems and telecommunications networks against unauthorised access or use, disruption of operations, destruction, misuse, or theft.
- Having the necessary authorisation to obtain access to information systems and/or information.

3.7. User team

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

- In the event of inactivity by the user, the equipment shall be automatically blocked within a maximum period of 15 minutes.
- No user equipment shall have any tools that could breach security systems and authorisations.
- User equipment shall be maintained according to the manufacturer's specifications.
- All user equipment shall be adequately protected against malware:
    - Anti-malware software should be installed and used on all personal computers to reduce the operational risk associated with viruses or other malicious software.
    - Be kept up to date with the latest security updates available.
    - Anti-malware software should always be enabled and up to date.

Particular care shall be taken to ensure the security of all user mobile equipment containing or otherwise accessible to protected information:

- Verifying that they do not include more information than is strictly necessary.
- Ensuring that access controls are applied to such information.
- Minimising access to this information in the presence of persons not involved in the service provided.
- Transporting equipment in cases, or similar equipment incorporating appropriate protection against environmental agents.

3.8. Management of hardware equipment

Service provider organisations shall ensure that all equipment provided by LORIOT for the provision of services, regardless of its type, is properly managed. To this end, they shall comply with the following standards:

- The provider organisation shall maintain an updated list of equipment provided by LORIOT and persons using such assets, or associated responsible persons in case the assets are not for single person use. This list may be requested by LORIOT.
- Whenever a provider organisation wishes to reassign any LORIOT equipment that has contained protected information, it must temporarily return it so that the necessary secure deletion procedures can be carried out prior to reassignment.
- In case a provider organisation wants to remove any of the received LORIOT equipment from the list of LORIOT equipment, it must always return it, so that LORIOT can treat the removal appropriately.
- In the event that a provider organisation ceases to provide the service, it must return to LORIOT the entire list of equipment received, as stipulated in the relevant service provision contracts. Only in the case of paper documents and computer media may the provider organisation securely dispose of them, in which case it must notify LORIOT of such disposal.

4. Specific guidelines

4.1. Scope of application

All supplying organisations shall comply, in addition to the general rules, with the specific rules set out in this section that apply to them in each case, depending on the characteristics of the service provided to LORIOT.

The types of service envisaged are as follows.

- Place of performance of the service, depending on the main place where the services are performed, a distinction is made between two cases:
- LORIOT: The service is provided by the provider organisation mainly from LORIOT's own headquarters.
- Remote: The provider organisation provides the service mainly from its own premises, although occasional activities may be carried out at the LORIOT site.

- 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 can be distinguished:
- LORIOT.
- Providing organisation.

- Level of access to LORIOT systems, depending on the level of access to LORIOT information systems, three cases are distinguished:
- With privileged access: The service provided requires privileged access to LORIOT's information systems, with the ability to administer those systems and/or the production data they process.
- With user level access: The service provided requires the use of LORIOT's information systems, so that the persons providing the service have user accounts that allow them to access some of these systems with regular privileges.

- No access: The service provided does not require the use of LORIOT information systems, so the persons providing the service do not have user accounts on those systems.

Depending on each of the three categories into which each service falls, the provider organisation must comply, in addition to the general safety standards, with the specific standards set out in the sections indicated in the following table:

	LOCATION		*INFRASTRUCTURE*		*ACCESS*		
	LORIOT	*Remote*	*LORIOT*	*Provider organisation*	*Privileged*	*Normal*	*No access*
selection of persons	NO	NO	NO	NO	YES	NO	NO
security audit	NO	NO	NO	NO	YES	NO	NO
communication of incidents	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 the 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. Selection of people

The provider organisation shall verify the professional background of the employee assigned to the service, guaranteeing LORIOT that they have not been sanctioned in the past for professional malpractice nor have they been involved in incidents related to the confidentiality of the information processed that have led to any type of sanction.

The provider organisation shall guarantee LORIOT the possibility of immediate removal from the persons assigned to the service of any person in relation to whom LORIOT wishes to exercise the right of veto, in accordance with the conditions set out in section "3.1.".

4.3. Security audit

The supplier organisation shall allow LORIOT to carry out the requested safety audits, cooperate with the audit team and provide all evidence and records requested.

The scope and depth of each audit will be expressly established by LORIOT in each case. The audits shall be carried out according to a schedule to be agreed in each case with the service provider organisation.

LORIOT reserves the right to conduct additional extraordinary audits, provided that there are specific grounds for doing so.

4.4. Reporting of incidents

When you detect any information security incident, you must notify us immediately via the e-mail address **security@loriot.io**.

Any user may use the aforementioned mailbox to report any events, suggestions, vulnerabilities, etc. that may be related to information security and the guidelines contemplated in these rules of which they are aware.

Any incident detected that affects or may affect the security of personal data (e.g. loss of lists and/or computer media, suspicion of improper use of authorised access by other persons, recovery of data from backup copies, etc.) must be notified through the aforementioned mailbox.

This mailbox centralises the collection, analysis and management of the incidents received.

If access to the mailbox is not available, the communication channels established within the service itself should be used, so that the LORIOT interlocutor is the one to communicate the security incident.

