tinexta
infocert

Application Security Guidelines - Design

Emittente: Tinexta InfoCert SpA

tinexta
infocert

Sommario

1 New in this release

1.1 Version

Version n°:	6	**Version date**:	18/03/2026
Description of changes:	Updated new InfoCert logo and updated chap. 3.1		
Reason:	Annual review		
Version n°:	5	**Version date**:	12/12/2024
Description of changes:	updated chap. 3.1, 4.6, 4.9, 4.13, 4.14, 4.15; removed chap. 4.1.2, 4.3.2, 4.4.2, 4.5.2, 4.6.2, 4.8.2, 4.9.2, 4.10.2, 4.13.2, 4.14.2, 4.15.2		
Reason:	Annual review		
Version n°:	4	**Version date**:	30/11/2023
Description of changes:	inserted new Infocert logo; updated chap. 3.1; updated standard reference NIST SP 800-53 rev.5		
Reason:	revisione annuale		
Version n°:	3	**Version date**:	30/11/2022
Description of changes:	removed “A14” from title; updated the references contained in par. 1.2; removed previous par. 2.3; removed chap. 5		
Reason:	Annual review		
Version n°:	2	**Version date**:	08/11/2021
Description of changes:	References correction in par. 1.2; changes in chap 5		
Reason:	Annual review		
Version n°:	1	**Version date**:	30/04/2021
Description of changes:	First release		
Reason:	IMS Adoption		

tinexta
infocert

2 Purpose and Scope of the Document

2.1 Objectives

This policy aims to:

- provide guidance on performing in the design and maintenance of InfoCert products
- ensure compliance with laws and regulations

This document describes the security requirements that need to be considered when designing a brand-new product / service or a revision / extension of an already existing product / service.
These guidelines are obviously not meant to, and cannot, replace specialised documents and websites. Please refer to the latter for details on technical issues, theoretical insights and, above all, constant updates on the state of the art of vulnerabilities and development techniques.
The contents of this document also apply to applications or parts of them whose development has been outsourced to third parties. Where possible, they also apply to purchased packages.

2.2 Recipients

The policy applies to all staff and / or third parties engaged with designing and providing products and services on behalf of InfoCert and third parties.

All business units are involved.

2.3 Policy Update and Violations

Document updates will be reviewed at least annually. Violations of corporate security policies shall be managed in accordance with existing employment contract regulations.

3 Reference Standards and Legislation

3.1 Reference Standards and Legislation

Below is a non-exhaustive list of applicable legislation and regulatory and contractual obligations that inform this policy:

- Framework Nazionale per la Cybersecurity e la Data Protection
- ISO 27001
- NIST SP 800-53 rev.5
- GDPR (UE 2016/679), Regolamento Generale sulla Protezione dei Dati)
- NIS2 (UE 2022/2555), Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione)
- DORA (UE 2022/2554), Digital Operational Resilience for the financial sector)

tinexta
infocert

4 Policy

All products / services should comply with the requirements laid down in the following paragraphs. Any departure from such requirements shall be explicitly justified.

Requirements specific to product / service maintenance may only be ignored when designing a brand-new product / service.

Certain specific requirements may not be applicable depending on the type of product / service.

In such cases, the reason for excluding an audit shall be reported in the design documentation.

4.1 Regulations and Requirements

When developing a product / service, account shall be taken of any legislation (e.g., laws, regulations, standards) that regulates the area of that product / service.
Any additional requirements resulting from industry regulations shall be explicitly taken into account at the design stage.
Such regulations may provide for additional requirements other than those listed here (e.g., safety certifications of products or devices on which the product / service is based).
Each product / service shall be accompanied by a Data Protection Impact Analysis that identifies any risks (threats, probability and impact) for the rights of the parties whose data is to be processed.
It is important that the Recommendations for Privacy by Design and Default and the templates prepared by the Parent Company are adhered to and that the Privacy Officer is involved.
Data must be classified in advance and assessed for confidentiality.
When designing a product / service, steps must be taken to define its scope of use. These include identifying the type of data to be processed (according to privacy legislation or to the specific requests of a customer, in the case of supply of services and / or customised products) and determining which of the audits described in this document apply to such data.
If the scope cannot be predicted, the product / service shall be designed assuming a "worst-case" usage scenario.

