## ANNEX 6

## *Model security document*[[1]](#footnote-1)1

|  |  |
| --- | --- |
| Date of security document version | dd/mm/yyyy |
| Security document version | XXX |

**Security document for the files of...............**

*(Indicate the controller)*[[2]](#footnote-2)2

**Confidentiality notice**

This document, as well as other documents and information relating to the security measures for the files of.................... (*indicate the controller*), may be accessed only by the persons designated in this document, notwithstanding that compliance with obligations arising from the regulation on the right to the protection of personal data, and any other applicable rules, implies access to this document by third parties.

***Structure of the security document***

This document and its annexes include the technical and organisational measures necessary for guaranteeing the security of the data and processing operations in relation to files under the responsibility of ……………… (*indicate the data controller*). These measures are aimed at preventing the alteration, loss, non-authorised processing and access to the data they contain and to guarantee the availability of same.

* **General part**

*(Include the more general aspects of the security measures and those less likely to change over a short period of time)*

1. Document scope of application
2. Regulations applied and applicable security measures
3. Staff functions and obligations
4. Structure of files and description of processing systems
5. Incident management
6. Backup copies
7. Media and document management
8. Destruction of information and reuse of media
9. Auditing
10. Revision of security document

* **Annexes**

*(Include in the annexes technical descriptions, information, regulations, procedures, registers, etc., which are likely to change over time. You can identify these with a descriptive code of the type of information they contain, for example, INF (information relating to the data security, or REG (registers and/or inventories. If attached to security documents, these annexes can be in electronic format).*

|  |  |
| --- | --- |
| ***Document code***  ***(indicate code / classification used)*** | **Description**  *(indicate the name of the annex document)* |
| *INF001* | *Description of the computer system, technical characteristics of the hardware and software* |
| *INF002* | *Users and data access authorisations* |
| *INF003* | *Structure of the files* |
| *INF004* | *Delegation of authorisation* |
| *INF005* | *Data processors* |
| *INF006* | *Service providers without access to data* |
| *REG001* | *Delivery of security document* |
| *REG002* | *Register of incidents* |
| *REG003* | *Register of backups* |
| *REG004* | *Media inventory* |

**1. Document scope of application**

This security document was prepared by.................. (*indicate the data controller*), which is responsible for the files described below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **File description** | **Registration code** | **Date of registration** | **Security level** | **Processing  system** |
| ..................  (indicate the file description, e.g.  ‘students  ‘staff’  ‘suppliers’, etc. | ......................  (indicate the registration code assigned to the file) | dd/mm/yyyy  (indicate the date of file registration) | ..............  (indicate security level of file - low/ medium/high) | ..........................  (indicate the  automated/non- automated/partially automated system in which the information system is organised |

This document must be kept permanently up to date. Any significant modification will require a revision of the document and, if necessary, a partial or total update.

**2. Regulations applied and applicable security measures**

The following regulations were taken into account in the development of this security document:

* Art. 9 of Organic Law 12/1999, of 13 December, on the protection of personal data
* Art. 79 to 114 of the implementing Regulation of the LOPD (RLOPD), passed by Royal Decree 1720/2007, of 21 December
* Third paragraph of the 23rd additional provision of Organic Law 2/2006, of 3 May, on Education
* 14th additional provision of Law 12/2009, of 10 July, on Education
* ......................... (*indicate, if appropriate, any other applicable regulation*)

The security measures provided for in the RLOPD, and those specified in this security document, are applicable to the different files referred to in this document, in accordance with the level of security described for each one in section 1 of this document.

The measures described in this document for each security level are of an accumulative nature; that is, for each level not only the measures specifically indicated for that level must be applied, but also those corresponding to lower levels.

Non-compliance with this security document may be subject to a penalty, in accordance with..................... (*indicate the applicable penalty system).*

**3.Functions and obligations of the persons authorised to process the data**

The persons who have access to, or who process the data contained in the files of……………………………………….. (*indicate the data controller*) must know and must comply with the security measures and related obligations described in this security document.

To this end, a copy of the current security document[[3]](#footnote-3)3 must be delivered with the warning that it is a confidential document and that its contents must be kept in strict confidentiality. In order to access the data, the document must be signed upon receipt.

General obligations for persons with access to the data contained in the files:

1. Know and comply with, where applicable, the provisions of this security document.
2. Notify................... *(indicate the person or service that needs to be informed)* of any incident that could affect the security of the data.
3. Keep secret and confidential the personal data contained in the files.

Annex document.................. *(indicate the code used to designate the annex document relating to “Delivery of the security document”. Using the example of the annexes in this model, this would be document REG001)* lists the people who have received the security document, along with the date and signature of receipt.

Personnel external to................... *(indicate the school or organisation concerned)* who have access to the data are subject to the same conditions and obligations as in-house personnel, and to the specific provisions contained in this security document and those included in the data processing agreement or contract.

In the event of non-compliance with the provisions of this document, the................... *(indicate the data controller)* reserves the right to initiate the legal proceedings they deem appropriate in order to protect their interests or those of third parties.

3.1. Data access control

Staff may only access the data and resources necessary for performing their functions. The persons authorised to access the data contained in the files, and the operations that each may perform, are listed in annex document.................. *(indicate the code used to designate the annex document relating to “Users and data access authorisations”. Using the example of the annexes in this model, this would be document INF002).* Persons with access to the data may only use such data in relation to the functions assigned to them.

