AlbatrossProjects

Information Security Guideline

Company
Albatross Projects GmbH
Daimlerstrasse 17
89564 Nattheim

INFORMATION SECURITY GUIDELINE

Organisation key:	VA-GU-00001
Storage location:	IMS
Version:	1.0
Reference documents:	3.0 - 41 Information Security Guideline
Date of the version:	08 May 2023
Revision interval:	12 months
Created by:	M. Schuster
Audited by:	B. Kienle
Authorised by:	Management
Approved on:	01 June 2023
Confidentiality level:	1

CHANGE HISTORY

Date	Version	Created by	Description of the change
21 April 2023	1.0	MSR	First draft of the document
08 May 2023	1.0	BK	Modification of the document

Contents

1. PURPOSE AND AREA OF APPLICATION

Our operational processes are increasingly supported by information technology, which means that we increasingly depend on it. In order to protect our processes and data processing systems as well as the IT infrastructure and databases from threats such as misuse, malware, espionage and operating errors, we developed a policy including suitable measures. These measures are designed to ensure that the safety objectives of accessibility, confidentiality and integrity are met. Please find further information and details on our objectives in our policy "IT-Security".

2. SCOPE AND OBJECTIVES

This policy applies without restriction to all staff of Albatross Projects GmbH, including those who are away on a construction job and those who work from home. It also applies to external staff who may be involved in certain projects. For external staff, it may be necessary to ensure that they comply with the provisions of this policy, either by means of appropriate letters of intent or contractual arrangements. The policy applies to all types of hardware and software as well as all data processing procedures and mobile data carriers used in the company, including those managed by external bodies. This includes devices such as laptops, tablets, smartphones and USB sticks. Should it ever become necessary to deviate from this policy in exceptional cases, a substitute policy may only be implemented with the prior authorisation of the management. It is essential that all staff, including external staff, fully understand and comply with this policy in order to ensure that the safety objectives of the company are met: accessibility, confidentiality and integrity of the company's data. By complying with this policy, potential security risks can be minimised and secure handling of the company's data can be ensured.

3. ORGANISATION

A security organisation is set up in order to meet the objectives of information security and data protection. An external consultant has been commissioned for this purpose. This consultant supports the persons in charge and is the contact person for all staff of the company in matters relating to information security and data protection.

The contact details are issued within the company.

4. GENERAL REGULATIONS

4.1 Appropriation of systems and work equipment

Albatross Projects GmbH provides all IT-equipment such as PCs, notebooks, USB sticks, memory cards and mobile drives as well as other mobile devices such as PDAs, tablets etc. for business purposes which are all subject to the provisions of this policy. The acquisition of IT-equipment for use within the company is only permitted after review and approval by the IT-Department and in accordance with the defined specifications. The use of hardware and/or software that has not been acquired and set up in accordance with the defined specifications is not permitted. Exceptions may only be made after consultation with the responsible departments and written documentation. Before any type of hardware and software is put into operation, it must be technically approved by the responsible department and, if necessary, professionally authorised by the appropriate departments. The authorisations must be documented. The use of unapproved software, in particular IT-services from outside the organisation, is not permitted. Changes are only permitted upon request of the responsible department and must be documented.

4.2 Mobile work

In order to ensure the security of mobile work, particularly with regard to the protection of confidential data and information, we ensure that all staff adhere to defined regulations in the form of guidelines.

4.2.1 Mobile communication devices

In order to avoid the loss of company data, only copies of the company data may be saved on notebooks and mobile communication devices such as mobile phones and PDAs. If personal or other confidential data is saved in accordance with the provisions of the confidentiality policy, it must be encrypted.

The following precautions must be observed:

- The hard drives of portable devices such as notebooks must be encrypted using BitLocker.
- Each mobile device must be protected by a secure password in accordance with this policy or by another secure and approved method.
- It must be ensured that unauthorised persons do not have access to any private space.
- It is not permitted to pass notebooks on to unauthorised persons or to allow family members to use them.
- If notebooks are used by different users or in insecure or unknown environments, they must be regularly checked for security risks.
- In public space, e.g. while using public transport, privacy filters must be used in order to prevent the unauthorised processing of personal or other sensitive data.
- Mobile devices must not be left unattended and must be stored safely.

- Only mobile devices without any personal or confidential data may be connected to external computers.
- After having been connected to external computers, the mobile devices must be checked for viruses and other malware.

