



**International  
Standard**

**ISO 24596**

**Drinking water, wastewater and  
stormwater systems and services —  
Guidelines for the planning and  
implementation of infrastructure  
hardening for water and  
wastewater systems**

*Systèmes et services relatifs à l'eau potable, à l'assainissement  
et à la gestion des eaux pluviales — Lignes directrices pour  
la planification et la mise en œuvre du renforcement des  
infrastructures des services de l'eau et de l'assainissement*

**First edition  
2024-02**

STANDARDSISO.COM : Click to view the full PDF of ISO 24596:2024



**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

	Page
<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Protection principles</b> .....	<b>2</b>
4.1 General.....	2
4.2 General objective for water infrastructure hardening.....	2
4.3 Main water and wastewater systems components.....	3
<b>5 Risk assessment</b> .....	<b>3</b>
5.1 General.....	3
5.2 Vulnerability investigation.....	4
5.2.1 General.....	4
5.2.2 Site security plan.....	4
5.2.3 All hazards risk assessment.....	5
5.3 Asset risk categorization.....	6
<b>6 Protective measures for infrastructure</b> .....	<b>7</b>
6.1 General protective measures.....	7
6.2 Security protection methods.....	7
6.2.1 General.....	7
6.2.2 Property protection by physical means.....	8
6.2.3 Monitoring and detection of intrusion.....	8
6.2.4 Property protection by human means.....	8
6.2.5 Security zones.....	9
6.2.6 Property protection by organizational means.....	9
6.3 Protection measure validation.....	9
6.4 Protection assessment.....	9
6.4.1 General.....	9
6.4.2 Ongoing review.....	9
6.4.3 Corrective measures.....	9
<b>7 Documentation</b> .....	<b>9</b>
<b>8 Infrastructure hardening examples and configurations</b> .....	<b>10</b>
8.1 General.....	10
8.2 Recommended configurations for the hardening of the different elements of a water system.....	10
<b>Annex A (informative) Example of recommended security measure configurations for water and wastewater infrastructure as practised in Israel</b> .....	<b>11</b>
<b>Annex B (informative) Example of the indicative asset security categorization and security treatment schedules as practised in Australia</b> .....	<b>14</b>
<b>Annex C (informative) Example of recommended security measure configurations for water and wastewater infrastructure as practised in Germany</b> .....	<b>24</b>
<b>Annex D (informative) Example of general protection elements for water and wastewater infrastructure</b> .....	<b>26</b>
<b>Bibliography</b> .....	<b>31</b>

## Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see [www.iso.org/directives](http://www.iso.org/directives)).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at [www.iso.org/patents](http://www.iso.org/patents). ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html).

This document was prepared by Technical Committee ISO/TC 224, *Drinking water, wastewater and stormwater systems and services*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at [www.iso.org/members.html](http://www.iso.org/members.html).

## Introduction

Hardening of water and wastewater infrastructure is one of the most crucial issues to address when formulating and implementing a plan for assuring the security of water and wastewater systems. The delivery of strong safety and security outcomes is essential to protect employees, the public and the assets of the water utility. Securing the assets and operations, where these facilities constitute an essential element of water service continuity or contain hazards or risks to the public, should be central to each water utility's safety and security programme and demonstrated through applied risk management principles, business activities and associated corporate documentation. These assets are crucial to ensure service continuity and minimize risks to the community.

Over the past few years there has been an increase in water and wastewater supply crisis events associated with:

- climate change;
- cyberattacks on water infrastructure;
- civil disruption;
- terrorist-related physical attacks on civil targets.

There has also been an increase in public awareness of water and wastewater incidents.

Under these circumstances, the protection of water and wastewater infrastructure is of critical importance.

Hardening of water and wastewater infrastructures has the aim of enhancing the protection of these infrastructures. Hardening consists of construction and creation of barriers, that can include physical and electronic elements, personnel and organizational measures, with the purpose of making it difficult to intentionally or unintentionally disrupt service continuity, supply and quality.

Examples of such barriers include fences, buildings, electronic alarms and cameras connected to control rooms, remote valves, both manual and remote controlled, backflow preventers, analysis software, such as event detection systems (EDS, as described in ISO/TS 24522)<sup>[1]</sup> and software designed to prevent cyberattacks.

Another type of protective system is the installation of monitoring equipment for water quality and operational parameters. This document only briefly refers to this type of protection. For more information, see ISO/TS 24541<sup>[2]</sup>.

[STANDARDSISO.COM](https://standardsiso.com) : Click to view the full PDF of ISO 24596:2024

# Drinking water, wastewater and stormwater systems and services — Guidelines for the planning and implementation of infrastructure hardening for water and wastewater systems

## 1 Scope

This document provides guidelines for the planning and implementation of hardening of different water and wastewater infrastructures aiming to improve the resilience of water and wastewater services provided by water utilities through security measures.

It applies to the determination of measures for the protection of water supply systems and sewer collection systems from unwanted or unplanned access, as part of risk management. This document is applicable to all water and/or wastewater utilities.

This document does not include guidelines for the protection of large water sources such as lakes or rivers.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 24513, *Service activities relating to drinking water supply, wastewater and stormwater systems — Vocabulary*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 24513 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

### 3.1

#### **access point**

opening or accessible opening in the perimeter of a site, building, structure or cabinet

### 3.2

#### **alarm**

audible and visual signal alerting a condition requiring immediate attention or user action

[SOURCE: ISO 8468:2007, 3.1.3<sup>[3]</sup>]

### 3.3

#### **alarm response**

type and timeframe of physical response to a designated site to enable an informed management decision in response to an *alarm* (3.2) or other alert

### 3.4

#### **detector**

item of electronic hardware which transmits designated signals (e.g. fire or movement) under specified environmental conditions to a control panel

### 3.5

#### **integrate**

conceptual and physical linkage between the planning aspects of protective monitoring systems

EXAMPLE Fire systems linked to intruder alarm systems and access control systems, with common interphase and signalling under prescribed conditions.

### 3.6

#### **security**

resistance to intentional acts designed to cause harm or damage

[SOURCE: ISO 28001:2007, 3.20, modified — the phrase “to or by the supply chain” was removed<sup>[4]</sup>.]

## 4 Protection principles

### 4.1 General

Hardening of assets should be based on the following principles:

- risk-based approach;
- continuity and integration of water services;
- security and safety of the community and employees;
- assurance that appropriate standards and controls have mitigated risks inherent to water and wastewater infrastructure.