In order for people not mentioned in this security document to be able to access the information, they will require the authorisation of the data controller (or persons delegated by the same) or the security manager.

|  |
| --- |
| HIGH LEVEL **ACCESS LOG**  AUTOMATED FILES  For each access to data in high-level files, the user’s identity must be registered, together with the date and time of access, the file that was accessed, the type of access, and whether access was authorised or denied. If access was authorised, the information that allowed identification of the register accessed.  ........................... *(state any other information relevant to the access registration system)*  The information in the access log must be kept for.................... *(specify the period, which must be at least two years).*  This access log is under the direct control of the security manager. It must not be disabled under any circumstances.  The security manager must check the registered control information at least once a month and prepare a report.  ............................ *(describe the procedure for preparing the monthly report on the access log for high-level data, as regulated by article 103 of the RLOPD).*  NON-AUTOMATED FILES  Access to documents is restricted exclusively to the authorised personnel named in annex document.................. *(indicate the code used to designate the annex document relating to “Users and data access authorisations*”. *Using the example of the annexes in this model, this would be document INF002).*  The mechanism used for identifying access to related documents is..................... *(indicate the types of documents that can be used by multiple users, and the mechanism established to control access to them).* |

3.2. Identification and authentication

Each user that is authorised to access the data contained in the files is assigned a personal username and password that identifies them unequivocally and allows them to verify themselves on the equipment needed to access the information.

.............................. *(indicate the data controller or, where applicable, the security manager)* is responsible for registering and de-registering users on the system and providing them with a username and the password assigned....................... *(indicate how this information will be provided to ensure confidentiality).* The password assigned and the changes made must be stored encrypted.

The passwords assigned must meet the following characteristics: ............................ *(indicate the characteristics of the passwords. The password should have a minimum of 8 characters and a combination of uppercase and lowercase letters, numbers and, if the system allows, symbols)*.

The passwords must be changed the first time the user logs on to the computer and before accessing or processing the data contained in the files. Similarly, all users must change their password every................... *(specify the period, which must be at least once a year).*

|  |
| --- |
| MEDIUM OR HIGH LEVEL  For medium and high-level files, the possibility of repeatedly trying to gain non-authorised access to the information system is restricted in the following manner .................... *(state the mechanisms, such as blocking the username after three failed attempts to gain access).* |

3.3. Security manager

..................... *(indicate the person/persons designated)* is/are designated as security manager/s, and will coordinate and monitor the measures established in this security document in relation to...................... *(indicate whether the designation relates to all files or not. In the case of the latter, please specify),* classed as medium or high level.

In no circumstances does designation imply an exemption of the liability corresponding to................... *(indicate the data controller)* as data controller, pursuant to the RLOPD.

This designation is for a period of................. *(indicate the period for which the position will be held).* After this period, the same person may be reappointed as security manager or else a different person.

Annex.................... *(indicate the annex, if applicable, that includes the appointments (the original or a copy) that affect the different profiles in this security document)* includes ................... (*the* *original or a copy)* of the appointment of the security manager.

The security manager must carry out regular checks, at least every................... months, to verify compliance with the provisions of this security document.

3.4. Provision of services by third parties with access to data

The provision of services by third parties or entities that involves access to personal data in the files or systems for which................. *(indicate the data controller)* is responsible*,* requires the signing of a data processing agreement or contract as referred to in article 12 of the LOPD, and is considered a data processing service.

Annex document.................. *(indicate the code used to designate the annex document relating to “Data processors”, Using the example of the annexes in this model, this would be document INF005),* details the third parties acting as data processors on behalf of .....................*(indicate the data controller),* indicating whether the information necessary to provide the service is processed at the premises of ..................... *(indicate the data controller)* or at the premises of the third party processing the data, and the data processing agreement or contract signed and its validity.

The data processor must keep secret and confidential the personal data contained in the files they have access to for the provision of the contracted service.

3.4.1. *Processing data at the premises of the.................. (indicate the organisation to which the data controller belongs):*

If, in accordance with the signed data-processing agreement or contract, the service is provided on the premises of................... *(indicate the organisation to which the data controller belongs)*, access by the data processor to the data files and systems must be done using the resources and information systems provided by.................... *(indicate the data controller).*

The personnel of the data processor must comply with the security measures provided for in the RLOPD and in this security document, in accordance with the level of security described for each of the files in section 1 of this document. For this purpose, a complete and current copy of the security document must be delivered and certified in annex document.................. *(indicate the code used to designate the annex document relating to “Delivery of the security document”. Using the example of the annexes in this model, this would be document REG001*).

The data in the files accessed for the provision of the service must not be removed from the premises of.................... *(indicate the organisation to which the data controller belongs):*

Removal of the files from the premises of.................... *(indicate the usual workplaces)*, or incorporating them into portable devices, must be authorised pursuant to Annex......... *(indicate the code used to designate the annex document relating to “Users and data access authorisations”. Using the example of the annexes in this model, this would be document INF002)* of this security document*.* In these cases, the corresponding level of security must be guaranteed.