4.2.2 Conduct and work in unfamiliar environments

In order to avoid the loss of company data, only copies of the company data may be saved on notebooks and mobile communication devices such as mobile phones or PDAs. If personal data or other confidential or highly confidential data needs to be saved in accordance with document control, this data should be encrypted in order to guarantee data protection.

While travelling, notebooks and other mobile data carriers should never be left unattended, not even on trains or at security controls at airports or other public places. Checking in laptops as luggage on flights or leaving them lying around visibly in the car is to be avoided. If a taxi or a hired car is used, data carriers should not be left behind inside the vehicle. If a notebook is carried as hand luggage, it should be concealed as well as possible in order to protect it from theft. While working on public transport, it is important to have sufficient privacy to prevent unauthorised persons from looking on. Personal or sensitive data should not be processed. While travelling it is important to regularly use a secure connection to back up the acquired data and forward the results to central systems or mobile data carriers. Backup data carriers should be encrypted and stored separately from the notebook. When travelling abroad, attention should be paid to special risks, precautions should be taken and regulations adhered to. It is important to comply with local regulations to ensure that both data and devices are secure in other countries. It is advisable to take appropriate precautions to protect data and devices while travelling, as they may represent potential security vulnerabilities. Careful planning and implementation of protective measures can help to ensure the security of data and devices.

In addition, the following precautionary measures must be observed:

The hard drives of portable devices (notebooks) must be encrypted using BitLocker

- Each mobile device must be secured by a secure password in accordance with a guideline or by another secure and approved method.
- Unauthorised access must be ruled out in private spaces.
- Access by unauthorised persons or a transfer of the notebook to third parties for use, including family members, is not permitted.
- If notebooks are used by various users or in insecure or unknown environments, they must be regularly checked for security risks.

- Privacy filters must be used on notebooks in public spaces, e.g. on public transport etc., otherwise the processing of personal or other sensitive data is not permitted.
- Mobile devices must not be left unattended and must be stored securely.
- Only mobile devices that do not contain any personal or other confidential data may be used to be connected to external computers.
- After having been connected to external computers, the mobile devices must be checked for viruses and other malware.
- Desktop PCs (desktops, notebooks, handhelds, etc.) and peripheral devices must be locked in if they are not under supervision.
- Precautions must be taken during conversations and meetings about confidential matters to ensure that these conversations cannot be overheard by unauthorised persons.
- Saving or processing internal and confidential information on external systems is not permitted.
- Internal and confidential information may only be printed on printers that are suitably protected and must be collected from the printer immediately. Printers and copiers with extensive memory functions should be avoided for printing confidential information.

4.3 Use and approval of software

Prior to collecting, processing or using personal or confidential data, the required systems and programmes (hardware and software) must be successfully tested and approved. This also applies to the introduction of standard software, the installation of updates or other changes to programmes or procedures. The extent of the test and approval is defined in the process documentation and must be individually specified in each case. If new procedures or applications are supposed to be used, written approval must be requested from the IT-management.

4.4 Use of private hardware and software and private use of company devices

4.4.1 Private devices

The use of private hardware and software such as notebooks, USB sticks, memory cards and mobile drives for business purposes as well as the use of private data carriers such as floppy discs, CDs and memory sticks on company PCs is prohibited in accordance with the company guidelines.

4.4.2 Use of company devices for private purposes

It is prohibited to use company hardware and software for private purposes and to use company mobile data carriers on private devices. The same applies to the business use of company-owned mobile data carriers on private devices and their transfer to persons outside the company, including family members. Copies of programmes may only be made for business purposes and only to the extent permitted by the licensing conditions and in so far as required for business reasons. As soon as the copies are no longer required, they must be deleted or destroyed. The creation of copies of data is also only permitted for operational purposes and only in consultation with the owner of the information, depending on the degree of confidentiality.

4.5 Management and administration of data processing procedures

4.5.1 Administration rights

Administrators may only be given privileged rights if this is absolutely necessary in order to carry out their administrative tasks. Standard accounts should be used for tasks that can be performed without these rights. The administrator's access to company data content is only permitted upon the instructions of the Manager in charge. When it comes to private content, such as private emails, the administrator may only access them with the consent of the person concerned. This consent should preferably be given in private or in the presence of the person concerned. Please note that this rule does not apply to necessary data access in the event of a suspected criminal offence during the employment relationship or in order to avert danger (in the event of imminent danger).