Hardening of water and wastewater infrastructure is divided into electronic and non-electronic, personnel and organizational measures, with the purpose of making it difficult to intentionally or unintentionally disrupt the service supply and cause the quality to deteriorate.

For initial security measures, a combination of physical measures (i.e. non-electronic measures) are often used – e.g. fencing or other entry barriers. Where the physical protection measures do not meet the required level of protection, electronic security measures should be used. In particular, physical property protective measures primarily refer to buildings and above-ground facilities or to buildings with above-ground access. As a rule, personnel and organizational measures are required for the property protection of underground assets.

The property protective measures should be based on a risk assessment approach and may also be staged based on the level of hardening required. Basic protective measures in the event of increasing danger should be supplemented by additional prevention measures, depending on the situation. These preventive measures may consist of personnel or organizational measures. Personnel measures are related to access control, patrolling and guarding. Organizational controls relate to, for example, employment and periodic safety visits and the conduct of exercises and post-security incident analysis.

### 4.2 General objective for water infrastructure hardening

Measures used to harden a water or wastewater facility should be conceived and revised in line with evolving national security risk advice, national security guidelines, legal risk determinations and local and regional risk conditions, as well as organizational and operational risk assessments.

The general objectives for the hardening of water infrastructure should be:

- preventing or delaying unauthorized access to water and wastewater assets, to avoid destruction or interference, creating the conditions for conveying to the relevant bodies immediate knowledge that someone may have accessed a water infrastructure without authorization;
- allowing the detention or identification of intruders and the initiation, if necessary, of subsequent prosecution by law enforcement.

### 4.3 Main water and wastewater systems components

The main water and wastewater systems components which should be considered for hardening purposes are:

- treatment plants and their components;
- water and wastewater reservoirs and tanks (open and closed);
- water abstraction and bulk water storage facilities, such as dams and groundwater wells;
- water supply off-takes and diversions;
- water and wastewater supply network infrastructure.

The application of risk-based benchmarked security and public safety principles and standards to the water and wastewater assets should be applied to achieve a cohesive protective security effect. The following key principles should be considered:

- a) The levels of risk control should be determined using evidenced-based risk assessments.
- b) Risk assessments should be benchmarked against infrastructure, community security and public safety risk experience.

Water utility managers should:

- identify the risk to public safety and security;
- monitor conformity with safety and security standards;
- operate and maintain assets in accordance with corporate requirements;
- ensure the applied public safety and security treatments are appropriate to the risk environment.

## 5 Risk assessment

### 5.1 General

To formulate a plan for the hardening of water system infrastructure, risk assessment of the system should be performed to decide which elements of the water system will be hardened and to what extent, and to establish a priority order of implementation.

The risk management plan should be developed in a manner consistent with ISO 31000.<sup>[5]</sup> In the development of a risk management plan, all stakeholders, including external regulators and institutions, should be identified. Accountability for the risk management plan development, delivery and review should be clearly designated.

To assist in developing the risk management plan, a system vulnerability investigation should be performed on all the elements of the system mentioned in [5.2](#).

## 5.2 Vulnerability investigation

### 5.2.1 General

A vulnerability investigation requires the development of a site security plan and undertaking of an “all hazards” review (see [5.2.2](#) and [5.2.3](#)).

### 5.2.2 Site security plan

The site security plan should document the current conditions of the installation in relation to security.

The site security plan should:

- a) document the layout (see ISO 24518<sup>[6]</sup> and ISO/TS 24520<sup>[7]</sup>) and site security aspects of the system or facility being secured, including items such as:
  - water wells;
  - tanks or reservoirs and other storage facilities;
  - hydrants, accessories, pipelines and connections;
  - open channels;
  - water treatment plant components;
  - wastewater treatment plant components;
- b) note the requirements of relevant, occupational health and safety, environmental and security legislation;
- c) identify specific requirements of the water utility, including provision for future expansion of the system and/or required augmentation to the existing system;
- d) include critical details related to the “all hazards” risk management plan, including:
  - impacts on the community (see ISO 24518<sup>[6]</sup> and ISO/TS 24520<sup>[7]</sup>);
  - alternative drinking water, wastewater, stormwater and non-drinking water services;
  - product quality performance requirements;
  - quantity and reliability requirements;
  - outcomes from the asset risk classification;
- e) document the security profile of the system, including an assessment of the local environment and general area of influence, including:
  - geography;
  - meteorology;
  - demography;
  - emergency, police, security and medical response services;
  - asset categorization of the site and its individual components;
  - operations of the site;
  - other equipment and assets;

- visible deterrence level required, versus the detection and response capacity available for the subject site;
  - total loss effect, redundancy capacity, depth of contingency planning and repair capacity;
- f) document engagement with key stakeholders, including government officials and the police, as deemed necessary by the water utility.

### 5.2.3 All hazards risk assessment

During the planning, concept and design phases of new, extended, upgraded and renewed water systems, a practical and appropriately documented “all hazards” risk assessment should be undertaken in accordance with ISO 31000.<sup>[5]</sup> To ensure effective property protection, a precise analysis and evaluation of hazards of both the individual infrastructure and the entirety of the water supply systems in accordance with risk management practices should be carried out on the basis of the protection objectives described in 4.2. This should include recurring and event-related hazards and consider the nature and extent of the hazard and its potential impact on the infrastructure (see [Annex C](#)).

Risk should be defined by the components of likelihood (plausibility) and consequence. In determining the consequence, the vulnerability of the infrastructure, including functional susceptibility and replaceability, should be taken into account.

The functional susceptibility includes aspects such as the dependence or effect on other internal and external infrastructure and the intrinsic robustness of the water infrastructure against external influences. Replaceability includes aspects such as redundancy and the expected effort to restore services. In addition to the direct effects on the infrastructure, the effects on the whole or parts of the water supply system should be determined and taken into account in the risk classification.

The “all hazards” risk assessment should qualitatively and quantitatively identify and assess the following risk areas, as a minimum:

- a) environmental hazards;
- b) external and internal human environment:
  - 1) natural hazards, e.g. fires or floods;
  - 2) human induced, e.g. vandalism, sabotage, terrorism (noting that this can require engagement with authorities such as the police to determine effectively);
  - 3) geographic environmental risks:
    - proximity to population centres' direct and indirect risks to the population;
    - number of people served by the relevant system element;
    - supply to special type of users (e.g. hospitals, schools, key factories);
  - 4) collateral systems and operational effects:
    - physical conditions of the system, e.g. accessibility, level of protection;
    - hydraulic nature of the system, e.g. gravity, pressure, open channel;
    - digital connectivity, e.g. manual operation, on-site automation, networked automation, centralized or distributed data collection;
    - operational, essential and emergency services and security response capabilities;
    - contingency bypass, replacement or recovery capability.

