KINEXON

# A.15.1 · Supply Security Policy

*Public*

# Table of Contents

KINEXON GmbH
Schellingstr. 35

80799 München

Tel.: +49 (0)89 / 200 61 65-0

info@kinexon.com

www.kinexon.com

This document has been validated for external publication and contains information that is the property of Kinexon GmbH. Reproduction is not permitted without the express written consent of the author. (info@kinexon.com).

If you have any questions, uncertainties or suggestions concerning this document, please send the problem description by mail to KINEXON GmbH. While the utmost care has been taken in preparing this document, KINEXON GmbH does not guarantee that it is absolutely free of errors.

Document Information

| Code: | Version | Date | Author | Approved by | Confidentiality level |
|---|---|---|---|---|---|
| A.15.1 · Supply Security Policy | 1.0 | 17/11/2021 | J. Sanz | Executive Board | Public |

Change history

| Date | Version | Created by | Description of change |
|---|---|---|---|
| 04/06/2021 | 0.1 | J. Sanz | Basic document outline |

Table of Contents

# 1 1. Purpose, scope and users

The purpose of this document is to establish the information security policy framework for Kinexon's external providers (suppliers). This policy must be applied to all activities carried out by suppliers that imply accessing Kinexon information, IT systems, applications, or any other IT asset, to protect their confidentiality, integrity, and availability.

This would only be for those suppliers whose services affect information security:

- Confidentiality: Suppliers access non-public information of Kinexon or its stakeholders.
- Integrity: An incident in this dimension would cause an impact other than slight (easily resolvable, no significant negative impact, serious, very serious or critical.
- Availability. An impact on this dimension would result in an impact other than slight.

**Slight impact** means an incident that is easily resolvable, **without a Extreme, Major, Moderate or Minor impact:**

- **Extreme:** Complete operational failure, "bet the farm" impact, unsurvivable.
- **Major:** Severe loss of operational capability, highly damaging and extremely costly but survivable.
- **Moderate:** Substantial operational impact, very costly.
- **Minor**: Noticeable but limited operational impact, some costs.

The "General guidelines" included in this policy are applicable to any supplier, regardless of the type of service provided to Kinexon. The "Specific guidelines" also included in this policy are applicable in addition to the "General guidelines" but only to those suppliers that provide to Kinexon any of the specific services indicated within that section of the document. All suppliers are responsible for informing their employees and subcontractors providing their services ultimately to Kinexon of the "General/Specific Guidelines" that are applicable to them.

## 1.1 1.1 Target Audience

Users of this document are all Kinexon's suppliers (their employees, as well as their subcontractors) with access to any information, IT system, application, or any other IT asset of Kinexon as well as all employees of Kinexon in charge of or involved in the managing these processes provided externally.

# 2 2. Reference documents

- ISO/IEC 27001 standard
- Information Security Policy (ISP).

# 3 3. General Guidelines

## 3.1 3.1 Service provision

1. All suppliers may only perform for Kinexon those activities covered under their service agreement (contract).
2. Every supplier shall periodically provide Kinexon with a list of persons, profiles, functions, and responsibilities associated with the service provided, and shall promptly inform Kinexon of any change that may occur in that list (registra-tion, termination, substitution or shifting of persons, functions, or responsibilities).
3. In accordance with contract clauses associated with the delivery of the hired ser-vice, all external persons carrying out work for Kinexon must comply with the security guidelines set out in this document. In case of non-compliance with any of these obligations, Kinexon re-serves the right to veto the person who has committed the infraction, as well as to adopt the sanctioning measures that may be pertinent regarding the supplier.
4. The minimum security clauses applicable to Kinexon suppliers are detailed in the current policy.
5. All Kinexon suppliers shall ensure that all its staff have the appropriate training for the performance of the service provided.
6. Any type of exchange of information that may take place between Kinexon and any of its suppliers shall be understood to have been carried out within the framework established in the service agreement (contract) signed by both parties, so that the ex-changed information may not be used outside this framework or for other purposes.
7. Generally, Kinexon assets include:
   a. **Protected information** – any data that makes it possible to identify individuals and/or legal entities, and information linked to the configuration of information systems and/or communication networks.
   b. **Assets linked to the processing of protected information –** any software, hard-ware, communication network, information support, auxiliary equipment, or installation used to process protected information.