4.1.1 Responsibilities

Ensuring that the rules and recommendations mentioned in this document are complied with and that the privacy risk analysis is carried out is the responsibility of the Developer Manager of the application team in charge of developing and / or maintaining the product / service. The Developer Manager may be assisted by the product / service Owner, particularly in the case of regulated services.

4.2 Risk Assessment

An assessment of risks (threats, probability and impact) for the company, customers and users shall be conducted in order to identify appropriate audits.
Potential risks for the company in terms of its reputation, financial loss, compliance, sanctions etc. shall be determined through a combined analysis taking into account the classification of processed data, data protection impacts and the product / service scope of use.

4.2.1 Responsibilities

Risk analysis is the responsibility of the Developer Manager of the application team in charge of developing and / or maintaining the product / service. The Developer Manager may be assisted by the product / service Owner, particularly in the case of regulated services.

4.3 Data Integrity

Data integrity shall be ensured for at-rest, in-transit and end-to-end data. Specifically:

- HTTPS or signature technologies shall be used to ensure that data being transmitted is not altered as it goes across the network. To this end, the TLS 1.2 or higher protocol shall be used.
- Only authorised entities shall be allowed to update stored data and the possibility for unwanted changes, whether accidental or intentional, shall be prevented.
- The integrity of data stored on any physical device shall be ensured through access-control and other techniques that detect unwanted changes (and which may be embedded in the basic products adopted). These include, where applicable, successful task verification techniques. Data backup and retention policies shall also be defined.
- When using packages developed by third parties, automatic processes must be in place to check the integrity and authenticity of the products installed.

4.3.1 Responsibilities

Ensuring that all data integrity recommendations are complied with is the responsibility of the Developer Manager of the application team in charge of developing and / or maintaining the product / service. The Developer Manager may be assisted by the product / service Owner, particularly in the case of regulated services.

4.4 Data Confidentiality

Data confidentiality shall be ensured for “at-rest”, “in-transit” and “end-to-end” data. Specifically:

- It shall be ensured that personal data passing through the network is not readable by unauthorised parties. This can be achieved by encrypting the data through a HTTPS protocol or via VPN, as long as both ends of the secure connection are under the control of authorised parties.
- For other types of data that are not subject to the GDPR, the decision on whether or not traffic protection functionalities should be applied depends on the outcome of the analysis of the requirements under the previous paragraph. However, it is strongly recommended using an HTTPS protocol.
- Stored data shall only be readable by authorised persons. To this end, users (system administrator, DBA, end users or others) shall be profiled by establishing which data each profile is allowed to access, and for what tasks. Data segregation - i.e., preventing User X from accessing the data of User Y, if X≠Y - should also be ensured. Data stored on backup devices shall also be segregated, so that it can be selectively processed in the event of cancellation and restoration

- Sensitive data, such as data that would reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data or intended to uniquely identify a natural person, data concerning health or sex life or orientation of the person concerned, judicial data and data relating to means of payment shall be encrypted even when at rest. Encryption of other types of data shall be assessed according to their nature and any threats associated with them.
- Compliance with all the requirements described in this paragraph shall also be guaranteed for backup media and any other media through which data is transmitted or in which it resides, including (complete or partial) copies prepared for development and testing purposes.

4.4.1 Responsibilities

Ensuring that all data integrity recommendations are complied with is the responsibility of the Developer Manager of the application team in charge of developing and / or maintaining the product / service. The Developer Manager may be assisted by the product / service Owner, particularly in the case of regulated services.

4.5 Service and Data Availability

Product / service-specific availability requirements need to be in place and established with regard to:

- High reliability
- Maximum acceptable time of unavailability
- Disaster recovery
- Business continuity

4.5.1 Responsibilities

Availability requirements for the product / service concerned shall be established by the Developer Manager of the application team in charge of developing and / or maintaining the product / service, in consultation with the infrastructure management team. The Developer Manager may be assisted by the product / service Owner, particularly in the case of regulated services.