Following risk assessment, an appropriate and cost-effective level of hardening and asset protection should be determined for each asset category within the system using the asset risk categorization (see [5.3](#)). These

appropriate protection components or required design features should in turn be incorporated into the final design of the infrastructure and reflected in the site security plan.

**NOTE** This approach assumes that consequence is the dominant variable in determining whether to harden a facility. The likelihood of an event can be of lesser significance than the consequence and is used to determine the aspects of the facility that require hardening. The reasoning is that if the potential consequence component of the risk is deemed high or medium, then even though the likelihood of an event is low, consideration must be given to hardening the installation. This is because the current environment of rapidly evolving threats, particularly terrorism and cyberattacks, coupled with customer expectations and reputational damage from successful attacks on this infrastructure area, means that compromise of the system is an unacceptable outcome.

### 5.3 Asset risk categorization

Asset risk categorization relates to the consequences of asset function loss. It provides a basis for selection of appropriate infrastructure protection treatments relevant to the impact on downstream water services during a period of disruption, taking account of the intrinsic ability to bypass the asset functionality and continue to deliver water services to achieve the required goals.

The water utility should define the asset categorization and the operational environment based on the risk assessment (implementing criticality analysis methods).<sup>[8]</sup>

A complex site (multiple functions and assets) may have an overall high rating with specific components receiving differing ratings, dependent on their criticality. In such cases, security of specific assets within a site perimeter should be considered as more practicable than treating the entire site.

[Table 1](#) provides guidance on assigning the level of hardening relative to the impacts of loss of asset functionality.

**Table 1 — Generic infrastructure protection guidance**

Asset risk level	Description	Loss effect (impact)	Suggested hardening level
A	Critical operational site or component. Identified by external and internal stakeholders as critical for operation, loss effect, community perception and national defence or strategic requirements. Critical to the control and operational integrity of the integrated services or supply.	Community, commercial and industrial loss. Major contingency effort to continue operations. Major media and government attention, regulator investigation and potential action.	High
B	Key operational site. Key link in the integrated supply system. Significant or single source. May be remote with extended travel times or no local community. Located close to high-density population area. Essential supply link to important national defence or strategic asset.	Potential commercial and industrial loss for the community. Significant contingency effort to continue operations. Media and ministerial attention. Regulator investigation and potential action.	Medium
C	Operational site. Short effect. Or non-essential site. Minimal or no loss effect.	Minimal or zero commercial loss in the community. Limited or zero media attention. Regulator routine investigation.	Low

Once the desired level of security is determined, the outcomes from the risk assessment should be used to determine the necessity and priority for implementation of individual protective measures (see [Annex A](#), [Annex B](#) and [Annex C](#) for examples).

## 6 Protective measures for infrastructure

### 6.1 General protective measures

The following provide general guidance for design treatments in relation to site hardening.

- a) For properties adjacent to high-volume roads and sites subject to sustained construction, robust security detection equipment should be adequate; in some instances, seismic detection equipment or smoke detection apparatus can be considered.
- b) For agricultural, semi-rural and high crime areas, ballistically tolerant lighting fixtures, closed-circuit television (CCTV) enclosures and detection apparatus should be adequate.
- c) For assets located near schools and places of mass gathering, greater levels of security treatment should be adequate.
- d) For urban high-density population areas with evidence of repeated site intrusion, vandal-resistant external lighting, CCTV and detection apparatus fixtures should be adequate.
- e) All external and internal infrastructure should take into account the extremes of weather over a longer time period appropriate to each country, e.g. 50 or 100 years. Considerations could include:
  - water and flood levels, frequency and severity;
  - temperature extremes and ranges;
  - UV (ultraviolet) levels;
  - wind (prevailing, seasonal and maximal);
  - dust levels;
  - salinity levels;
  - condensation, cyclic, mist and ambient moisture levels;
  - fire hazards;
  - seismic movement, volcanic activity or tsunamis.

The installations should also consider adjacent foliage and fauna, including:

- trees;
- insects;
- birds and bats;
- large and small burrowing animals;
- animals with the potential to scale, burrow under or cross fences.

### 6.2 Security protection methods

#### 6.2.1 General

Security protection requires physical, personnel or organizational measures aimed at reducing risks to acceptable levels. Specific risk-control measures should be prioritized, with a preference for those measures that demonstrate high reliability and operational stability (e.g. low false reporting rate).

An integrated combination of physical, personnel and organizational measures offers the most effective property protection.

When defining the measures to be implemented, responsibilities and deadlines for their implementation should be clarified.

It is advisable to employ suitably certified security officers in order to support the selection and implementation of appropriate protective measures.

For examples of general protective elements for water and wastewater infrastructure, see [Annex D](#).

### 6.2.2 Property protection by physical means

Property protection by physical means should include structural (e.g. building materials), mechanical (door chains, box locks) and electronic security measures that increase the time to penetrate the infrastructure by intrusion attempts. These measures are required to provide early and timely warning to the water utility and may include the following:

- maximizing the structural integrity of external building surfaces (hardening the outer skin) to minimize injury to personnel and equipment within the structure;
- delaying intrusion by making access difficult or preventing unauthorised access to the site, buildings and facilities.

For further information on physical property protection measures and a comparison of mechanical burglary protection security levels, see [Annex A](#), [Annex B](#) and [Annex C](#).

Where mechanical protection is not sufficient or cannot be achieved, additional electronic safety systems should be used.

Particular attention should be paid to intercoupling the mechanical and electronic safety systems such that all mechanical and electronic protective elements are coordinated with each other and work effectively together, considering that the weakest link determines the security level for the overall system.