## 3.2 3.2 Information confidentiality

1. External people having access to Kinexon information shall consider that such information is by default protected information. Only information accessed via public dissemination means put in place by Kinexon shall be considered as unprotected information.

2. The information is classified as defined in A.8.3 Information Classification Policy in the following levels:
   a. Public
   b. Internal
   c. Confidential
   d. Secret

3. Disclosure, modification, destruction, or misuse of Kinexon information, whatever the medium on which it is held, shall be prevented.
4. Maximum confidentiality shall be maintained indefinitely for Kinexon protected information, and it shall never be released to the public, unless duly authorized.
5. Reports in paper containing Kinexon protected information shall be kept to a minimum and shall be kept in a secure place out of the reach of third parties.
6. If, for reasons directly related to the tasks to be delivered by an employee of a Kinexon supplier, he/she comes into possession of Kinexon protected information, contained in any type of medium, he/she shall consider such possession as strictly temporary, and shall follow the obligation of secrecy without assuming any right of possession, ownership or copying of such information.
7. Likewise, any Kinexon supplier employee must return this Kinexon protected information immediately upon completion of the tasks that have given rise to the temporary use of it and, in any case, upon termination of the relationship of his/her company with Kinexon.

8. All these obligations shall apply after the termination of the activities that the supplier's staff carried out for Kinexon. Failure to comply with these obligations may constitute an offense of disclosure of secret information.
9. To ensure the security of confidential or secret data, in addition to the considerations already mentioned, all Kinexon supplier's staff shall observe the following rules of conduct:
    a. No personal data shall be stored on the local disk drives of the user's PC workstations.
    b. The extraction of media and documents (including emails) outside the premises where such information is located, may only be authorized by Kinexon, and shall be carried out in accordance with the defined procedure.
    c. The media and documents must allow the type of information they contain to be identified, inventoried, and stored in a place with restricted access only to authorized persons.
    d. The transmission via telecommunication networks (e.g., email) shall be carried out by encrypting such data or by using any other mechanism that ensures that the information cannot be intelligible or manipulated by third parties.

In case you deal with information classified as confidential or secret in your service or have any doubts about the above, please contact your Kinexon IT Security Officer (ITSecurity@kinexon.com) to find out what security measures you need to comply with to protect it.

## 3.3 3.3 Intellectual property

1. Compliance with legal restrictions regarding the use of content protected by intellectual property law shall be ensured.
2. Users may only use material authorized by Kinexon for the performance of their duties.
3. The use of unlicensed software on Kinexon information systems is strictly prohibited.
4. Likewise, the use, reproduction, transfer, transformation, or public communication of any type of work or invention protected by intellectual property without due written authorization is prohibited.
5. Kinexon only authorizes the use of internally produced contents, or contents authorized or supplied to Kinexon by its owner, in accordance with the agreed terms and conditions and the provisions of the intellectual property regulations in force.

## 3.4 3.4 Information exchange

1. No person shall conceal or manipulate his or her identity under any circumstances.
2. The distribution of information either in electronic or physical format will be done through the resources determined in the service provision contract for such purpose and for the exclusive purpose of facilitating the functions associated to such contract. Kinexon reserves the implementation of control, registration, and audit measures on these dissemination resources, depending on the risk identified in each case.
3. Regarding the exchange of information within the framework of the service provision contract, the following activities shall always be considered as unauthorized:
    a. Transmission or reception of any material protected by copyright in violation of Intellectual Protection Law:
    b. Transmission or reception of any kind of pornographic material, sexually explicit material, racially discriminatory statements and any other kind of statement or message that can be classified as offensive or illegal.
    c. Transmission of protected information to unauthorized third parties.
    d. The transmission or reception of non-business-related applications.
    e. Participation in any Internet activity not directly related to the provision of the service, such as newsgroups, and games, amongst other activities.