Once the provision of the service is complete, the data processor must destroy or return the copies of the data and, if applicable, the media that contains them, pursuant to Annex................... *(indicate the code used to designate the annex document relating to “Data* processors”. *Using the example of the annexes in this model, this would be document INF005)* of this security document.

If it has been agreed that the data processor will return the personal data to the data controller or to another processor that the latter has designated, and, if applicable, also the media that contain them, the data processor shall ensure that all the data has been completely erased from the computer equipment used by them to provide the service, in order to prevent reuse of the same.

If it has been agreed that the personal data and, if applicable, the media that contain them, must be destroyed, this destruction must be carried out in accordance with the procedure described in section 8 of this security document and must be certified in writing. This certification must be provided to.................. *(indicate the data controller)* as soon as possible.

Remote access to the data by the data processor, if stipulated in the signed data processing contract or agreement, is carried out through the authentication system for registered users, as described in section 3.2 of this security document.

The data processor must report................... *(indicate the person or service to be informed of an incident)* any incident that could affect the security of the data, pursuant to the procedure described in section 5 of this security document.

3.4.2. *Processing data at the data processor’s premises:*

*(The security document must include the cases where the data necessary for providing the contracted service will be incorporated and processed exclusively in the data processor’s systems, in accordance with the signed data processing agreement or contract).*

If, pursuant to the signed data processing agreement or contract, the data contained in the files for which.............................. *(indicate the data controller)* is responsible, necessary for providing the service, are processed at the data processor’s premises and exclusively using their systems, the data processor shall develop a security document or adapt their own security document, if applicable, specifying:

* The files affected by the provision of the service
* The data controller
* Processing conditions, especially the security measures established in the data processing agreement or contract
* Validity period of processing

The data in the files accessed for the provision of the service cannot be removed from the data processor’s premises. In the event that it is necessary to change the location where the data are processed, the processor must first inform...................... *(indicate the data controller).*

To process the data outside the data processor’s premises, or to incorporate them into portable devices, this must be authorised pursuant to Annex................... *(indicate the code used to designate the annex document relating to “Users and data access authorisations”. Using the example of the annexes in this model, this would be document INF002)* of this security document*.* In these cases, the corresponding level of security must be guaranteed.

The data processor must note any security incidents in their incident register and must immediately inform................... *(indicate the person or service to be informed of an incident),* of any incident that occurs during the execution of the contract that might affect the security of the data, in accordance with the procedure described in section 5 of this security document.

If the provision of the contracted service involves the processing of data in medium or high-level files the data processor must inform...................... *(indicate the data controller)*, as soon as possible, of the identity and professional profile of the person (or persons) designated as security manager.

The data processor shall submit to compliance audits in relation to data protection regulations, decided by...................... *(indicate the data controller)* at the beginning of the service provision, every ....................at least *(indicate the period, which for files classified as medium or high level must be at least every two years)* and, in any case, whenever there are substantial modifications to the information systems.

Once the provision of the service is complete, the data processor must destroy or return the copies of the data and, if applicable, the media that contains them, pursuant to Annex................... *(indicate the code used to designate the annex document relating to “Data* processors”. *Using the example of the annexes in this model, this would be document INF005)* of this security document. All this notwithstanding that they may keep a copy, blocked, for the purpose of dealing with any liability that might arise from the processing.

If it has been agreed that the data processor will return the personal data to the data controller or to another processor that the latter has designated, and, if applicable, also the media that contain them, the data processor shall ensure that all the data has been completely erased from the computer equipment used by them to provide the service

If it has been agreed that the personal data and, if applicable, the media that contain them, must be destroyed, this destruction must be certified in writing. This certification must be provided to.................. *(indicate the data controller)* as soon as possible.

3.5. Provision of services by third parties with access to data

The service provider shall inform their personnel about the measures detailed below and to keep proof of compliance with this duty.

The personnel of companies contracted to provide services that do not involve the processing of personal data cannot access the data contained in the archives, documents, files and information systems of.................... *(indicate the data controller).*

The personnel of the service provider who require access to the premises of.................... *(indicate the data controller)* must..................... *(indicate the system/control of physical access to the premises).*

Annex..................... *(indicate the code used to designate the annex document relating to “Service providers without access to data”. Using the example of the annexes in this model, this would be document INF006)* lists the service providers of.................... *(indicate the data controller)* without access to personal data.

Access to the places where....................’s *(indicate the data controller)* servers are located must..................... *(indicate the system/control of physical access to servers or archives where the data is located).*

Access to documents is restricted exclusively to the authorised personnel named in annex document.................. *(indicate the code used to designate the annex document relating to “Users and data access authorisations”. Using the example of the annexes in this model, this would be document INF002).*

The service provider must immediately inform...................... *(indicate the person or service to be notified)* of any incident that occurs during the execution of the service that might affect the integrity or confidentiality of the personal data processed by...................... *(indicate the data controller),* in accordance with the procedure described in section 5 of this security document.

This circumstance must be noted in the incident register.

In the event of accidental access to personal data, the service provider’s personnel are obliged to keep this secret, even after the contractual relationship has ended. In no circumstances may they use the data or disclose them to third parties.

3.6. Delegating permissions and monitoring functions

Annex................... *(indicate the code used to designate the annex document relating to “Delegating permissions*”. *Using the example of the annexes in this model, this would be document INF004*) lists the persons to whom the data controller has delegated the permissions mentioned therein.