### 6.2.3 Monitoring and detection of intrusion

Detection of intrusion or compromise of the facility and its associated water supply can occur in the following ways:

- a) Direct detection of the intruder or trespasser, which can be of a physical or virtual nature. The intruder or trespasser is observed and then the appropriate countermeasures engaged, to delay, detain or remove them.
- b) Indirect detection, where a disruption to the normal performance of the system is detected through the use of sentinel monitoring systems, such as the following:
  - Part of the electronic cyber security system, whereby digital detection systems track, delay, decoy, detail, identify and remove the intrusion or report it to a relevant authority for manual intervention. ISO/IEC 27000<sup>[9]</sup> and the IEC 62443 series<sup>[10]</sup> provide guidance on the relevant approaches.
  - Part of the water quality monitoring network, whereby online sensors or intermittent sampling detects a system change requiring further investigation. ISO/TS 24541<sup>[2]</sup> provides guidance on the use of these measures.

### 6.2.4 Property protection by human means

Property protection using personnel essentially includes the patrolling of the area, buildings and facilities by the water utility's own personnel, a commissioned security service or the police.

It may also include the preparation and implementation of standard operational procedures (SOPs) in password management and two-factor authentication (2FA), i.e. use of a password and code sent to a mobile phone to allow access.

### 6.2.5 Security zones

Plant-related security zones and the appropriate protection levels should be considered by the water utility during planning for water and wastewater infrastructure using the appropriate risk management criteria.

[Annex A](#), [Annex B](#) and [Annex C](#) provide some examples of detailed description of and proposals for the elements that provide physical protection for the different infrastructure of water and wastewater systems.

### 6.2.6 Property protection by organizational means

Organizational infrastructure protection includes:

- access authorizations;
- action plans for alarm response;
- agreements with the local police authorities and/or the fire brigade on joint procedures when alarms are raised.

### 6.3 Protection measure validation

All measures installed for protection purposes should be validated by a qualified person within the water utility or a suitably qualified third-party organization. When undertaking the validation, the following should be considered:

- theoretical approaches and calculations;
- simulation of specific hazard conditions;
- valuation of data or records collected from measures implemented during normal operation.

### 6.4 Protection assessment

#### 6.4.1 General

For reliable property protection, all recommended property protective security measures should be implemented. Once installed, their effectiveness in operation should be monitored, tested and audited. In addition, the effective interaction of each security measure should be assessed critically and for interdependencies with other measures, confirmed and, if necessary, modified and optimized.

#### 6.4.2 Ongoing review

The audit should be repeated periodically. The frequency of the auditing depends on the condition of the water system in relation to its environmental conditions (e.g. the need for protection or threats to the infrastructure). If critical changes occur in water and wastewater systems regarding legal requirements, technical regulation or environmental threats, then the frequency of revision should change accordingly.

#### 6.4.3 Corrective measures

If the protection level required is not achieved, appropriate corrective measures should be taken.

## 7 Documentation

The evaluation of water supply systems, the selected measures for risk control, the validation, the implementation and operational monitoring of measures, the definition and implementation of corrective measures and verification should be documented in a comprehensive manner (see ISO 24518<sup>[6]</sup> and ISO/TS 24520<sup>[7]</sup>).

## 8 Infrastructure hardening examples and configurations

### 8.1 General

The hardening of an element in a water system may be achieved in a basic configuration or in a configuration that includes additional hardening elements.

The decision on which configuration to choose should depend on:

- the level of risk to the specific water system being considered, as discovered during the investigation described in [5.2](#) and [5.3](#);
- the budget and assets allocated to the water utility for the hardening of the water system.

### 8.2 Recommended configurations for the hardening of the different elements of a water system

[Annex A](#) provides an example of recommended configurations for water and wastewater infrastructure, as practiced in Israel.

[Annex B](#) provides an example of the indicative asset security categorization and security treatment schedules as practiced in Australia.

[Annex C](#) provides an example of recommended configurations for water and wastewater infrastructure, as practiced in Germany.

NOTE Security treatments can be permanent or temporary. Permanent security treatments are installed to form an integral component of the ultimate asset infrastructure. Temporary security treatments do not form an integral component of the ultimate asset infrastructure and can be considered during construction periods or following emergency events.

STANDARDSISO.COM : Click to view the full PDF of ISO 24596:2024

## Annex A (informative)

### Example of recommended security measure configurations for water and wastewater infrastructure as practised in Israel

#### A.1 General

This annex details recommended configurations for basic and additional security measures for the different components of water and wastewater systems.

#### A.2 Water and wastewater treatment plants

The basic configuration consists of:

- peripheral physical fence or electronic fence and gates;
- magnetic sensors on all doors and openings;
- automatic outlet valves shut off when the sensors are tripped;
- volume detector;
- video cameras (drones can be considered);
- cyber security protection, hardened according to the IEC 62443 series<sup>[10]</sup> and ISO/IEC 27000<sup>[9]</sup>;
- online water quality analysers.

All sensors should be monitored through a centralised SCADA (supervisory control and data acquisition) system or any other system that can receive the data and control the actions that have to be taken.

#### A.3 Closed water reservoir or tank

The basic configuration consists of:

- peripheral physical fence or electronic fence and gates;
- magnetic sensors on all tank openings;
- sensors on ladders;
- automatic outlet valves on the tank that shuts off when the sensors are tripped.

All sensors should be monitored through a central SCADA system or any other system that can receive the data and control the actions that have to be taken.

Additional site security measures configuration options may include:

- volume detector;
- video cameras (drones can be considered);
- peripheral beam detectors;
- automatic operation of lighting system.

#### **A.4 Water reservoir**

The basic configuration consists of:

- peripheral physical fence or electronic fence and gates;
- automatic peripheral lighting that is activated when a sensor is tripped;
- video cameras (drones can be considered).

All sensors should be monitored through a central SCADA system or any other system that can receive the data and control the actions that have to be taken.

Additional site security measure configuration options include:

- volume detectors;
- human guards.

#### **A.5 Open channels**

The basic configuration consists of:

- physical or electronic fence with hardened locked gates throughout the length of the channel;
- volumetric sensors for detecting unauthorized activity along the channel;
- automatic peripheral lighting that is activated when a sensor is tripped;
- video cameras (drones can be considered).

All sensors should be monitored through a central SCADA system or any other system that can receive the data and control the actions that have to be taken.

#### **A.6 Water pipeline**

The basic configuration consists of:

- burying the pipeline 0,6 m to 1-m underground;
- in the sectors of the pipeline that have to be above ground, the protection should include a physical fence with a hardened locked gate;
- continuous monitoring system and an EDS (to be considered).