4. In general, all activities that may damage the image and reputation of Kinexon are prohibited on the Internet and elsewhere.

## 3.5 3.5 Appropriate use of resources

1. All Kinexon suppliers undertake to periodically inform Kinexon of the assets used to provide the hired service.
2. All Kinexon suppliers undertake to use the resources made available by Kinexon for the provision of the service in accordance with the conditions for which they were designed and implemented.
3. The resources that Kinexon makes available to external parties, regardless of their type (e.g., IT, data, software, networks, communication systems, etc.) are available exclusively to fulfil the obligations and purpose of the operation for which they were provided. Kinexon reserves the right to implement control and/or audit mechanisms to verify the appropriate use of these resources.
4. All supplier equipment that may be connected to the Kinexon production network shall be of approved makes and models. All suppliers shall make such equipment available to Kinexon to co-ordinate the installation of the approved software and to configure it appropriately.
5. Any file introduced into the Kinexon network, or any equipment connected to it through automated media, Internet, e-mail, or any other means, must comply with the requirements set out in these General Guidelines and, in particular, with those relating to intellectual property, personal data protection, and malware control.
6. All assets shall be returned to Kinexon without undue delay after termination of the contract. All personal computers on which Kinexon has installed software shall be taken to Kinexon to have the hard drive formatted upon termination of the service.
7. All persons with access to the Kinexon network shall be obliged to use up-to-date anti-malware software.

**It is expressly prohibited**:

1. The use of resources provided by Kinexon for activities not related to the purpose of the service.
2. To connect to the Kinexon production network using equipment and/or applications that are not specified as part of the software or standards of the own computing resources.
3. To introduce obscene, threatening, immoral or offensive content into Kinexon's information systems or corporate network.
4. To voluntarily introduce into the corporate network of Kinexon any type of malware (e.g., virus, worms, trojans, spyware, ransomware, etc.), 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.
5. To obtain rights or access other than those assigned to them by Kinexon without explicit authorization.
6. To gain access to restricted areas of Kinexon information systems without explicit authorization.
7. To distort or falsify the log records of Kinexon information systems.
8. To decrypt the encryption keys, systems or algorithms and any other security elements involved in Kinexon's telematic processes without explicit authorization.
9. To possess, develop or execute programs that could interfere with the work of other users, or damage or alter Kinexon's computer resources.
10. To destroy, alter, disable, or otherwise damage data, programs or electronic documents containing protected information (these acts may constitute a criminal offence).
11. To harbor protected information on the local disk drives of user PC workstations.

## 3.6 3.6 User responsibilities

1. Service provider organizations shall ensure that all persons performing work for Kinexon respect the following basic principles within their activity:
    a. Each person with access to Kinexon information is responsible for the activity carried out by his/her user-per-son identifier 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.
    b. Users must not use any identifier belonging to another user, even if they have the owner's authorization.
    c. Users are aware of and apply existing requirements and procedures relating to the information they handle.

2. Anyone with access to protected information should follow the following guidelines regarding password management:
    a. Select quality passwords, i.e., passwords that are difficult for other users to guess.
    b. Ask for the password to be changed whenever there is a possible indication of knowledge by other users.
    c. Change passwords at least once every 90 days and avoid reusing old passwords.
    d. Change default and temporary passwords on first login.
    e. Avoid including passwords in automated login processes (e.g., those stored in browsers).
    f. Re-port any security incidents related to your passwords, such as loss, theft, or indications of loss of confidentiality.

3. Anyone with access to protected information should ensure that computers are protected when they are to be left unattended and should observe at least the following clean desk rules, to protect paper documents, computer media and portable storage devices and to reduce the risks of unauthorized access, loss, and damage to information, both during and outside normal working hours:
    a. Store paper documents and computer media under lock and key when not in use, especially outside normal working hours.
    b. Lock up paper documents and IT equipment when they are not being used, especially outside working hours.
    c. Lock user sessions or switch off the PC when it is left unattended.
    d. Protect both the points where information is received and sent (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.
    e. Remove, without undue delay, any protected information once printed.
    f. Destroy protected information once it is no longer needed.