**4. Structure of files and description of processing systems**

The structure of the files is detailed in annex.............. *(indicate the code used to designate the annex document relating to “Structure of files and description of processing systems”. Using the example of the annexes in this model, this would be document INF003).*

The processing system for file data is partially automated, as some data is contained in computer files, according to the characteristics described in documents ................. and ..................., *(indicate the codes used to designate the annex document relating to “Description of the computer system. Technical characteristics of the hardware and software” and to “Structure of files and description of processing systems”. Using the example of the annexes in this model, these would be documents INF001 and INF003, respectively),* and some information is paper-based, either as a medium for data collection or printed outputs from the computer system.

The level of the security measures implemented for each file are those specified in section 1 of this document, pursuant to the data protection regulations for automated and non-automated processing.

The data in the files can be subject to any operation in relation to their purpose. Therefore, in accordance with that established in annex.................. *(indicate the code used to designate the annex document relating to “Users and data access authorisations”. Using the example of the annexes in this model, this would be document INF002),* authorised users can collect, register, store, develop, modify, consult, use, cancel, block or delete data and, where applicable, can pass on data to third parties as a result of data communications, consultations, interconnections or transfers.

These operations are performed with respect to both automated and non-automated media, in each case adapted to the specific processing system.

4.1. Information system

The file information system is based on........................ *(indicate, for all files or for each one, the name of the computers/servers on which the database and/or media containing the files is located, with a brief description of the data they contain).*

The file information system is complemented with a paper-based archive in which the documents relating to....................... *(indicate, for each file, what information is on paper)* are archived in organised manner.

4.2. Working copies of documents or temporary files

A partial or full working copy of the files or paper-based documents, for a specific or auxiliary task relating to the purposes of the files, is considered a “temporary file”. The level of security that needs to be applied to this file, will be that specified by the criteria laid down in the RLOPD and that established in this security document.

Once the temporary task has been completed, the working copy of the file or the document must be destroyed, pursuant the procedure described in section 8 of this document.

4.3. Working procedure outside the premises of............*(indicate the usual workplaces).*

The personal data contained in the files.................... *(indicate the files affected by the processing)* may be processed outside the premises of....................... *(indicate the data controller)* in the following circumstances: ..................... *(indicate the circumstances in which the data can be used outside the data controller’s premises).* Portable devices can be used in the following circumstances: .......... *(indicate the circumstances in which portable devices can be used).*

The persons authorised for this purpose are listed in annex........... *(indicate the code used to designate the annex document relating to “Users and data access authorisations”. Using the example of the annexes in this model, this would be document INF002).*

4.4. Access to data via communications networks

The following files can be accessed via communications networks...................... *(list the access expected and the files that can be accessed).*

When accessing files via communications networks, measures must be taken to ensure a level of security equivalent to that required for access in local mode.

|  |
| --- |
| HIGH LEVEL  The communication of personal data contained in high-level files that are transmitted across public networks or wireless communications networks must be.......... *(indicate whether the data are transmitted encrypted, or are sent through mechanisms other than the encryption of information, that ensure that the information is unintelligible and cannot be manipulated by third parties).* |

**5. Managing incidents**

A “security incident” means any breach of the applicable regulations or the provisions of this security document, or any other anomaly that affects or might affect the security of the personal data of...................... *(indicate the data controller).*

......................... *(indicate the persons obliged to report the incident, such as those authorised to access the files)* must report the incident as soon as possible to............................. *(indicate the person or service to inform about the facts or circumstances that may, or are certain to, affect the security of the data).*

This communication must be made........................ *(indicate how the incident should be reported: orally, in writing or by any other means deemed appropriate).*

....................... *(indicate the person or service that manages incidents)* handles the reports received, evaluates them and, if necessary, takes the appropriate measures to rectify the situation detected.

....................... *(indicate the person or service managing incidents)* must note in the incident register (see annex document ............) *(indicate the code used to designate the annex document relating to* *“Incident register”. Using the example of the annexes in this model, this would be document REG002*) the following information regarding the incident detected:

1. Type of incident
2. The moment in which it occurred and was detected
3. Who reported it
4. To whom was it reported
5. Consequences
6. Corrective measures taken or proposed

|  |
| --- |
| MEDIUM AND HIGH LEVEL  The incident register must also include a record of the data recovery operations that affect medium or high-level files................... *(provide details of the procedure followed to recover the data, indicating the person who has carried it out, the data recovered and, if applicable, the data that had to be manually registered in the recovery process. In the case of automated management,* *for information relating to incidents a specific code is needed for the recovery of the data).*  For data recovery procedures for these files, written authorisation must be provided by................... *(indicate the data controller).* |

**6. Backup and recovery copies**

6.1. Backup copy

A backup copy of the files must be made.................. *(indicate the frequency, which must be at least once a week),* unless the data has not been modified during this entire period.

This process consists of copying the files to an external device, following the procedure below:

The backup process must ensure that the files are restored to same state they were in at the time the potential loss or destruction of data occurred.