4.5. Physical security

The venue shall be locked and shall have some form of access control system.

There shall be some form of visitor control, at least in areas of public access and/or loading and unloading.

The site shall at least have adequate fire detection and fire extinguishing systems and shall be constructed in such a way as to be sufficiently resistant to flooding.

If any backup is maintained, the systems hosting and/or processing such information shall be located in a specially protected area, which includes at least the following security measures:

- The specially protected area shall have an access control system independent of that of the headquarters.
- Access to specially protected areas by outsiders shall be limited. Such access shall be granted only when necessary and authorised, and always under the supervision of authorised persons.
- A record shall be kept of all access by outsiders.
- Outsiders may not remain or carry out work in the specially protected areas without supervision.
- The consumption of food or drink in these specially protected areas shall be prohibited.
- Systems located in these areas shall have some form of power failure protection.

4.6. Asset management

The provider organisation 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 shall have a responsible person, who shall ensure that such assets incorporate the minimum security measures established by the provider organisation, which shall at least be those specified in this regulation.

The Provider Organisation shall notify LORIOT of the decommissioning of assets used for the provision of the service. If the asset contains other LORIOT property (hardware, software or other assets), it must be handed over to LORIOT prior to the decommissioning in order for LORIOT to proceed with the removal of the assets owned by LORIOT.

Whenever an asset has contained protected information, the provider organisation shall carry out asset retirement by ensuring the secure disposal of such information, either by applying secure deletion functions or by physically destroying the asset, so that the information contained therein cannot be recovered.

4.7. Security architecture

Whenever the service provider organisation carries out development and/or testing of applications for LORIOT or with protected information, the environments in which such activities are carried out shall be isolated from each other and also isolated from production environments in which protected information is housed or processed.

All access to information systems hosting or processing protected information shall be protected at least by a firewall, which limits the ability to connect to them.

Information systems housing or processing particularly sensitive information shall be isolated from other information systems.

4.8. System security

Information systems that host or process protected information shall record the most significant events surrounding their operation. These activity logs shall be covered by the provider organisation's backup policy.

The clocks of the provider organisation's systems that process or host protected information shall be synchronised with each other and with the official time.

The service provider organisation shall ensure that the capacity of information systems storing or processing protected information is adequately managed, avoiding potential downtime or malfunctioning of such systems due to resource saturation.

Information systems hosting or processing protected information shall be adequately protected against malicious software by applying the following precautions:

- Systems will be kept up to date with the latest security updates available, in 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 malicious software.
- Anti-malware software should always be enabled and up to date.

The provider organisation shall establish a backup policy to ensure the safeguarding of any data or information relevant to the service provided, on a weekly basis.

Whenever e-mail is used in connection with the service provided, the provider organisation shall respect the following premises:

- The transmission via e-mail of protected information shall not be permitted unless the electronic communication is encrypted and the transmission is authorised in writing.
- The transmission via e-mail of information containing specially protected personal data (e.g. health) is not permitted, unless the electronic communication is encrypted and the transmission is authorised in writing.

Whenever LORIOT e-mail is used for the provision of the service, at least the following principles must be respected:

- E-mail will be considered as another work tool provided for the exclusive purpose of the contracted service. This consideration will empower LORIOT to implement control systems aimed at ensuring the protection and proper use of this resource. This power shall, however, be exercised in a manner that safeguards the dignity of individuals and their right to privacy.
- The LORIOT e-mail system shall not be used to send fraudulent, obscene, threatening or otherwise similar communications.
- Users shall not create, send or forward advertising or pyramid messages (messages that are spread to multiple users).
- Access to information systems housing or processing protected information must always be authenticated, at least by using a person identifier and an associated password.
- Information systems that house or process protected information shall have access control systems that limit access to such information to service personnel only.
- Access sessions to information systems hosting or processing protected information shall be automatically blocked after a certain period of inactivity of the users.

Whenever using software provided by LORIOT, the following rules must be observed:

- All persons accessing LORIOT information systems must use only the software versions provided and in accordance with its rules of use.
- All persons are prohibited from installing illegal copies of any software.
- The use of software not validated by LORIOT is prohibited.
- It is also forbidden to uninstall any of the software installed by LORIOT.

4.9. Network security

Networks over which protected information flows must be adequately managed and controlled, ensuring that there are no uncontrolled accesses or connections whose risks are not appropriately managed by the provider organisation.

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

Networks allowing access to LORIOT ICT infrastructure shall be appropriately secured, and the following requirements shall be met:

- Access of remote users to the LORIOT network shall be subject to compliance with identification and pre-authentication and access validation procedures.
- These connections shall be time-limited and through the use of virtual private networks or dedicated lines.
- No communications equipment (cards, modems, etc.) that would allow alternative uncontrolled connections shall be allowed on these connections.
- Access to networks through which protected information circulates shall be limited.
- All equipment connected to networks over which protected information flows shall be appropriately identified so that network traffic can be identified.