4.6 Deletion of Data

Physical and / or logical deletion of data must be provided. For data that may no longer be lawfully retained, their deletion must be provided for across all devices, including backup systems. Such deletion must be carried out in a secure manner.

4.6.1 .Responsibilities

Ensuring availability of data deletion functionalities is the responsibility of the Developer Manager of the application team in charge of developing and / or maintaining the product / service. The Developer Manager may be assisted by the product / service Owner, particularly in the case of regulated services.

4.7 Authentication and Timeout

Except for information purposes, all interaction with users must include user authentication.
For sensitive data, strong (multi-factor) authentication shall be used.
Authentication methods (i.e., simple vs. strong authentication) shall be proportionate to the type of data being processed.
Any product / service that does not rely on a centralised authentication system shall:

- use credentials that comply with the company's password policy and applicable regulations
- not store any passwords
- allow password change
- have a password expiration policy
- limit the number of login attempts with incorrect credentials (accounts must be disabled after a certain number of attempts, not exceeding 10)
- provide for a time lag between one authentication attempt and the next (a delay of 5s between one authentication attempt and the other significantly reduces the effectiveness of "brute force" and "Dictionary" attacks)
- implement a timeout to abort a session in the event of prolonged idle time from the user (human or system). The timeout interval should be configurable; however, it should not exceed 15 minutes.

4.7.1 Responsibilities

Ensuring compliance with the above-mentioned authentication and time-out recommendations and with the guidelines laid out in the company's password policy for the product / service being developed / maintained shall be the responsibility of the Developer Manager of the application team in charge of developing and / or maintaining the product / service. The Developer Manager may be assisted by the product / service Owner, particularly in the case of regulated services.

4.8 Logging

Activities shall be logged for debugging and tracing purposes. Multilevel configurable logging should be provided.
At its most basic level, logging should allow to establish:

- the user who performed the task
- when the task was performed
- the items on which the task was performed.

The need to include a timestamp in each log should be assessed on the basis of any legal obligations and on whether it would be expedient in the event of a dispute.
Log retention requirements must be defined based on applicable regulatory obligations. In particular, with regard to privacy, Digital Certification, and Certified Electronic Mail (PEC), the project must establish the retention periods and procedures for log preservation.

4.8.1 Responsibilities

The level of logging and log retention shall be determined by the Developer Manager of the application team in charge of developing and / or maintaining the product / service. The Developer Manager may be assisted by the product / service Owner, particularly in the case of regulated services.

4.9 Separation of Environments

Development, testing, and production environments must be segregated to reduce the risk of unauthorized access or changes.

The segregation of environments must be ensured by keeping users, data, and systems dedicated to development, testing, and production separate.

The use of production data outside the production environment is prohibited. Where its use is strictly necessary, for example during debugging activities in non-production environments, the data must be appropriately sanitized. Only anonymized, pseudonymized, or randomized production data may be stored in non-production environments.

The implementation methods for this requirement are described in the detailed operational documents and any related supporting documentation.

4.9.1 Responsibilities

Physical separation of environments shall be implemented at the network level by the team in charge of the infrastructure. Logical separation is implemented according to the access control process implemented by InfoCert.

4.10 Data and Software Life Cycle

Shall be defined a software and data life-cycle management process.
Methods for tracking the life cycle of personal data (from collection to storage and dissemination) shall be defined and documented.
Any changes to the type of data processed by the product / service shall be checked for compliance with the requirements specified in this document. For example, a product / service originally designed to process only public data may be extended to process also personal or health data. Such an extension involves a review of the project to ensure that it will be valid in the new application environment.
Changes to systems within a life cycle are to be monitored by means of formal change management procedures.
Only formally approved changes may be implemented. All changes shall be documented, assessing their potential impacts on safety.
When changes occur in operating platforms, business-critical applications shall be reviewed and tested to ensure that there are no negative impacts on the organisation's operations or safety.

