Compliance with the Organic Law for Data Protection in Pandora FMS

BASIC LEVEL

Article 89. Personnel duties and obligations.

1. The duties and obligations of each user or user profile with access to personal data and record-keeping systems will be clearly defined and documented in a security-purposed document. Control duties or delegate authorizations made by the person(s) responsible for the file or its management will also be clearly stated.

2. The person(s) responsible for the file or its management will adopt necessary measures so that the rest of the staff knows comprehensibly about all the security norms that would affect the development of their duties, as well as the consequences that incompliance with those norms would carry.

Pandora: ACL user system. System administration operational procedures (depends on the organization applied, the tool will stand it).

Article 91. Access control.

1. Users will only have access to those resources necessary to accomplish their duties.

2. The person(s) held responsible for these files will establish updated and correct user to user profile relationships, ensuring that proper file authorization is given to each user.

3. The responsible persons will establish the necessary mechanisms to avoid a user accessing files without the proper authorization or user permissions.

4. Only authorized personnel (listed in the security document) will be able to grant, alter or deny access to resources, based on the criteria established by those persons responsible.

5. In case there should exist foreign personnel who has access to available resources, they must also be submitted to the same conditions and security obligations as the rest of regular personnel.

Pandora: ACL user system. System administration operational procedures (depends on the organization applied, the tool will stand it).

Article 92. Document and platform management.

1. Documents and platforms that contain data classified as personal must have the possibility to be identified in relation to its contents, be inventoried, and must only be accessible by authorized personnel (listed in the security document). There will be exceptions to these obligations when the physical characteristics of the platform will not allow their fulfillment, which will be registered in the security document.

2. The release of platforms and documents that contain personal data, including those comprised and/or annexed o an e-mail message, outside the premises controlled by the file or file treatment supervisor must be authorized by the responsible person(s) or properly authorized in the security document.

3. During data migration, measures aimed to avoid the theft, loss or improper access to the data will be taken, as long as the process perdures.

4. When discarding a file or platform that contains personal information, it must be destroyed or completely erased. This must be done applying all possible measures to avoid access to the information contained in that file, or its latter recovery.

5. The proper identification of platforms that contain personal data, and that the organization responsible should deem especially sensitive, can be done through comprehensive tagging systems. They must be easily accessible for authorized personnel, and at the same time difficultly identifiable by parties foreign to that authorization.

Article 93. Authentication and Identification.

1. The person(s) responsible for the file and its treatment must adopt measures to guarantee the correct user ID and authentication.

2. The person(s) responsible for the file and its treatment must establish a mechanism to allow the unequivocal and personalized identification of an user who tries to access the information system, as well as the authentication being used for access, verifying its authorization.

3. When the authentication system relies on a series of passwords, there will be an established protocol to assign, distribute, and store these passwords; that guarantees confidentiality and integrity.

4. The security document will establish the frequency, in no case over a year, with which passwords should be changed. While in use, said passwords must be stored in an unintelligible manner.

Pandora: authentication system. Strong encryption (on v6). Password policy.

Article 94. Backup copies and file recovery.

1. Protocols for actions must be established to guarantee a weekly minimum of backup copies, unless during said time interval there were to be no data updates.

2. In the same way, there will be data recovery procedures established that at all times guarantee their reconstruction in the same state they were in at the time of loss or improper destruction.

Only in the case that the loss or destruction should affect the files or their partially automated treatment, and as long as the existence of documentation allows the objectives mentioned in the above paragraph to be accomplished, there must be a procedure to manually record data, leaving tangible registry of these acts on the security documented.

3. The person(s) responsible for the file will be in charge of verifying the correct definition, functionality and application of data backup and recovery procedures once every six months.

4. Trials previous to the establishment or modification of the information system storing files with personal data will not be done with real data, unless a security level correspondent to the treatment is established, and all activities are registered in the security document.

If trials with real data are planned, previously a security backup copy must be done previously.

PANDORA: Backup, recovery, and HA available.

MEDIUM LEVEL

Article 98. Identification and authentication.

The person(s) responsible for the file or its adequate treatment will establish a mechanism to limit the possibility of reiterated, unauthorized access to the information system.

Pandora: User authentication system. Double authentication (v6).

Article 99. Physical access control.

Only those personnel members authorized by the security document will have access to those places where the physical equipment correspondent to the information system is installed.

PANDORA: this doesn't apply to Pandora FMS (physical security).

HIGH LEVEL

***** Data encryption during platform distribution: encryption in backend SQL, transport encryption (Tentacle SSL/X509), customer encryption (HTTPS).

***** Keep security copies in a different place from your equipment. Depends on external processes, but it's possible.

***** Make encrypted data transfers. Tentacle includes SSL and HTTPS for the customer.

***** Authorized access control to non-automatized files, as well as access ID for documents available to multiple users: Internal Audit Control.