4. Persons with access to Kinexon systems and/or information shall never, without written authorization, conduct tests to detect and/or exploit a suspected security weakness or incident. No person with access to Kinexon systems and/or information shall, without express written authorization, attempt by any means to breach the security system and authorizations. The capture of network traffic by users is prohibited, except in the case of auditing tasks authorized in writing.
5. All persons accessing protected information must follow the following rules of conduct:
    a. Protect protected information from unauthorized disclosure, modification, destruction, or misuse, whether accidental or not.
    b. Protect all information systems and telecommunications networks against unauthorized access or use, disruption of operations, destruction, misuse, or theft.
    c. Have the necessary authorization to gain access to information systems and/or information.

## 3.7 3.7 User equipment

1. Service provider organizations shall ensure that all user equipment used to access protected information complies with the following standards:
    a. Upon user inactivity, the equipment shall be automatically locked within 15 minutes.
    b. No user equipment shall be equipped with tools that could breach security systems and authorizations.
    c. User equipment shall be maintained in accordance with the manufacturer's specifications.
    d. All user equipment shall be adequately protected against malware:
    e. Anti-malware software shall be installed and used on all personal computers to reduce the operational risk associated with viruses or other malicious software.
    f. They shall be kept up to date with the latest available security updates.
    g. Anti-malware software shall always be enabled and kept up to date.

2. Special care shall be taken to ensure the security of all user's mobile equipment that contains or otherwise allows access to protected information:
    a. Verifying that they do not contain more information than is strictly necessary.
    b. Ensuring that access controls are applied to such information.

c. Minimizing access to such information in the presence of persons not involved in the service provided.
d. Transporting equipment in cases, briefcases or similar equipment that incorporates appropriate protection against environmental agents.

## 3.8 3.8 Hardware management

1. Service provider organizations shall ensure that all equipment provided by Kinexon for the provision of services, regardless of its type, is properly managed. To this end, they shall comply with the following standards:
2. The provider organization shall maintain an up-to-date list of equipment provided by Kinexon and persons using such assets or associated responsible persons in case the assets are not for single person use. Such a list may be requested by Kinexon.
3. Whenever a provider organization wishes to reassign any Kinexon equipment that has contained protected information, it must return it temporarily so that the necessary secure deletion procedures can be carried out prior to reassignment.
4. If a provider organization wishes to remove any of the received Kinexon equipment from the list of Kinexon equipment, it must always return it, so that Kinexon can treat such removal appropriately.
5. If a provider organization ceases to provide the service, it must return to Kinexon the entire list of equipment received, as stipulated in the corresponding service provision contracts. Only in the case of paper documents and computer media, the supplier organization may securely dispose of them, in which case it must notify Kinexon of such disposal.

# 4 4. Specific Guidelines

## 4.1 4.1 Scope

1. All suppliers must comply, in addition to the General Guidelines (see section 3), 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 Kinexon.
2. The types of service contemplated are those indicated below:
    a. **Location** of the execution of the service: depending on the main place where the services are carried out, two cases are distinguished:
    b. **Kinexon**: the supplier provides the service mainly from Kinexon own headquarters.
    c. **Remote**: the supplier pro-vides the service mainly from its own premises, although occasional activities may be carried out at Kinexon headquarters.

    d. **Ownership** of the ICT infrastructure used: depending on who owns the main ICT infrastructures (communication, user equipment, software) used to provide the service, two cases can be distinguished:
    e. **Kinexon.**
    f. **Supplier.**

3. **Level of access** to Kinexon systems: depending on the level of access to Kinexon information systems, three cases can be distinguished:
    a. **Privileged access**: the service to be provided requires privileged access to Kinexon's information systems, with the ability to administer these systems and/or the production data they process.
    b. **Normal user access**: The service provided requires the use of Kinexon's information systems, so that the persons providing the service have user level accounts that allow them to access some of those systems with regular privileges.
    c. **No access**: the service to be provided does not require the use of Kinexon information systems, so that the persons providing the service do not have user accounts on these systems.