4.5.2 Monitoring of interfaces and access points

Interfaces to external devices such as Wi-Fi or USB interfaces as well as external drives such as CD- or DVD-drives are deactivated if they are not required. If these interfaces are required to fulfil tasks, they are monitored to ensure that only authorised and approved devices are connected to them. Network access points, which are no longer required, are also deactivated or monitored in an appropriate manner in order to detect and prevent unauthorised devices from being connected as soon as possible. Any access with unauthorised devices is documented and automatically stopped. We are proud of ensuring the security of our IT-systems and data in this way.

4.6 Management and evaluation of company assets

Information security was ensured comprehensively. A detailed inventory list was drawn up containing all relevant information. Every piece of this information was assigned to an Information Manager who determined the level of protection based on a carefully developed classification scheme. This ensures that all the information is adequately protected and the safety objectives of information security, such as accessibility, confidentiality and integrity have been fully considered.

In order to ensure that the protective measures are continuously updated and improved, the inventory list is regularly reviewed by the Information Managers. This review is carried out at least once a year to ensure that the classification of information and the protective measures applied are still relevant and appropriate.

The consistent implementation of this inventory and classification process has ensured that all necessary protective measures have been identified and implemented to ensure information security and organisational know-how. The organisation can therefore be sure that its information is adequately protected and potential risks are effectively minimised.

4.7 Suppliers

While working with co-operation partners and contractors, it is very important that an appropriate level of information security is maintained. Our strict rules for information security apply here, especially when it comes to our customers' data, which must be handled in accordance with its protection requirements. We assess contractors based on their protection requirements and assign them to a certain protection level. In order to ensure compliance with information security, we must conclude at least one non-disclosure agreement and a declaration of information security commitment with contractors on the "high" and "very high" protection levels. The document "3.0 - 41 Information Security Guideline" contains a binding regulation. Compliance with this regulation is regularly reviewed and documented.

4.8 Data protection

As part of our business activities, we obtain personal data from the contacts of our customers and suppliers. We documented the regulations for handling personal data and data protection in a data protection manual. Compliance with and implementation of the requirements of the German „Datenschutzgrundverordnung” (DSGVO) - General Data Protection Regulation (GDPR) and the German „Bundesdatenschutzgesetz” (BDSG) - Federal Data Protection Act is monitored by our external Data Protection Officer, Kutzschbach. Enquiries regarding data protection are solely answered by the external Data Protection Officer.

4.9 Training of staff

There is a potential risk if staff are not informed about the requirements and risks of information security and consequently commit misconduct. It is therefore essential that information security is understood and practised as an integral part of the company.

Staff are invited to the planned training programmes in accordance with our training concept. Participation in the training courses is generally mandatory. However, the management may authorise exceptions for individual staff in special cases.

5. USE AND HANDLING OF INFORMATION TECHNOLOGIES

5.1 IT-Security

5.1.1 General principles

Please note that personal data and business data may only be saved in the drives, directories and folder structures of IT-systems provided for this purpose. Staff are only authorised to create subfolders within this structure. The sole data storage of original data on local data carriers such as mobile hard drives or memory sticks is not permitted. Copies may be made if necessary.

It is also advisable to regularly delete files and e-mails that are no longer required.

5.1.2 Connection of external IT-systems

In accordance with the IT-security guidelines, connections from interconnected PCs to external systems and networks may only be established via the connecting paths that are approved and controlled by the persons in charge. This particularly applies to Internet access (e.g. in hotels, at airports, railway stations or on trains) for which Wi-Fi connections are permitted to the necessary extent, provided that the protective mechanisms provided therefor are available, updated and functioning.

It is of the utmost importance that the security measures against unauthorised access to the company's IT-infrastructure are always updated. In order to minimise the risk of security breaches, the connecting paths defined and controlled by the IT-Department must be used.

Using public Wi-Fi connections poses an increased risk, as unencrypted connections or vulnerabilities in network security may be utilised. For this reason, the provided protective mechanisms, such as firewall and antivirus software, must always be updated and functioning in order to ensure the security of the IT-infrastructure.

Failure to comply with the above IT-security guidelines may have serious consequences and lead to legal action. It is therefore essential that all staff adhere to these guidelines and informs the IT-Department immediately in the event of any questions or problems.