The backup copy must be made by.................... *(indicate the person or service in charge of making backup copies).*

Every six months...................... *(indicate the person or service responsible for checking this process)* must check that the backups have been done correctly and that the data can be restored. To do this, the backup and recovery procedures must be performed without affecting the current data. The resulting files must be deleted once done the checks have been made.

If, between the date of the last backup and the date on which the recovery needs to be made, the information has been modified and can be retrieved manually from the paper-based documents, this fact must be noted in the incident register giving as much detail as possible.

If the hardware needs to be changed, the computers replaced or the data relocated to another type of file, a backup must be made first.

Testing with real data should be avoided, before establishing or modifying information systems. If this is not possible, a backup copy should be made first, the level of security corresponding to the processing carried out must be ensured and the tests must be recorded in this security document.

In document................. *(indicate the code used to designate the annex document relating to “Register of backups*”. *Using the example of the annexes in this model, this would be document REG003),* the date and time each backup copy was made, the person who carried it out and any other observations related to the process must be noted.

6.2. Recovery

If the backup copy needs to be used to retrieve information, the backup procedure must be followed in reverse, by copying the information from the external device to the computer folder where the file should be located.

If the recovery information is entered manually, this must be noted in the incident register.

|  |
| --- |
| MEDIUM AND HIGH LEVEL  To perform the data recovery procedure, the authorisation of the data controller is required.  In files containing medium or high-level data, the recovery must be noted in document............... *(indicate the code used to designate the annex document relating to “Incident register”*. *Using the example of the annexes in this model, this would be document REG002),* indicating the person who has carried out the process, the data restored and, if applicable, which data had to be registered manually in the recovery process. |

|  |
| --- |
| HIGH LEVEL  In high-level files, a backup copy of the data and the data recovery procedures must be stored in...................... *(indicate the location, which must be different to the location of the computer systems on which the data is processed and must comply with the security measures or use elements that ensure the integrity and retrieval of the information).* |

**7. Media and document management**

Media containing personal data must be identified by the type of information they contain, and be inventoried and stored in a location with restricted access pursuant to annex................... *(indicate the code used to designate the annex document relating to “Media Inventory”. Using the example of the annexes in this model, this would be document REG004)*, to which only people listed in said annex have access.

The media inventory includes the persons authorised to access each media.

In the event that, due to an emergency or force majeure, the media need to be accessed by unauthorised personnel, it is necessary to.................. *(describe the procedure for accessing premises in these circumstances).*

These obligations do not apply to the following media.................... *(name them)*, as their physical characteristics make compliance impossible.

The media must be stored in accordance with the following rules:...................... *(indicate the rules for labelling and storing the media).*

If the data needs to be transferred to an external medium (e.g. external hard disk, USB flash drive, CD or DVD, etc.) from the equipment where it is normally processed, this medium must be labelled with the name......................... *(indicate the name of the file and the date on which the data is being transferred, e.g., fileX\_dd/mm/yyyy),* so that the content and the date the data was copied can be easily recognised.

7.1. Storage devices for paper-based documents

For keeping paper-based documents containing personal data, the following storage elements can be used: ....................... (*filing cabinets or other storage elements used),* which must be locked with................... *(name the features they have to prevent them from being opened or, in their absence, the measures taken by the data controller to prevent unauthorised persons from accessing the information).*

|  |
| --- |
| HIGH LEVEL  Paper-based documents containing personal data must be stored in...................... *(filing cabinets, or other storage elements used),* that must be locked with....................... *(name the mechanism used to prevent opening, such as keys or other devices)* and located in the following areas:.................. *(indicate the place where the storage elements are located)*. These areas must be kept closed when the documents do not need to be accessed.  *(If it is not possible to comply with the above, the controller must take alternative measures to prevent unauthorised persons accessing the information and must describe these in this section of the security document).* |

7.2. Criteria for filing paper-based documents

Filing media or documents must be done in accordance with the following criteria: ...................... *(indicate the filing criteria stipulated in the relevant legislation or, in the absence of the same, those established by the data controller. In any case, the storage and location of the documents and consultation of the information must be ensured, as well as the possibility of granting the rights of access, rectification, opposition and cancellation).*

7.3. Custody of paper-based documents

When paper-based documents are not placed in the usual storage devices, which may only be the case if they are being worked on, the person using them must safeguard them and prevent them from being accessed by unauthorised persons. Special care must be taken not to leave papers on the desk, in other common areas or in areas that are freely accessible.

7.4. Removal of media and documents

Included in the media inventory are the authorisations for removing media and documents, including those contained in emails or on any mobile device, from.................... *(indicate the usual place for processing the information),* and the name of the person who has authorised it*.* It should include, separately, the removal authorisations for generic media and documents of periodic processes stipulated in the security document, and authorisations for the occasional removal of media and documents made specifically by the data controller.