4. Depending on the service to be provided, the supplier must comply, in addition to the General Guidelines (see section 3), with one or more of the following Specific Guidelines (see sub section numbers indicated in the following table):

| | LOCATION | | INFRASTRUCTURE | | ACCESS | | |
|---|---|---|---|---|---|---|---|
| | Kinexon | Remote | Kinexon | Supplier | Privileged | Normal | No access |
| 4.2 People selection | No | No | No | No | Yes | No | No |
| 4.3 Security audit | No | No | No | No | Yes | No | No |
| 4.4 Incident reporting | Yes | Yes | Yes | No | Yes | Yes | No |
| 4.5 Physical security | No | Yes | No | No | No | No | No |
| 4.6 Asset management | No | No | No | Yes | No | No | No |

|  | LOCATION |  | INFRASTRUCTURE |  | ACCESS |  |  |
|---|---|---|---|---|---|---|---|
| 4.7 Security architecture | No | No | No | Yes | Yes | Yes | No |
| 4.8 System security | No | No | No | Yes | No | No | No |
| 4.9 Network security | No | No | No | Yes | No | No | No |
| 4.10 Traceability of system usage | No | No | No | Yes | Yes | No | No |
| 4.11 Identity/access control & management | No | No | No | Yes | No | No | No |
| 4.12 Change management | No | No | No | Yes | Yes | Yes | No |
| 4.13 Technical change management | No | No | No | No | Yes | No | No |
| 4.14 Development security | No | No | No | No | Yes | Yes | No |
| 4.15 Contingency management | No | No | No | Yes | No | No | No |

## 4.2 4.2 People selection

1. The supplier organization must verify the professional background of the persons assigned to the service, guaranteeing Kinexon that in the past they have not been sanctioned for professional malpractice nor have they been involved in
2. incidents related to the confidentiality of the information processed that have led to any type of sanction.
3. The provider organization shall guarantee Kinexon the possibility of immediate removal from the persons assigned to the service of any person in relation to whom Kinexon wishes to exercise the right of veto, in accordance with the conditions set out in section 3.1.

## 4.3 4.3 Security audit

1. The supplier organization shall allow Kinexon to carry out the requested security audits, collaborating with the audit team and providing all required evidence and records.
2. The scope and depth of each audit shall be expressly established by Kinexon on a case-by-case basis. The audits will be carried out following the planning agreed in each case with the organization providing the service.
3. Kinexon reserves the right to carry out additional extraordinary audits, provided that there are specific causes that justify it.

## 4.4 4.4 Incident reporting

1. When any information security incident is detected, it must be notified immediately to the following Kinexon e-mail address: ITSecurity@kinexon.com

2. Any user may report through said address any events, suggestions, vulnerabilities, etc. that may be related to information security and the guidelines contemplated in these rules of which he/she becomes aware.
3. Any incident detected that affects or may affect the security of personal data (e.g., loss of lists and/or computer media, suspicions of improper use of authorized access by other persons, recovery of data from backup copies, etc.) must be also notified using the e-mail address previously indicated.
4. This address centralizes the collection, analysis and management of the incidents received.
5. If access to this e-mail address is not available, the communication channels established within the service itself must be used, so that the right Kinexon interlocutor does communicate the security incident

## 4.5 4.5 Physical security

1. The site shall be locked and shall have some form of access control system.
2. There shall be some form of visitor control, at least in public access and/or loading and unloading areas.
3. The site shall have at least adequate fire detection and suppression systems and shall be constructed to provide sufficient resistance to flooding.
4. If any backup is maintained, the systems housing and/or processing such information should be located in a specially protected area, which includes at least the following security measures:
    a. The specially protected area shall have a separate access control system from that of the headquarters.
    b. Access to persons outside the specially secured area shall be limited. Such access shall be granted only when necessary and authorized, and always under the supervision of authorized persons.
    c. A record shall be kept of all access by outsiders.
    d. Outsiders may not remain or perform work in the specially protected areas without supervision.
    e. The consumption of food or drink in these specially protected areas shall be prohibited.
    f. Systems located in these areas shall have some form of power failure protection.