#### **A.7 Air release valves, drain pipes, fire hydrants and other above-ground devices**

The basic configuration consists of:

- the device should be surrounded by a physical fence with a hardened locked gate;
- optional: in vulnerable areas, the air release valve is enclosed in a special locked metal box;
- optional: in highly vulnerable areas, the air release valve is enclosed in a special locked metal box with magnetic sensors.

## A.8 Dosing pumps

The basic configuration consists of:

- dosing pumps installed in a locked room while the chemical tank is installed in a separate ventilated locked room;
- the entire system located in a fenced site with magnetic sensors on the doors and/or volume detectors.

## A.9 Wells, water and wastewater pumping stations

The basic configuration consists of:

- the water wells and water and wastewater pumping stations site enclosed in a fence with a peripheral beam alarm;
- openings that allow access to the water or wastewater body, for level measurement and other purposes, locked and strengthened;
- optional: the water well or pumping station enclosed in a conventional concrete building with hardened locks and magnetic sensors on the doors and/or volume detectors.

## A.10 SCADA systems

The basic configuration consists of:

- UPS backup;
- additional stand-alone computer;
- hierarchy: central controller, secondary control centres (intercommunicating) and end infrastructure that can work locally or remotely;
- cybernet protection, hardened according to the IEC 62443 series<sup>[10]</sup> and ISO/IEC 27000<sup>[9]</sup>.

## A.11 Communication systems

The basic communication systems are:

- wireless;
- satellite;
- Internet.

These systems should be hardened according to the IEC 62443 series<sup>[10]</sup> and ISO/IEC 27000<sup>[9]</sup>.

## A.12 Internet of things (IoT) system security

There is a wide range of IoT devices and systems. These should be hardened according to the IEC 62443 series.<sup>[10]</sup>

**Annex B**  
(informative)

**Example of the indicative asset security categorization and security treatment schedules as practised in Australia**

Security treatment schedule					
	Category 5: very high-risk sites	Category 4: high-risk sites	Category 3: moderate-risk sites	Category 2: mild-risk sites	Category 1: low-risk sites
<b>Indicative asset types</b>	<ul style="list-style-type: none"> <li>— important dams or reservoirs</li> <li>— major pumping stations</li> <li>— important communications facilities</li> <li>— operating centres</li> <li>— important WWTPs and WTPs</li> <li>— critical office complex</li> </ul>	<ul style="list-style-type: none"> <li>— minor dams or reservoirs</li> <li>— storage tanks</li> <li>— semi-major PSs</li> <li>— important PRVs</li> <li>— important borefields and ancillary equipment</li> <li>— important GWTPs</li> <li>— minor WWTPs and WTPs</li> <li>— regional office, major operations depots</li> </ul>	<ul style="list-style-type: none"> <li>— minor storage tanks</li> <li>— PRVs</li> <li>— important PSs (riverwise)</li> <li>— minor borefields and ancillary equipment</li> <li>— minor GWTPs</li> <li>— major office complex incorporating an operations depot</li> </ul>	<ul style="list-style-type: none"> <li>— minor PSs</li> <li>— minor PRVs</li> <li>— drainage basins</li> <li>— steep-sided open drains</li> <li>— small borefields and ancillary equipment</li> <li>— small operations depots</li> </ul>	<ul style="list-style-type: none"> <li>— pipe reserves</li> <li>— swale drains</li> <li>— recreational-type basins</li> <li>— pits in isolated locations</li> <li>— flood protection structures with valves that release water</li> <li>— drainage drop structures easily accessed by the public</li> <li>— drainage monitoring stations</li> </ul>
<p><b>Key</b></p> <p>ADWG Australian drinking water guidelines</p> <p>GWTP groundwater treatment plant</p> <p>PRV pressure reducing valve</p> <p>PS pumping station</p> <p>WPS water pump station</p> <p>WTP water treatment plant</p> <p>WWPS wastewater pump station</p> <p>WWTP wastewater treatment plant</p> <p>NOTE For the ASTM Standard, Australian Standards (AS), New Zealand Standards (NZS) and British Standards (BS) used to inform this hardening specification, see in bibliography References [12] to [92].</p>					

## ISO 24596:2024(en)

Security treatment schedule					
	Category 5: very high-risk sites	Category 4: high-risk sites	Category 3: moderate-risk sites	Category 2: mild-risk sites	Category 1: low-risk sites
<b>Physical barriers</b>	<p>Category 4 requirements, plus: Consider multiple barriers and/or levels of hardened protection.</p>	<p>Category 3 requirements, plus: Strong deterrent fencing considered (palisade, electric, razor wire). or Substantially engineered structures and operating equipment enclosures with substantial engineered preventive mechanism placed on access and entry points.</p> <p>Consider vehicle penetration and perimeter bollards or similar controls considered to prevent damage to buildings and operating equipment.</p> <p>Drinking water storage hatches to be alarmed.</p> <p>Dams – hardened locking, hinge fittings and door or grill access to gallery and tunnel.</p> <p>Consider intruder alarm on major external valve pits and control cubicles.</p> <p>Consider chain mesh fencing higher than 1,8 m.</p>	<p>Category 2 requirements, plus: Door plates of substantial thickness. Hinges and locks protected, enclosed and intruder-resistant. Secure profile keying to critical site elements. Fencing installed to minimum 1,8 m high with three strands of barbed wire.</p> <p>Buildings, structures and operating equipment provided with hardened protection. Drinking water storage hatches to be alarmed, where practicable.</p>	<p>Category 1 requirements, plus: Basic fencing 1,8 m chain mesh with barbed wire top and bottom or inherent exclusion provision from operational units (i.e. install equipment in pits with manhole covers, cabling in conduit, light covers locked). Drinking water storages to have locked hatches (padlocks to be covered).</p>	<p>Child exclusion fencing, where appropriate (1,2 m chain mesh). Child safety barriers on structures. Design out of unsafe features, i.e. use of swale drains and other velocity minimization techniques. Pits covered, where necessary.</p> <p>Restricted profile locks on all access hatches.</p>
<b>Lighting</b>	<p>Category 4 requirements, plus: Strong comprehensive and building permanent perimeter lighting installed where practicable in vandal-resistant containers.</p>	<p>Category 3 requirements, plus: Movement sensor switched lighting to key access areas with short strike rate.</p>	<p>Where appropriate, all-night building perimeter lighting on all doors and access points.</p>		
<p><b>Key</b></p> <p>ADWG Australian drinking water guidelines            GWTP groundwater treatment plant            PRV pressure reducing valve            PS pumping station            WPS water pump station            WTP water treatment plant            WWPS wastewater pump station            WWTP wastewater treatment plant</p> <p>NOTE For the ASTM Standard, Australian Standards (AS), New Zealand Standards (NZS) and British Standards (BS) used to inform this hardening specification, see in bibliography References [12] to [92].</p>					