Authorisation for the removal of the media must be provided in the following manner.................... *(indicate the authorisation procedure).*

During the physical transfer of media containing personal data, the following measures must be applied to prevent theft, improper access or loss of information: ..................... *(specify the measures and procedures established).*

The person transferring the media is responsible for its safekeeping. Therefore, they must act with the necessary diligence to apply these measures and to avoid incidents with the data. In any case,.................. *(indicate the data controller)* may give specific instructions for their protection if deemed appropriate. This fact should be noted in the media inventory.

|  |
| --- |
| MEDIUM AND HIGH LEVEL. **REGISTERING INCOMING AND OUTGOING MEDIA**  The incoming and outgoing of media related to medium and high-level files must be registered following this procedure:................... *(give details of the procedure for registering incoming and outgoing media).* The register of incoming and outgoingmedia is managed by.................... *(indicate whether the register should be stored manually or electronically)* and must include ....................... *(indicate the fields of the register, which must include at least: the type of document or media, the date and time, the issuer, the name of the documents or media included in the dispatch, the type of information they contain, the method of dispatch and the person authorised to receive it (incoming); the type of document or media, the date and time, the recipient, the name of the documents or media included in the dispatch, the type of information they contain, the method of dispatch and the person authorised to send it (outgoing).*  *(If the register is managed automatically, indicate in this section the computer system used).* |
| HIGH LEVEL. **MEDIA** **MANAGEMENT AND DISTRIBUTION**  The media must be identified with a label.................... *(indicate the criteria for labelling, which should be understandable for users authorised to access them and enable them to identify the content, while at the same time making identification difficult for other persons).*  The distribution and outgoing of media containing the personal data of high-level files must be.................. *(indicate the procedure for encrypting the data or, if applicable, for using a mechanism that guarantees that the information is unintelligible and cannot be manipulated while being transported. The data contained in portable devices must be also be encrypted, when outside the facilities under the control of the data controller).*  The following portable devices................. *(name those which do not allow data encryption),* because of.................. *(justify the reason*), instead of using encryption devices the following measures................... *(state the alternative measures to encryption, which must take into account the risks of processing data in unsecure environments)* must be applied. |

7.5. Copying or reproducing paper documents

Copying or reproducing documents containing the personal data of high-level files can only be carried out under the control of the authorised personnel named in annex........... *(indicate the code used to designate the annex document relating to “Users and data access authorisations”. Using the example of the annexes in this model, this would be document INF002).*

Rejected copies must be destroyed in such a way that makes it impossible to access the information they contain, as described in section 8 of this document.

**8. Destruction and reuse of media**

* 1. . Information contained in digital media

Digital media –such as internal or external hard drives, or USB flash drives– that need to disposed of or reused for other purposes must be reformatted.

This can be done using.............. *(indicate the chosen “secure” deletion software. The “secure” deletion of information in digital format using a specific software is based on overwriting the device multiple times so that it is virtually impossible to recover or reconstruct the information).*

Simply erasing or deleting a file is not enough, as this is not a secure procedure and the information could be retrieved by third parties.

As CDs and DVD devices are impossible to delete securely, they must be physically destroyed using a shredder............ *(state the location of the shredder),* to make them unusable.

If the device does not need to be destroyed or reused for another purpose, and all that is required is the removal of files or information stored on the computers, choose the “remove” or “delete” option and then empty the folder of eliminated messages or the computer’s Recycle Bin.

* 1. . Paper-based information

Paper-based documents containing personal data can be destroyed in the following ways:

1. By using the paper shredder located............. (*specify the location of the shredder, type and model, etc.)*.
2. By depositing the papers in closed containers identified as............... (*specify how these containers will be identified*) and located............... *(specify the location of the containers),* which can only be accessed by the authorised personnel of the company contracted for its secure destruction.

It is forbidden to throw documents containing personal information into bins or similar containers or to reuse them.

**9. Auditing**

|  |
| --- |
| MEDIUM AND HIGH LEVEL. **AUDITING**  *(Indicate the procedures to follow in order to carry out an internal or external audit, at least every two years, to verify compliance with Title VIII of the RLOPD, regarding security measures, in accordance with articles 96 and 110 in relation to automated and non-automated files, respectively.*  *An audit must also be carried out when substantial modifications have been made to the information system which could affect compliance with the security measures implemented, in order to verify adaptation, adequacy and effectiveness. The two-year period mentioned begins from the time of this audit.*  *The report must analyse the adaptation of the measures and controls to the LOPD and the RLOPD, identify any shortcomings, and propose the corrective or complementary measures necessary.*  *The security manager must analyse the audit reports and present the findings to the data controller, so that corrective measures can be taken. This report must be made available to the Catalan Data Protection Authority).* |

**10. *Revision of the security document***

This security document must adapt to the provisions in force in relation to the security of personal data and must be kept constantly up to date by means of a revision every two years.

It should also be revised and updated when there have been significant changes to the processing systems or to the information processed. Significant changes are understood to be those that could affect compliance with the established security measures.

