

Information Security Policy



Contents

1. Purpose	4
2. Scope	4
3. Definitions	4
4. Information Security Policy	5
4.1 Werfen Commitment.....	5
4.2 Responsibility	5
4.3 Security policy guidelines	5
5. Communication mechanism for this policy	6
6. Policy review and modifications mechanism	6

Version Control

Version	Date	Modifications
001	November 2018	Creation
002	June 2021	Definitions in section have been removed. New security guidelines have been added.

1. Purpose

The purpose of this policy is to establish the commitment of Werfen board members to information security, and to provide guidelines for all employees regarding the protection of information assets.

2. Scope

This policy applies to all Werfen employees (internal and external), and to any third parties who use the relevant information and communication technology resources.

3. Definitions

The terminology used in this procedure needs to be understood in the most common sense of the words used. For concepts that need extra clarification, see ISO/IEC 27000, Information technology — Security techniques — Information security management.

4. Information Security Policy

The Werfen Information Security Policy is based on the three basic concepts of information security: Confidentiality, Integrity, and Availability. Based on these concepts, this policy provides guidelines for protecting information and physical assets by providing the level of protection required by business objectives, and at accepted risk levels.

4.1 Werfen Commitment

The commitment of board members is essential to ensuring the success of the Information Security Policy. This commitment acknowledges that this Policy is appropriate for the needs of the organization. Management supports this policy and will grant the resources required to make this policy effective.

4.2 Responsibility

All Werfen employees (internal and external), and any third parties who use the relevant information and communication technology resources, should read and comply with the Werfen Information Security Policy and the related procedures. It is then the responsibility of all internal and external employees to protect the information assets.

4.3 Security policy guidelines

Werfen management believes that the attainment of Werfen objectives must be in compliance with the various requirements designed to ensure Information Security within the organization. Information Security is therefore considered to be a priority for the organization. As such, the present policy establishes the following guidelines:

- The information to which Werfen is the owner and / or depositary, must only be accessible by authorized persons, who may or may not be employees of Werfen companies.
- This Security Policy must be accessible to all Werfen employees and to non-Werfen employees who are related to Werfen through any of its processes.
- The Organization must comply with all applicable legal, regulatory, and statutory requirements, and any contractual requirements.
- The confidentiality of information must be guaranteed at all times.
- All the processes involved in managing, processing, and storing such information must guarantee the integrity of the information.
- The availability of information must be guaranteed through adequate measures of support and business continuity.
- Any incident or weakness that may compromise, or has compromised, the confidentiality, integrity, and/or availability of the information must be recorded and analysed in order to implement the corresponding corrective and/or preventive measures.
- All Werfen employees must have adequate training and awareness of Information Security.
- The organization must establish a continuous improvement approach to Information Security.

5. Communication mechanism for this policy

In order to ensure that the content of this policy is known to, and applied by, Werfen professionals, it will be available to all employees through the SAP, which has been activated to this effect. The responsibility of communicating this policy lies with Werfen headquarters (IT department).

6. Policy review and modifications mechanism

This policy has been validated by the Executive Committee.

No fixed term has been set for the review of this policy. It will be reviewed in the event of any relevant operational, legal, regulatory, or contractual changes in the business.

In all the aforementioned cases, Werfen headquarters (IT department) will lead a review process for this policy, during which the content of the policy will be examined to determine its current validity. The result of the review, and the suggested modifications (if any), will be presented to the Executive Committee for validation.

All reviews and any modifications will be documented in the version tracker on the first page of this policy.