## ISO 24596:2024(en)

Security treatment schedule					
	Category 5: very high-risk sites	Category 4: high-risk sites	Category 3: moderate-risk sites	Category 2: mild-risk sites	Category 1: low-risk sites
<b>Electronic</b>	Category 4 requirements, plus: Consider CCTV integrated with photoelectric external perimeter beams with offsite control.	Category 3 requirements, plus: Monitored intruder alarms to asset physical perimeter and / or critical buildings and operational equipment. Consider CCTV access control to entrance points, where appropriate.	Category 2 requirements, plus: Monitored intruder alarms to buildings and operational equipment, where appropriate. Consider movement detectors as part of alarm system. Monitored smoke detection alarm installed, where appropriate.	All exposed externally run communications cabling and wiring enclosed in vandal-resistant conduit.	
<b>Community</b>	Category 4 requirements, plus: Regular regional and district police and emergency services liaison. Regular active utility and stakeholder liaison occurring (e.g. rangers)	Category 3 requirements, plus: Active local community watch operating. Regular community watch stakeholder briefings occur.	Category 2 requirements	Signage identifies all hours emergency and security number.	
<b>Access control</b>	Category 4 requirements, plus: Site access restricted to operational and necessary access only, at all times.	Category 3 requirements, plus: Specific site access control management procedures apply. Consider electric (auto) gates at treatment plants and major depots.	Active identification pass system in place where intruder alarms exist. All contractors and visitors require entry authorization and notification.		
<p><b>Key</b></p> <p>ADWG Australian drinking water guidelines</p> <p>GWTP groundwater treatment plant</p> <p>PRV pressure reducing valve</p> <p>PS pumping station</p> <p>WPS water pump station</p> <p>WTP water treatment plant</p> <p>WWPS wastewater pump station</p> <p>WWTP wastewater treatment plant</p> <p>NOTE For the ASTM Standard, Australian Standards (AS), New Zealand Standards (NZS) and British Standards (BS) used to inform this hardening specification, see in bibliography References [12] to [92].</p>					

ISO 24596:2024(en)

Security treatment schedule					
	Category 5: very high-risk sites	Category 4: high-risk sites	Category 3: moderate-risk sites	Category 2: mild-risk sites	Category 1: low-risk sites
<b>Information</b>	Category 4 requirements, plus: Signage or community-based corporate information reviewed for sensitive operational information. Site plans, operational procedures and processes are all available, marked for sensitivity and actively controlled.	Category 3 requirements, plus: Plans on site to be secured and controlled. All emergency plans and manifests secured within a designated building within the perimeter.	Category 2 requirements, plus: Clear perimeter ownership and deterrent signage on all perimeter fence panels or buildings and structures, where no fence exists, which are readily viewable by the community (min. 100 metres apart, 50 metres recommended). All emergency manifests secured within the external perimeter.	Perimeter signage restricted to ownership and specific hazard warning information. Documented security systems plans, alarm response measures, commissioning certificates and maintenance requirements.	
<b>Response</b>	Category 4 requirements, plus: On-site static security guards when advised. Contingency plan integrated and actively practised with emergency services and response agencies. Contingency resources readily available and routinely checked.	Category 3 requirements, plus: 24/7 response applies. Enhanced response from: on-site security alarm police emergency services corporation staff, if safe detailed and practiced active contingency plan.	Category 2 requirements, plus: Corporation security response in tandem with contract security response.	Reactive response only based on local information or reports. Security response when advised of confirmed security breach.	
<b>Procedural</b>	Category 4 requirements, plus: Site operations and safety strictly controlled. Site visits closely monitored and controlled. Specific safety training required where applicable.	Category 3 requirements, plus: Site-specific safety and security briefing. Site entry and exit reporting and documented. Contractor independent attendance documented and monitored. Annual protective systems testing and review programme.	Category 2 requirements, plus: Site specific annually reviewed site safety and security assessment conducted and documented.	Routine documented safety assessment conducted with documented safety procedure where required.	
<p><b>Key</b></p> <p>ADWG Australian drinking water guidelines            GWTP groundwater treatment plant            PRV pressure reducing valve            PS pumping station            WPS water pump station            WTP water treatment plant            WWPS wastewater pump station            WWTP wastewater treatment plant</p> <p>NOTE For the ASTM Standard, Australian Standards (AS), New Zealand Standards (NZS) and British Standards (BS) used to inform this hardening specification, see in bibliography References [12] to [92].</p>					

ISO 24596:2024(en)

Security treatment schedule					
	Category 5: very high-risk sites	Category 4: high-risk sites	Category 3: moderate-risk sites	Category 2: mild-risk sites	Category 1: low-risk sites
<b>Maintenance</b>	Category 3 requirements, plus: Any security systems and physical control failures to be investigated, documented and rectified as a priority maintenance item.	Category 3 requirements apply	Category 2 requirements, plus: Review of designated physical security controls (i.e. fences, gates and locks) and security systems to ensure they are covered as part of the automatic annual maintenance plan.	Active annual maintenance programme.	
<b>Asset types (indicative)</b> <b>Refer to asset category rating table</b>	<ul style="list-style-type: none"> <li>— important dams or reservoirs</li> <li>— major pumping stations</li> <li>— important communications or data facilities</li> <li>— operation centres</li> <li>— major WTP or WWTP</li> <li>— critical office complex</li> </ul>	<ul style="list-style-type: none"> <li>— minor dams or reservoirs</li> <li>— storage tanks</li> <li>— semi-major PSs</li> <li>— important PRVs</li> <li>— important borefields and ancillary equipment</li> <li>— important WTPs and GWTPs</li> <li>— minor WWTPs</li> <li>— regional office and major operations depots</li> <li>— important communication towers or nodes</li> </ul>	<ul style="list-style-type: none"> <li>— minor storage tanks</li> <li>— PRVs</li> <li>— important WPSs and WWPS (riverwise)</li> <li>— minor borefields and ancillary equipment</li> <li>— minor WTPs and GWTPs</li> <li>— major office complex incorporating an operations depots</li> <li>— individual bores</li> <li>— minor communication towers</li> <li>— small operations depots</li> </ul>	<ul style="list-style-type: none"> <li>— minor PSs</li> <li>— minor PRVs</li> <li>— drainage basins</li> <li>— steep-sided open drains</li> <li>— small borefields and ancillary equipment</li> <li>— bridges and drainage drop structures easily accessed by public</li> </ul>	<ul style="list-style-type: none"> <li>— pipe reserves</li> <li>— swale drains</li> <li>— recreational-type basins</li> <li>— pits in isolated locations</li> <li>— flood protection structures with valves that release water</li> <li>— drainage monitoring stations</li> </ul>
<p><b>Key</b></p> <p>ADWG Australian drinking water guidelines</p> <p>GWTP groundwater treatment plant</p> <p>PRV pressure reducing valve</p> <p>PS pumping station</p> <p>WPS water pump station</p> <p>WTP water treatment plant</p> <p>WWPS wastewater pump station</p> <p>WWTP wastewater treatment plant</p> <p>NOTE For the ASTM Standard, Australian Standards (AS), New Zealand Standards (NZS) and British Standards (BS) used to inform this hardening specification, see in bibliography References [12] to [92].</p>					