The original and updated version of this security document is in the possession and under the control of....................... *(indicate the individual, area or department that has the original version).*

The following table sets out the changes and updates made to this security document, as well as the periodic revisions made to date.

|  |  |  |  |
| --- | --- | --- | --- |
| **Control of security document versions** | | | |
| **Version** | **Date** | **Content  update/revision** | **Revised by** |
| XXX | dd/mm/yyyy | ...............................  *(indicate the content updated or revised )* | ............................................  *(indicate the individual, the area or department that has revised or updated it)* |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control of annex versions** | | | | |
| **Annex** | **Version** | **Date** | **Content  update/revision** | **Revised by** |
| XXX | XXX | dd/mm/yyyy | ..............................  *(indicate the content updated or revised)* | .............................  *(indicate the individual, the area or department that has revised or updated it)* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Annex............**

|  |  |
| --- | --- |
| Annex INF001 version date | dd/mm/yyyy |
| Version | XXX |

|  |  |
| --- | --- |
| ***INF001*** | *Description of the computer system*  *Technical characteristics of hardware and software* |

Technical characteristics of the hardware and software used to process the file data....................*(write the name of the file).*

|  |
| --- |
| **HARDWARE** |

Computer brand and model:

Serial number:

RAM memory:

**Storage devices**

Internal hard drive [label] *(indicate capacity)*

CD *(yes/no)*

DVD *(yes/no)*

USB ports *(indicate number of ports)*

Disk drive *(yes/no)*

Other external ports / interfaces *(describe them)*

**Connectivity**

Connected to a local area network *(yes/no)*

Network interface Cable/Wireless

Connected to the Internet *(yes/no)*

Internet access service *(dedicated or shared network or ADSL*

*[with/without cable])*

**Other devices**

Printer *(yes/no)*

Scanner *(yes/no)*

|  |
| --- |
| **SOFTWARE** |

Operating system *(name and version)*

Antivirus *(yes (indicate name and version) /no)*

Firewalls *(yes/no)*

Internet Browser *(name and version)*

Email client *(name and version)*

**Office applications**

Word processor *(name and version)*

Spreadsheets *(name and version)*

Presentations *(name and version)*

**Other applications**

*(indicate functionality) (name and version)*

**Annex............**

|  |  |
| --- | --- |
| Annex INF002 version date | dd/mm/yyyy |
| Version | XXX |

|  |  |
| --- | --- |
| ***INF002*** | *Users and data access authorisations* |

List of users authorised to access files, indicating the processing operations they are authorised to carry out, both automated and non-automated.

**File**: *(enter the name of the file)*

User *(enter name and surname of the user)*

Position / function *(indicate position or function)*

Other external ports / interfaces *(enter only the username, not the password)*

**Authorisations**

Consult *(yes/no)*

Add *(yes/no)*

Modify *(yes/no)*

Cancel *(yes/no)*

Permanently delete *(yes/no)*

Print *(yes/no)*

Copy *(yes/no)*

Communicate *(yes/no)*

Unblock *(yes/no)*

Supervise making paper copies *(yes/no)*

**Technical operations**

Manage system *(yes/no)*

Make backup copies *(yes/no)*

Restore backup copies *(yes/no)*

Destroy / erase devices *(yes/no)*

Reuse devices *(yes/no)*

***Working outside the premises of*** .............. *(yes/no)*

***Physical access to equipment*** *.................. (yes/no)*

*(Add as many entries as needed, one for each file user).*

**Annex............**

|  |  |
| --- | --- |
| Annex INF003 version date | dd/mm/yyyy |
| Version | XXX |

|  |  |
| --- | --- |
| ***INF003*** | *Structure of the files and description of processing systems* |

|  |
| --- |
| **File identification:** .............*(enter the name of the file)*  **Processing system:** ............*(indicate whether automated, not automated or partially   automated)* |

**Data belonging to**............ *(indicate the data subjects, for example, students)*

Name and surname

ID

Nationality

Postal address

Telephone

Email

Etc.

**Data belonging to**.............*(indicate the data subjects, e.g., teachers)*

Name and surname

ID

Nationality

Sex

Private telephone

etc.

**Annex............**

|  |  |
| --- | --- |
| Annex INF004 version date | dd/mm/yyyy |
| Version | XXX |

|  |  |
| --- | --- |
| ***INF004*** | *Users and data access authorisations* |

................ *(indicate data controller)* delegates the functions listed below to the following people:

Person Delegated function

....................................... ................................................

*(indicate the delegations made, such as authorising the removal of portable devices; authorising the destruction of media; checking backups every 6 months, etc.).*

**Annex............**

|  |  |
| --- | --- |
| Annex INF005 version date | dd/mm/yyyy |
| Version | XXX |

|  |  |
| --- | --- |
| ***INF005*** | *Data processors* |

List the natural or legal persons, public or private, or administrative bodies to whom. .................. *(data controller)* has contracted for the provision of services that involve access to personal data in files or systems for which the data controller is responsible.

..................... ***(indicate the name of the data processor*: providing the service of**.................. ***(indicate the service contracted)***

To provide the service of.................... *(indicate the service contracted),* and exclusively for this purpose,..................... *(name the data processor)* is granted access to the personal data in the files........................ *(name the files concerned),* in order to provide the service contracted, in accordance with the provisions of ................... *(indicate the contract or agreement that regulates the conditions of the data processing agreement with the third party. Optionally, a copy of the contract or agreement can be appended to this security document).*

The data in these files must be processed at....................... *(indicate the premises of the data controller or the premises of the processor)*.

*(Optional for cases in which remote access has been authorised)*. The data processor is forbidden to incorporate these data into any systems or media other than those of................... *(indicate the organisation to which the data controller belongs):*

........................... *(indicate the data processor),* when processing these personal data, undertakes to apply a .......................level of security measures *(indicate whether the security level is low, medium or high according to the files concerned)* as stipulated in this security document, in accordance with the provisions of section 3.4.