5.1.3 External communication resources

External computers, i.e. computers from third parties that are not under the control of the company's own Managers, may not be connected to the company network without the Manager's permission. Such permission must be obtained by the responsible department if necessary. If it is necessary to grant third-party or cooperation companies access to personal or confidential data, this may only be done upon the instructions of the person in charge of the department or the owner of the information and only to the extent that is absolutely necessary. Access must be granted via secure connections using reliable user identification and authentication and only after the approval by the IT- Manager or staff that are authorised by him/her. The security measures must be defined depending on the protection requirements of the data and the associated risks if access is granted.

Service partners may only be granted access via defined secure access points and paths with secure and reliable authentication. If external companies or other persons require access to security areas or personal or confidential data or information, these persons must be appropriately monitored during their activities. The details and security requirements must be regulated in the corresponding contracts and, if necessary, in confidentiality agreements. The authorisations to be granted must be carefully considered taking the protection requirement of the data and information into account and may only be granted to the smallest extent possible. The activities of these partners must be documented and reviewed in an audit-proof manner if possible.

5.1.4 Removable storage media

The following regulations must be observed in order to protect personal and other confidential company data when mobile data carriers are used:

- Only copies of company data may be saved on mobile data carriers such as mobile disc drives, USB sticks, memory cards and CDs/DVDs in order to prevent data loss. If personal or otherwise confidential data is saved, it must be encrypted.
- Only mobile data carriers that have been authorised or provided by the IT-Department for business purposes may be used. The allocation and destruction of mobile data carriers must be documented in an audit-proof manner.
- Mobile data carriers must be regularly checked for viruses, especially after having been connected to external systems, data storage from external sources or before transferring external data into the company's own systems.
- Data may only be passed on and copied to external data carriers within the scope of the confidentiality guidelines and only to the extent that is absolutely necessary in order to fulfil operational tasks.
- Personal or other confidential data must not be saved unencrypted on removable storage media.
- Mobile data carriers must always be stored securely and must not be left unattended.
- Only mobile data carriers that do not contain any personal or confidential data may be used to connect to external computers. If possible, these mobile data carriers should be write-protected and used in a write-protected state.
- Data on mobile data carriers that is no longer required must be deleted immediately.

5.1.5 Firewall and antivirus software

In addition to the essential security measures, all computers and laptops are protected by a locally installed firewall and internet security software. Corresponding instructions and user information are available. This ensures that the devices are adequately protected even if the internet is accessed externally. In order to ensure the continuous security of the devices, it is prohibited to install or operate security software that has not been approved by the IT-Department. The configuration of the protection software must not be changed and it is strictly forbidden to deactivate or uninstall the protection software. The automatic update of the protection software in particular must not be deactivated or changed, and the devices may only be connected to the Internet when the protection status is updated.

The configuration of the firewall and its functionality must be checked at appropriate intervals by the department in charge.

5.1.6 Passwords

Access to data processing procedures is only permitted via a secure login procedure, which must be specially designed for sensitive procedures to display the date and time of the last successful or unsuccessful login attempt and to document unsuccessful login attempts. Users are identified and authenticated by a personal login assigned to each staff member plus an additional password. The password is the key to identifying the authorised user and must therefore be treated confidentially. In order to ensure the security of the password, certain rules must be observed, which must be sufficiently automated and enforced. Access must be blocked after three to five unsuccessful login attempts and may only be authorised again once the user has been identified beyond doubt.

5.1.7 Unauthorised access to company assets

In rooms open to the public, IT-workplaces must be arranged in such a way that third parties cannot see the screens directly. If necessary, the monitors must be fitted with privacy screens to prevent unauthorised views. Printers may only be set up in secure areas that are inaccessible to unauthorised persons. After printing, printouts must be removed from the printer immediately. For confidential matters in particular, confidential printing functions should be used if possible. If the user leaves the workplace, he/she must log out of the system or activate the keyboard/screen lock (password-protected screen saver). Regardless of this, the lock must automatically be activated after a period of five to ten minutes without any user input. Data carriers, printouts or other documents with confidential or strictly confidential content must always be locked in if the user leaves the workplace. End devices such as PCs or printers must be switched off at the end of the working day. Notebooks that are not secured by a cable lock must be locked in at the end of the working day. Unless other regulations apply, lockable individual offices must be locked when the staff are leaving.