## ISO 24596:2024(en)

Security treatment schedule					
	Category 5: very high-risk sites	Category 4: high-risk sites	Category 3: moderate-risk sites	Category 2: mild-risk sites	Category 1: low-risk sites
<b>Physical</b>	<p>Category 4 requirements, plus: Consider multiple barriers and/or levels of hardened physical protection.</p>	<p>Category 3 requirements, plus: Consider strong deterrent fencing (e.g. palisade, electric, razor wire). or Substantially engineered structures and operating equipment enclosures with substantial engineered preventive mechanism placed on access and entry points. Consider vehicle penetration and perimeter bollards or similar controls to prevent damage to buildings and operating equipment. Drinking water storage hatches to be alarmed. Dam offtake tower bridge: substantial anti-climb protective barriers above and below the access structure  Dams: hardened locking, hinge fittings and door or grill access to gallery and tunnel. Consider intruder alarm on major external valve pits and control cubicles. Chain mesh fencing higher than 2,1 m.</p>	<p>Category 2 requirements, plus: Door plates of substantial thickness. Hinges enclosed or intruder-resistant. Secure profile keying to critical site elements. Fencing installed to minimum 1,8 m high with three strands of barbed wire. or Buildings, structures and operating equipment provided with hardened protection. Drinking water storage hatches to be alarmed, where practicable. Single emergency action egress to all perimeter and internal doors.</p>	<p>Category 1 requirements, plus: Basic fencing 1,8 m chain mesh with barbed wire top and bottom and/or inherent exclusion provision from operational units. Install equipment in pits with manhole covers, cabling in conduit, light covers locked.</p>	<p>Public safety or child exclusion fencing where appropriate (1,2 m chain mesh). Child safety barriers on structures. Design out of unsafe features, i.e. use of swale drains and other velocity minimization techniques. Pits covered where necessary. Graffiti-resistant treatments. Restricted profile locks on all access hatches.</p>
<p><b>Key</b></p> <p>ADWG Australian drinking water guidelines            GWTP groundwater treatment plant            PRV pressure reducing valve            PS pumping station            WPS water pump station            WTP water treatment plant            WWPS wastewater pump station            WWTP wastewater treatment plant</p> <p>NOTE For the ASTM Standard, Australian Standards (AS), New Zealand Standards (NZS) and British Standards (BS) used to inform this hardening specification, see in bibliography References [12] to [92].</p>					

## ISO 24596:2024(en)

Security treatment schedule					
	Category 5: very high-risk sites	Category 4: high-risk sites	Category 3: moderate-risk sites	Category 2: mild-risk sites	Category 1: low-risk sites
<b>Lighting</b>	Category 4 requirements, plus: Strong comprehensive and building permanent perimeter lighting.	Category 3 requirements, plus: Movement sensor switched lighting to key access areas with short strike activation.	Where appropriate, all night building perimeter lighting on all primary access doors and emergency access points. Installed where practicable in environmentally robust and vandal-resistant containers.		
<b>Electronic</b>	Category 4 requirements, plus: Consider CCTV integrated with photoelectric external perimeter beams with offsite control.	Category 3 requirements, plus: AS/NZS 2201.1 <sup>[32]</sup> compliant monitored intruder alarms to asset physical perimeter and/or critical buildings and operational equipment. Consider external intruder alarm beams and technology. Consider remote monitored, alarm integrated CCTV and access control to entrance points where appropriate. Dams – intruder alarms: — at offtake building — gallery and tunnel entrances	Category 2 requirements, plus: Monitored intruder alarms to buildings and operational equipment where assessed. Multisector activation detectors to be installed. Monitored smoke or heat detection alarm installed, where appropriate.	All exposed externally run communications cabling and wiring enclosed in vandal-resistant and fire-resistant conduit.	
<p><b>Key</b></p> <p>ADWG Australian drinking water guidelines            GWTP groundwater treatment plant            PRV pressure reducing valve            PS pumping station            WPS water pump station            WTP water treatment plant            WWPS wastewater pump station            WWTP wastewater treatment plant</p> <p>NOTE For the ASTM Standard, Australian Standards (AS), New Zealand Standards (NZS) and British Standards (BS) used to inform this hardening specification, see in bibliography References [12] to [92].</p>					