## 4.6 4.6 Asset management

1. The provider organization shall have an up-to-date asset register in which assets used for the provision of the service can be identified.
2. All assets used for the provision of the service shall have a responsible person, who shall ensure that these assets incorporate the minimum-security measures established by the provider organization, which shall at least be those specified in these rules.
3. The provider organization shall notify Kinexon of the disposal of assets used for the provision of the service. If such an asset contains other Kinexon proper-ty (hardware, software, or other types of assets), it must be handed over to
4. Kinexon prior to the decommissioning, in order for Kinexon to proceed with the removal of the assets owned by Kinexon.
5. Whenever an asset has contained protected information, the provider organization shall carry out asset retirement by ensuring the secure disposal of such information, by applying secure deletion functions or by physically destroying the asset, so that the information contained therein cannot be recovered.

## 4.7 4.7 Security architecture

1. Whenever the service provider organization carries out development and/or testing of applications for Kinexon or with protected information, the environments in which such activities are carried out shall be isolated from each other and also isolated from the production environments in which protected information is hosted or processed.
2. 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.
3. Information systems hosting or processing particularly sensitive information shall be isolated from other information systems.

## 4.8 4.8 System security

1. Information systems hosting or processing protected information shall record the most significant events surrounding their operation. These activity logs shall be covered by the provider organization's backup policy.
2. The clocks of the provider organization's systems that process or host protected information shall be synchronized with each other and with the official time.
3. The service provider organization shall ensure that the capacity of information systems storing or processing protected information is properly managed, avoiding potential downtime or malfunctioning of such systems due to resource saturation.
4. Information systems hosting or processing protected information shall be adequately protected against malicious software by applying the following precautions:
    a. Systems shall be kept up to date with the latest available security updates, in development, test and production environments.
    b. Anti-malware software shall be installed and used on all servers and person-al computers to reduce the risk associated with malicious software.
    c. Anti-malware software shall always be enabled and up to date.
5. The provider organization shall establish a backup policy to ensure that any data or information relevant to the service provided is safeguarded on a weekly basis.
6. Whenever electronic mail is used in connection with the service provided, the provider organization shall respect the following rules:
    a. The transmission via e-mail of protected information shall not be permitted unless the electronic communication is encrypted, and the sending is authorized in writing.
    b. The transmission via e-mail of information containing specially protected personal data (e.g., health information) shall not be permitted unless the electronic communication is encrypted, and the transmission is authorized in writing.
    c. Whenever Kinexon e-mail is used for the provision of the service, at least the following principles shall be observed:
    d. E-mail shall be considered as another working tool provided for the exclusive purpose of the contracted service. This consideration shall empower Kinexon to implement control systems to ensure the protection and proper use of this resource. This power, however, shall be exercised while safeguarding the dignity of individuals and their right to privacy.
    e. The Kinexon e-mail system shall not be used to send fraudulent, obscene, threatening, or other similar communications.
    f. Users shall not create, send, or forward advertising or pyramid messages (messages that are spread to multiple users).
7. Access to information systems hosting or processing protected information should always be authenticated, at least using a person identifier and associated password.
8. Information systems hosting or processing protected information shall have access control systems that limit access to such information to service persons only.
9. Access sessions to information systems hosting or processing protected information shall be automatically locked after a certain period of inactivity of the users.
10. Whenever software provided by Kinexon is used, the following rules shall be observed:
    a. All persons accessing Kinexon information systems must use only the software versions provided and in accordance with their rules of use.
    b. All persons are prohibited from installing illegal copies of any software.
    c. The use of software not validated by Kinexon is prohibited.
    d. It is also forbidden to uninstall any of the software installed by Kinexon.

## 4.9 4.9 Network security

1. Networks over which Protected Information flows should be adequately managed and controlled, ensuring that there are no uncontrolled accesses or connections whose risks are not appropriately managed by the provider organization.