5.1.8 Identification of staff members

The HR-Department is responsible for issuing means of identification such as keys and fingerprints. The IT-Department is responsible for issuing, managing, returning and destroying means of identification in the form of software/hardware tokens to ensure access to the company environment. The time limit for means of identification depends on the respective access areas. If means of identification are lost, this must be reported immediately to both the HR-Department and the IT-Department.

5.1.9 Visitors

In accordance with the applicable regulations, visitors who visit a specific location or person within the company are registered in a visitor information system. The name of the visitor and the start and end time of the visit must be documented. The monitoring of visitors within the company is necessary to ensure security. For this purpose, visitors must be supervised within the security areas. In order to further ensure the security of the company areas, visitors must not carry any mobile phones or other image or sound recording devices within the security areas. The specific provisions for implementing these measures are the responsibility of the Department Manager in charge of the respective security area.

5.2 Security incidents

5.2.1 Theft and loss of devices provided by the company

In accordance with the employment contract, staff are obliged to secure the devices entrusted to him/her against theft. In the event of theft or other loss of mobile devices or data carriers, it is the responsibility of the staff to inform their superior and the responsible IT-Department immediately. They must then initiate the necessary measures.

5.2.2 Conduct in the event of system failures and malfunctions

According to the definition, security incidents are incidents involving the loss or risk of loss or destruction of data or its confidentiality, integrity, authenticity and auditability. Such incidents must be reported to the Information Security Officer.

In the event of a security incident or a suspicion thereof and in the event of other malfunctions, please proceed as follows:

- Any failure or malfunction of IT-systems must be reported immediately to the IT-Manager/IT-Security Officer, regardless of the type and severity of the incident and the number of affected systems/workplaces. Depending on the nature of the incident, the IT-Manager/IT-Security Officer decides on the further course of action and on the departments to be notified or involved, e.g. departments responsible for the subject matter, HR-Department, Data Protection Officer, etc.

- Each incident must be documented with regards to type and extent, affected procedures, data and departments or sites.
- The way in which the incident was dealt with and rectified and the legal, organisational and technical measures that were initiated must be documented.
- The damage caused by the incident must be assessed. Non-material damage must also be taken into account, e.g. the impact on customers, staff, public image, etc., and a damage report must be prepared.
- The causes of the incident must be analysed and, if possible, measures must be derived from it and put in place to prevent similar incidents in the future.
- In the event of a loss of data confidentiality, any obligations to inform affected persons and the data protection supervisory authority must be observed.
- Staff may not attempt to clear up the incident themselves or take action against the person who caused it. The following must always be observed:
    - Running programmes must be closed down.
    - New programmes may no longer be started.
    - No more data or e-mails may be sent.
    - System instructions and system messages must be documented.
- The documentation of security incidents must be regularly analysed statistically and evaluated with regards to the type, scope, costs and risk potential of the incidents. Measures to prevent similar incidents in the future and to improve information security must be derived from the analyses in order to gain knowledge from such incidents.

5.3 Data protection and backup procedures

5.3.1 Backup of central databases

The central data backup is carried out on the basis of a defined backup concept onto designated systems and data carriers.

5.3.2 Backup of local data carriers

Data on local hard drives, e.g. on desktop-PCs or other mobile data carriers, is not backed up and is lost in the event of damage. Unsecured drives, e.g. local or personal drives, must therefore not be used as the sole storage location for business-critical data.

5.3.3 Resignation, transfer and absence of staff

Prior to a resignation, a transfer or an absence, every staff member is obliged to hand over all documents and data that are still relevant to the company and must be preserved and to delete private data or files that are no longer required. The transfer of relevant data and documents must be confirmed by the superior and the deletion of private files must be confirmed by the staff member.

5.4 Management of user accounts

In accordance with these provisions, users may only access those programmes, drives, folders and files that are necessary in order to fulfil their operational tasks. This is ensured by individual rights and authorisations for the systems and applications used. The allocation of authorisations must be handled restrictively and only to the necessary extent. Staff are prohibited from using system functions and ranges of data beyond the scope of their assigned work tasks, even if this is possible due to the inadequate assignment of rights or technical deficiencies. If this is the case, the superior or the IT-Manager/IT-Security Officer must be informed. User accounts and access rights are set up by the IT-Administration department at the written request of the superior. This request must specify the applications to be authorised and the required rights. Any requests to create or deactivate user accounts and to grant or withdraw user rights require a written request in order to ensure appropriate documentation. Staff are not permitted to have administrator rights unless there are good reasons for granting them. Should this become necessary, administrator rights may only be used to the extent necessary for operational tasks. Security-relevant settings or default system settings must not be changed.