Remote work, considered as access to the corporate network from outside, is regulated by the application of the following regulations:

- The use of equipment not controlled by LORIOT for teleworking activities is not permitted.
- Criteria for authorisation of teleworking will be established on the basis of the needs of the job.
- The necessary measures shall be put in place for secure connection to the corporate network.
- Security monitoring and auditing systems will be put in place for established connections.
- The revocation of access rights and the return of equipment after the end of the period of need for the equipment shall be controlled.

Whenever the Internet access provided by LORIOT is used, the following rules must be observed in addition:

- The Internet is a work tool. All activities on the Internet should be related to work tasks and activities. Users should not search for or visit sites that do not support LORIOT's business purpose or the performance of their daily work.

- Internet access from the corporate network shall be restricted by means of control devices incorporated in the corporate network. The use of other means of connection must be previously validated and shall be subject to the above considerations on the use of the Internet.
- Users shall not use the name, symbol, logo or similar symbols of LORIOT in any Internet element (e-mail, web pages, etc.) not justified by strictly work-related activities.
- The transfer of data to or from the Internet shall only be permitted when related to business activities. Transfer of files not related to these activities (e.g. downloading of software, multimedia files, ...) shall be prohibited.

4.10. Traceability of use of the systems

Privileged access shall be logged and these logs shall be retained in accordance with the Organisation's backup regulations.

The activity of the systems used to perform such privileged access shall be logged, and such logs shall be retained in accordance with the Organisation's backup regulations.

Errors and failures in systems activity shall be analysed and remedial action shall be taken.

4.11. Identity and access control and management

All users with access to an information system shall have an individual access authorisation consisting of a user ID and password.

Users shall be responsible for all activity related to the use of their authorised access.

Users shall not use any authorised access of another user, even if they have the owner's authorisation.

Under no circumstances should users disclose their identifier and/or password to any other person, nor should they keep it in writing in plain view or within the reach of third parties.

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

They must also be complex and difficult to guess, and therefore consist of a combination of at least 3 of these 4 options in the first 8 characters:

-Majuscules

-Minuscules

-Numbers

-Special features

It is recommended to use the following guidelines for password selection:

- Do not use familiar words, or words that can be associated with oneself, e.g. one's name.

- The password should not refer to any recognisable concept, object or idea. Therefore, the use of significant dates, days of the week, months of the year, names of people, telephone numbers, etc. should be avoided.
- The password should be 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 a phrase or expression.
- The provider organisation shall ensure that it is regularly ascertained that only duly authorised persons have access to the protected information.
- In those cases where LORIOT information systems are also accessed, the following regulations must also be considered:
- No user will receive an access identifier to LORIOT systems until he/she agrees in writing to the security regulations in force.
- Users shall have authorised access only to such data and resources as they require for the performance of their functions.
- In case the system does not request it automatically, the user shall change the assigned temporary password the first time he/she makes a valid access to the system.
- In the event that the system does not automatically request it, the user must change his/her password at least once every 90 days.
- Temporary authorised accesses shall be set up for a short period of time. After expiry of this period, they shall be deactivated from the systems.
- In relation to personal data, only authorised persons may grant, alter or cancel authorised access to data and resources, in accordance with the criteria established by the person responsible for the file.

If a user suspects that his/her authorised access (user ID and password) is being used by another person, he/she should change his/her password and notify the incident to the e-mail address **security@loriot.io**.

4.12. Change management

All changes to the ICT infrastructure must be controlled and authorised, ensuring that no uncontrolled components are part of it.

All new components introduced into the provider organisation's ICT infrastructure used for the provision of the service should be verified to ensure that they function properly and fulfil the purposes for which they were introduced.

4.13. Technical change management

All changes that are made shall be carried out in accordance with a formally established and documented procedure, which ensures that the appropriate steps for making the change are followed.

The change management procedure shall ensure that changes to the ICT infrastructure are minimised and limited to those that are strictly necessary.

All changes should be tested before deployment in the production environment to ensure that there are no unintended or undesirable side effects on the operation and security of the ICT infrastructure.

The provider organisations shall scan and mitigate technical vulnerabilities in the infrastructures used for the provision of the service, informing LORIOT of all those associated with critical components.

4.14. Security in development

The entire outsourced software development process will be controlled and supervised by LORIOT.

Identification, authentication, access control, auditing and integrity mechanisms will be incorporated throughout the software design, development, deployment and operation lifecycle.

The software specifications shall expressly contain the safety requirements to be covered in each case.

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

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

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

The output information provided by applications should be limited, ensuring that only relevant and necessary information is provided.

Access to the source code of the applications shall be limited to service personnel.

In the test environment, real data shall only be used if they have been appropriately decoupled or if it can be ensured that the security measures applied are equivalent to those in the production environment.

During the testing of the applications, it will be verified that there are no uncontrolled information gaps, and that only the intended information is provided through the established channels.

Only software that has been expressly approved shall 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 shall have a plan that allows for its provision even in case of contingencies.

The above plan shall be developed based on the events capable of causing service disruptions and their likelihood of occurrence.

The provider organisation shall be able to demonstrate the feasibility of the existing contingency plan.

4.16. Monitoring and control

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

Approved: LORIOT Management and CISO.