2. Services available on networks through which Protected Information flows should be limited to the extent possible.
3. Networks allowing access to Kinexon's ICT infrastructure should be appropriately protected, and the following requirements should be met:
    a. Access by remote users to the Kinexon network shall be subject to compliance with identification and pre-authentication procedures and validation of access.
    b. These connections shall be made for a limited time and using virtual private networks or dedicated lines.
    c. No communications equipment (cards, modems, etc.) enabling alternative uncontrolled connections shall be permitted on these connections.
4. Access to networks over which protected information circulates shall be limited.
5. All equipment connected to networks over which protected information flows must be appropriately identified so that network traffic can be identifiable.
6. Teleworking, considered as access to the corporate network from the outside, is regulated by the application of the following rules:
    a. The use of equipment not controlled by Kinexon for teleworking activities is not permitted.
    b. Criteria for authorization of teleworking will be established based on the needs of the job.
    c. Necessary measures for secure connection to the corporate network shall be established.
    d. Security monitoring and auditing systems shall be established for established connections.
    e. The revocation of access rights and the return of equipment at the end of the period of need shall be controlled.
    f. Whenever Internet access provided by Kinexon is used, the following rules must also be observed:
    g. The Internet is a working tool. All Internet activities must be related to work tasks and activities. Users should not search for or visit sites that do not support the business purpose of Kinexon or the fulfillment of their daily work.
    h. Access to the Internet 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 validated in advance and is subject to the above considerations on the use of the Internet.
    i. Users shall not use the name, symbol, logo, or similar symbols of Kinexon in any Internet element (e-mail, web pages, etc.) not justified by strictly work-related activities.
    j. The transfer of data from or to the Internet shall only be permitted when related to business activities. The transfer of files not related to these activities (e.g., downloading of software, multimedia files, etc.) shall be prohibited.

## 4.10 4.10 Traceability of system usage

1. All users with access to an information system shall have a single access authorization consisting of a user ID and password.
2. Users shall be responsible for all activity related to the use of their authorized access.
3. Users shall not use any authorized access of another user, even if authorized by the owner.
4. Users shall not under any circumstances disclose their identifier and/or password to any other person, nor shall they keep it in written form in plain view or accessible to third parties.
5. The minimum length of the password must be six (6) characters and must not contain the name, surname, or identifier of the user. It must be changed every forty-five (45) days and must not repeat at least the previous eight (8) passwords.
6. Likewise, they must be complex and difficult to guess, so they must be made up of a combination of at least three of these four options in the first eight (8) characters:
    a. Upper case.
    b. Lower case letters.
    c. Numbers.
    d. Special characters.
7. It is recommended to use the following guidelines for the selection of passwords:
    a. Do not use known words, or words that can be associated with oneself, e.g., one's name.

   b. The password should 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, telephone numbers, etc. in your password.
   c. The password should be something practically 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.

8. The provider organization must ensure that it is regularly checked that only those persons who are duly authorized to access the protected information have access to it.
9. In cases where Kinexon information systems are also accessed, the following rules should also be considered:
   a. No user will be given an access ID to Kinexon systems until he/she agrees in writing to the security regulations in force.
   b. Users shall have authorized access only to those data and resources that they require for the performance of their duties.
   c. If the system does not automatically request it, the user must change the temporary password assigned to him/her the first time he/she makes a valid access to the system.
   d. If the system does not automatically request it, the user shall change his/her password at least once every 90 days.
   e. Temporary authorized accesses shall be set up for a short period of time. After expiry of this period, they shall be deactivated from the systems.
   f. In relation to personal data, only authorized persons may grant, alter, or revoke authorized access to data and resources, in accordance with the criteria established by the person responsible for the file.

   - If a user suspects that his or her authorized access (user ID and password) is being used by another person, he or she must change his or her password and notify the incident to the following e-mail address: **ITSecurity@kinexon.com.**

## 4.11 4.11 Identity/access control & management

1. All users with access to an information system shall have a single access authorization consisting of a user ID and password.
2. Users shall be responsible for all activity related to the use of their authorized access and shall not use the authorized access of another user, even if authorized by the owner, nor un-der any circumstances disclose their identifier and/or password to any other person, nor keep it in written form in plain view or accessible to third parties.
3. The minimum length of the password must be six (6 ) characters and must not contain the name, surname, or identifier of the user. It must be changed every forty-five (45) days and must not repeat at least the previous eight (8) passwords.
4. Likewise, they must be complex and difficult to guess, so they must be made up of a combination of at least three of these four options in the first eight (8) characters:
   a. Upper case.
   b. Lower case letters.
   c. Numbers.
   d. Special characters.