If staff leave the company, are transferred or change tasks and responsibilities, the deletion of authorisations that are no longer required must be initiated immediately by the respective superior. New access rights must be assigned and set up in accordance with the new job description. In order to check the assignment of rights, the superior must carry out a check at regular intervals, for example annually or every six months, in order to ensure that the authorisations that are in place are still necessary. Authorisations that are no longer required must be deleted. External users may only log in to the company network using a 2-factor authentication.

5.5 Protection against malware

Certain guidelines must be observed in order to prevent damage caused by malware and spyware. Connecting interconnected PCs to external networks outside the company is only permitted to the necessary extent following security checks and approval by the IT-Administration and the protective measures set up by IT must be available, updated and functioning. Virus scanner alarms, computer abnormalities and system events or other abnormalities that indicate the activation of unknown software must be reported immediately to the IT-System Administrator. Unauthorised changes to security settings are not permitted. If a virus is suspected, certain steps must be followed and the IT-Administration must be informed immediately. The rules on data protection must also be observed when using e-mail and the Internet.

5.6 Transfer, deletion and disposal of devices and data carriers

5.6.1 Transfer of electronic data carriers

In accordance with designated procedures and in compliance with the authorisations, data carriers may only be passed on to authorised persons. Any deviations from this require prior authorisation by the department in charge. If personal or other confidential data is involved, the recipient of this data must confirm its receipt. If data carriers are posted, a reliable dispatch route must be selected that ensures complete traceability of the dispatch and postal receipt of the data carriers. Before sending personal or other confidential data by post, the data must be encrypted.

5.6.2 Deletion and disposal of data carriers

- **Deletion**

There is an obligation to delete all personal and other company data immediately as soon as it is no longer required for the fulfilment of the task in question and no retention periods are applicable or such periods have already expired. The instructions for the deletion must be given in writing by the responsible department, taking into account any existing retention periods or the retention interests of the company or affected persons. Secure deletion procedures and deletion software programmes must be used for the deletion of data from electronic data carriers, which ensure reliable and non-recoverable deletion by overwriting the saved data several times.

- **Destruction**

If data carriers are destroyed and disposed of, all necessary precautions must be taken to ensure that no personal data or other confidential data is made available to unauthorised persons. The applicable data protection regulations must be observed. Service companies commissioned with the destruction of data carriers are obliged to comply with the regulations on data processing during their commission. Electronic data carriers that are to be disposed of must be handed in by the user at the collection point set up by IT. There they will be collected, processed or destroyed or disposed of in an appropriate manner. If the data carriers contain personal data or data that is classified as confidential in accordance with the confidentiality guidelines, this data must be completely deleted from the data carrier by using a state-of-the-art deletion software programme before they are being passed on for destruction. If a data carrier is no longer accessible due to a defect, it must be destroyed. In warranty cases or in other special circumstances, the IT-Security

Officer may make a different decision depending on the individual case (e.g. type of data carrier, type and sensitivity of the saved data, warranty case or repair exchange), taking into account the security requirements. If a data carrier contains particularly sensitive or other particularly confidential data (e.g. personal data) that cannot be securely deleted, the data carrier must be destroyed in any case.

- **Disposal**

Due to the fact that confidential information may also exist on paper, a careful collection of waste paper and a reliable way of disposal are mandatory, including a written confirmation of the destruction carried out in accordance with data protection. The specifications for the destruction of paper are regulated in the German DIN standard 66399. According to this standard, the destruction of classified documents categorized as protection category 2 and security level 4 is mandatory. These requirements must be met if paper is disposed of and the disposal company must issue a written confirmation that the destruction has been carried out in accordance with data protection regulations.

6. REVISION

In accordance with this guideline, a regular review must be carried out to ensure that it is up-to-date, complete and complies with the existing legal, technical and organisational conditions. This review must be carried out every twelve months and, if necessary, additions or updates must be made.