4.10.1 Responsibilities

The Developer Manager of the application team in charge of developing and / or maintaining the product / service shall be responsible for defining the product / service life cycle management process as well

as for monitoring its change management process. The Developer Manager may be assisted by the product / service Owner, particularly in the case of regulated services.

4.11 Non-repudiation

The need to include non-repudiation functionalities shall be assessed. For example, agreements are to be concluded which include unfair terms.

4.11.1 Responsibilities

Assessing the need for non-repudiation functionalities is the responsibility of the Developer Manager of the application team in charge of developing and / or maintaining the product / service. The Developer Manager may be assisted by the product / service Owner, particularly in the case of regulated services.

4.12 Licences

The product / service shall comply with the licensing terms of third-party software used in its development.
In particular, for open licenses, please see the relevant dictionary.

4.12.1 Responsibilities

The Developer Manager of the application team in charge of developing and / or maintaining the product / service shall ensure that the licensing terms of third-party software used in the development of the product / service are complied with. The Developer Manager may be assisted by the product / service Owner, particularly in the case of regulated services.

4.13 Vulnerabilities

The product/service must not contain any known vulnerabilities.
Infocert shall conduct periodic assessments to identify potential vulnerabilities within the product/service and shall subsequently prepare an appropriate remediation plan.
Wherever feasible, the project shall provide for the use of dedicated tools during the design and development phases to identify and remediate vulnerabilities as early as possible in the software development lifecycle.
It is recommended that source code reviews and testing activities be performed, covering both static and dynamic analysis.
Proprietary software and, where possible, source code provided by third-party IT service providers or originating from open-source projects, must be analyzed and tested before being deployed to the production environment.

The provisions set out in this section also apply to IT systems developed or managed by external parties, following a risk-based approach.

4.13.1 Responsibilities

Periodic assessments of existing products / services shall be carried out and / or outsourced by the Cybersecurity Team, as illustrated in the Vulnerability Management process.
The use of tools that identify potential code vulnerabilities ever since the development phase shall be determined by the application team in charge of developing and / or maintaining the product / service.
The implementation methods for this requirement are described in the detailed operational document and in any related supporting documentation.

4.14 Outsourced Development

InfoCert shall supervise and monitor the development of any outsourced products / services.
Before entering into an agreement with a vendor, InfoCert shall check the latter's reliability and the processes it implements to design, develop, test its products / services.
All recommendations contained in this policy must also be applied when parts of the system are outsourced to third parties.

4.14.1 Responsibilities

Any codes developed through external vendors must comply with the policies defined by InfoCert. The Developer Manager shall ensure compliance with said policies. When developing ad hoc projects for individual clients, compliance shall be ensured by the Project Manager.

4.15 Testing

During development, testing activities related to the security functionalities of the product/service must be performed.

Test and acceptance plans, together with the related criteria, must be established for new products/services, updates, and new releases.

Application testing must include security functionality testing, and test data must be carefully selected, balancing the need for meaningful results with the risk of exposing sensitive or relevant data.

Data used for testing purposes must be carefully selected, protected, and properly controlled.

Any cases in which testing must be performed in a production environment shall be clearly identified and justified, limited in duration, and subject to approval by the competent function.

The availability, confidentiality, integrity, and authenticity of IT systems and production data must always be ensured during development and testing activities.

Where necessary, production data may be stored only for specific testing activities, for limited periods of time, subject to prior approval by the competent function and notification of such activities to the Cybersecurity Team.

The implementation methods for this requirement are described in the detailed operational document and in any related supporting documentation.

4.15.1 Responsibilities

During the planning phase, the Developer Manager shall set out a test plan covering all the (functional, non-functional, security, SLA) requirements listed in the design specifications and / or technical annexes agreed with the client. The Developer Manager may be assisted by the product / service owner, particularly in the case of regulated services.
The mapping of requirements as declared and of related test results will provide a baseline for managing testing activities for both the project being developed and for its subsequent modifications, if any.

tinexta
infocert

think next,
trust now