5. It is recommended to use the following guidelines for the selection of passwords:
   a. Do not use known words, or words that can be associated with oneself, e.g., one's name.
   b. The password should 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, telephone numbers, etc. in your password.
   c. The password should be something practically 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.

6. The provider organization must ensure that it is regularly checked that only those persons who are duly authorized to access the protected information have access to it.

7. In cases where Kinexon information systems are also accessed, the following rules should also be considered:
    a. No user will be given an access ID to Kinexon systems until he/she agrees in writing to the security regulations in force.
    b. Users shall have authorized access only to those data and resources that they require for the performance of their duties.
    c. If the system does not automatically request it, the user must change the temporary password assigned to him/her the first time he/she makes a valid access to the system.
    d. If the system does not automatically request it, the user shall change his/her password at least once every 90 days.
    e. Temporary authorized accesses shall be set up for a short period of time. After expiry of this period, they shall be deactivated from the systems.
    f. In relation to personal data, only authorized persons may grant, alter, or revoke authorized access to data and resources, in accordance with the criteria established by the person responsible for the file.
    g. If a user suspects that his or her authorized access (user ID and password) is being used by another person, he or she must change his or her password and notify the incident to the e-mail address Kinexon.

## 4.12 4.12 Change management

1. All changes to the ICT infrastructure shall be controlled and authorized, ensuring that no uncontrolled components are part of the ICT infrastructure.
2. All new components introduced into the provider organization's ICT infrastructure used for the provision of the service shall be verified as functioning properly and fulfilling the purpose for which they were introduced.

## 4.13 4.13 Technical change management

1. All changes that are implemented shall be carried out following a formally established and documented procedure, which ensures that the appropriate steps are followed to implement the change.
2. The change management procedure shall ensure that changes to the ICT infrastructure are minimized and limited to those that are strictly necessary.
3. All changes should be pro barred prior to deployment in the production environment to check that there are no unintended or undesirable side effects on the operation and security of the ICT infrastructure.
4. The provider organizations must scan and mitigate the technical vulnerabilities presented by the infrastructures used for the provision of the service, informing Kinexon of all those associated with critical components.

## 4.14 4.14 Development security

1. The entire outsourced software development process will be controlled and supervised by Kinexon.
2. Identification, authentication, access control, audit and integrity mechanisms shall be incorporated throughout the software design, development, implementation, and operation life cycle.
3. The software specifications shall expressly contain the security requirements to be covered in each case.
4. The software to be developed shall incorporate input da-ta validations to verify that the data is correct and appropriate and to prevent the introduction of executable code.
5. Internal processes developed by applications should incorporate all necessary validations to ensure that no corruption of information occurs.
6. Whenever necessary, authentication and integrity control functions should be incorporated in the communications between the different components of the applications.
7. The output information provided by applications should be limited, ensuring that only relevant and necessary information is provided.
8. Access to the source code of applications should be limited to service personnel.

9. In the test environment, real data shall only be used when it has been appropriately decoupled or when it can be ensured that the security measures applied are equivalent to those in the production environment.
10. During application testing, it shall be verified that there are no uncontrolled information gaps, and that only the intended information is provided through the established channels.
11. Only software that has been expressly approved shall be transferred to the production environment.
12. In relation to web services, the management of the OWASP Top 10 will be considered.

## 4.15 4.15 Contingency management

1. The service provided must have a plan that allows it to be granted even in the event of contingencies. This **Contingency Plan** shall be developed based on the events capable of causing service disruptions and their probability of occurrence.
2. All Kinexon supplier shall be able to demonstrate the feasibility of the Contingency Plan.

# 5 5. Monitoring & Control

To ensure the correct use of all resources, Kinexon will perform checks, either periodically or whenever a specific security or service reason makes it advisable, through the formal and technical mechanisms deemed appropriate in each case.