*(Optional)* The data processor is assigned the task of developing and managing the security document of.................... *(indicate the data controller).* This delegation does not affect the data included in the information systems of.................... *(indicate the data controller).* In this case, the processor must deliver a copy of the security document to................. *(indicate the data controller).*

The data processing service has a validity period of...................... *(indicate the expected period).*

Once the provision of the service has ended, the data processor must.................... *(indicate the action: return to the controller/give to the processor designated by the controller/destroy)* the data and, if applicable, the media in which they are contained.

*(Add to the annex as many sections as needed)*

**Annex............**

|  |  |
| --- | --- |
| Annex INF006 version date | dd/mm/yyyy |
| Version | XXX |

|  |  |
| --- | --- |
| ***INF006*** | *Service providers without access to data* |

List of natural or legal persons, public or private, contracted by................... *(indicate the data controller)* to provide services that do not require access to the personal data in the files or systems for which the data controller is responsible.

|  |  |
| --- | --- |
| **Provider** | **Service** |
|  |  |

*(enter the name of the third party) (name the service contracted)*

**Annex ............**

|  |  |
| --- | --- |
| Annex REG001 version date | dd/mm/yyyy |
| Version | XXX |

|  |  |
| --- | --- |
| ***REG001*** | *Delivery of the security document* |

**User Delivery date Signature of recipient**

(name and surname of user) (dd/mm/yyyy)

................................. ........................ ...................................

*(Add as many rows as needed)*

**Annex............**

|  |  |
| --- | --- |
| Annex REG002 version date | dd/mm/yyyy |
| Version | XXX |

|  |  |
| --- | --- |
| ***REG002*** | *Incident register* |

*(The registered information for each incident is included in a separate record and numbered)*

**Incident code**

**Number**............ *(indicate the number of the incident, for example, 1-2011)*

|  |  |
| --- | --- |
| Incident type or description | *(describe the circumstances in which the incident occurred)* |
| The moment in which it occurred | *(indicate the day, hour and minute, if possible)* |
| Moment in which it was detected | *(indicate the day, hour and minute, if possible)* |
| Person who reported the incident | *(write name and surname)* |
| Person notified of the incident | *(write name and surname)* |
| Consequences of the incident | *(describe how the incident affects the data)* |
| Measures taken | *(describe what corrective measures were taken after the incident)* |
| Recovery of data | *(Yes/no, say whether it was necessary to recover the data)* |
| Other information relating to the incident | *(add any other information relevant to the incident)* |

**Recovery operations**

*(This document must include the record of the recovery of the information of medium or high-level files. With regard to low-level files, only if the data is registered manually)*

User who carried out the recovery Date Type and observations

(name and surname) dd/mm/yyyy (*data restored; if done   
 manually; other   
 observations, such as the   
 reason for manual   
 registering)*

(name and surname) dd/mm/yyyy

.............................. ..........................

*(Add as many rows as needed)*

**Annex............**

|  |  |
| --- | --- |
| Annex REG003 version date | dd/mm/yyyy |
| Version | XXX |

|  |  |
| --- | --- |
| ***REG003*** | *Register of backups* |

User who made the backup File Date Type and observations

(name and surname) dd/mm/yyyy

............................... .......... .................. ................................

*(Add as many rows as needed)*

**Annex............**

|  |  |
| --- | --- |
| Annex REG004 version date | dd/mm/yyyy |
| Version | XXX |

|  |  |
| --- | --- |
| ***REG004*** | *Media inventory* |

Inventory of media, electronic or on paper, containing the personal data of the file.................... *(write the name of the file).*

**A) Electronic media**

|  |  |
| --- | --- |
| Label on the media: .............. | *(write the information to appear on the label)* |
| Location of the media: .............. | *(say where the media is located)* |
| Type and observations: ............. | *(indicate the type of backup and relevant observations, for example, USB flash drive - media for backups)* |
| Persons authorised to access them: ......... | *(write name and surname)* |
| Removal authorisation: ............ | *(G= General / S = Specific)* |
| Security instructions: .......... | *(describe the special instructions for removing the media)* |

**B) Paper-based media**

**Type of document or information:** ....................

|  |  |
| --- | --- |
| Label on the media: .............. | *(write the information to appear on the label)* |
| Location of the media: ............... | *(indicate the place where the media should be stored)* |
| Type and observations: ............... | *(indicate the types of documentation and/or relevant observations)* |
| Persons authorised to access them-......... | *(write name and surname)* |
| Removal authorisation: ............ | (*G= General / S = Specific*) |
| Security instructions: ............ | *(describe the special instructions for storing and removing the media)* |

*(Add as many records as needed, one for each media that needs to be inventoried)*

1. 1This model security document was prepared with the aim of including the minimum requirements established by the RLOPD. It is possible, and recommended, to include any other appropriate measure that would increase the security of the processing carried out in the school, in accordance with its particular circumstances. [↑](#footnote-ref-1)
2. 2 *In the case of public schools, indicate the body designated by the department answerable to the Administration of the Generalitat as being data controller. In the case of state-funded private schools, indicate the body that the school has designated as being data controller.* [↑](#footnote-ref-2)
3. 3 *Depending on the profile of the user, delivery may be limited to some parts of the document and, where appropriate, to the annexes that affect him.* [↑](#footnote-ref-3)