## ISO 24596:2024(en)

Security treatment schedule					
	Category 5: very high-risk sites	Category 4: high-risk sites	Category 3: moderate-risk sites	Category 2: mild-risk sites	Category 1: low-risk sites
<b>Fire</b>		<p>Category 2 requirements, plus: Consider requirement for separate integrated fire panel and detection or alert systems with direct brigade alarms (DBAs). Consider fire resistance level (FRL) separation for wall and floor structures. Consider independent fire suppression systems requirements. Consult with corporation insurers.</p>	<p>Category 2 requirements, plus: Structures all built according to principles of AS 3959[76]. Ember screens requirement and heat survivability assessed. Active, externally reporting fire detection systems installed to electronic systems (intruder alarm). Fire hose or hydrant requirement assessed. Consider AS compliant fire-rated door requirements.</p>	<p>Category 1 requirements, plus: Flammable material cabinets installed where required. Fire fuel load, hazard separation requirements assessed. Building structure flammability, hazard separation requirements assessed. Fire thermal barrier requirement for isolated assets risk assessed Fire extinguishers assessed and installed to AS 2444[73]. Emergency exits and emergency exit signs.</p>	<p>Maximum distance regulatory required fire breaks and asset fire protection zones (see AS 3959[76].)</p>
<b>Community</b>	<p>Category 4 requirements, plus: Regular regional and district police and emergency services liaison. Regular active utility and stakeholder liaison occurring (e.g. police, rangers.)</p>	<p>Category 3 requirements, plus: Active local “community watch” operating. Regular “community watch” stakeholder briefings occur.</p>	<p>Category 2 requirements</p>	<p>Signage identifies all-hours emergency and security number.</p>	
<b>Access control</b>	<p>Category 4 requirements, plus: Site access restricted to operational and necessary access only, at all times.</p>	<p>Category 3 requirements, plus: Specific site access control management procedures apply. Consider electric (auto) gates at treatment plants and major depots.</p>	<p>Active identification pass system in place where intruder alarms exist. All contractors and visitors require entry authorization and notification.</p>		
<p><b>Key</b></p> <p>ADWG Australian drinking water guidelines            GWTP groundwater treatment plant            PRV pressure reducing valve            PS pumping station            WPS water pump station            WTP water treatment plant            WWPS wastewater pump station            WWTP wastewater treatment plant</p> <p>NOTE For the ASTM Standard, Australian Standards (AS), New Zealand Standards (NZS) and British Standards (BS) used to inform this hardening specification, see in bibliography References [12] to [92].</p>					

## ISO 24596:2024(en)

Security treatment schedule					
	Category 5: very high-risk sites	Category 4: high-risk sites	Category 3: moderate-risk sites	Category 2: mild-risk sites	Category 1: low-risk sites
<b>Information</b>	Category 4 requirements, plus: Signage or community-based corporate information reviewed for sensitive operational information. Site plans and operational procedures and processes are all available, marked for sensitivity and actively controlled.	Category 3 requirements, plus: Plans on site to be secured and controlled. All emergency plans and manifests secured within a designated building within the perimeter.	Category 2 requirements, plus: Clear perimeter ownership and deterrent signage on all perimeter fence panels or buildings and structures, where no fence exists, which are readily viewable by the community (min. 100 m apart, 50 m recommended). All emergency manifests secured within the external perimeter.	Perimeter signage restricted to ownership and specific hazard warning information. Documented security systems plans, alarm response measures, commissioning certificates and maintenance requirements.	
<b>Response</b>	Category 4 requirements, plus: Onsite static security guards when advised. Contingency plan integrated and actively practised with emergency services and response agencies.  Contingency resources readily available and routinely checked.	Category 3 requirements, plus: 24/7 response applies. Enhanced response from: <ul style="list-style-type: none"> <li>— on-site security alarm</li> <li>— police</li> <li>— emergency services</li> <li>— corporation staff, if safe</li> </ul> Detailed and practised active contingency plan.	Category 2 requirements, plus: Corporation security response in tandem with contract security response.	Reactive response only based on local information or reports.  Security response when advised of confirmed security breach.	
<p><b>Key</b></p> <p>ADWG Australian drinking water guidelines            GWTP groundwater treatment plant            PRV pressure reducing valve            PS pumping station            WPS water pump station            WTP water treatment plant            WWPS wastewater pump station            WWTP wastewater treatment plant</p> <p>NOTE For the ASTM Standard, Australian Standards (AS), New Zealand Standards (NZS) and British Standards (BS) used to inform this hardening specification, see in bibliography References [12] to [92].</p>					

## ISO 24596:2024(en)

Security treatment schedule					
	Category 5: very high-risk sites	Category 4: high-risk sites	Category 3: moderate-risk sites	Category 2: mild-risk sites	Category 1: low-risk sites
<b>Procedural</b>	Category 4 requirements, plus: Site operations and safety strictly controlled. Site visits closely monitored and controlled. Specific safety training required where applicable.	Category 3 requirements, plus: Site-specific safety and security briefing. Site entry and exit reporting and documented. Contractor independent attendance documented and monitored. Annual protective systems testing and review programme.	Category 2 requirements, plus: Site-specific annually reviewed site safety and security assessment conducted and documented.	Routine documented safety and security assessment conducted with documented safety procedure where required.	
<b>Maintenance</b>	Category 3 applies Any security systems and physical control failures to be investigated, documented and rectified as a priority maintenance item.	Category 3 applies	Category 2 requirements, plus: Review of designated physical security controls (i.e. fences, gates and locks) and security systems to ensure they are covered as part of the automatic annual maintenance plan.	Active annual maintenance programme. Compliant with Australian or industry standards. Documented maintenance requirements.	
<p><b>Key</b></p> <p>ADWG Australian drinking water guidelines            GWTP groundwater treatment plant            PRV pressure reducing valve            PS pumping station            WPS water pump station            WTP water treatment plant            WWPS wastewater pump station            WWTP wastewater treatment plant</p> <p>NOTE For the ASTM Standard, Australian Standards (AS), New Zealand Standards (NZS) and British Standards (BS) used to inform this hardening specification, see in bibliography References [12] to [92].</p>					

## **Annex C** (informative)

### **Example of recommended security measure configurations for water and wastewater infrastructure as practised in Germany**

#### **C.1 Outside building barrier layer element examples**

##### **C.1.1 Physical protection**

- Burglar-resistant doors, windows (including glass) and access covers;
- window glass – cutting and breakage resistant;
- door locks;
- steel bar elements within doors, windows and walls.

##### **C.1.2 Electronic protection**

- Infrared outdoor systems;
- video sensors;
- light barriers;
- high-speed auto dome cameras (drones can be considered);
- door monitors (e.g. magnetic sensors);
- window monitors (e.g. open-close sensors, breakage sensors).

#### **C.2 Inside building barrier layer element examples**

##### **C.2.1 Physical protection**

- Door locks;
- steel bar elements within doors, windows and walls.

##### **C.2.2 Electronic protection**

- Infrared systems;
- movement sensors;
- block lock systems;
- alarm systems;
- personnel access systems.

### **C.3 Device barrier layer element examples**

#### **C.3.1 Sensors monitoring water flow**

- Pressure;
- flow.

#### **C.3.2 Sensors monitoring water quality**

- Turbidity;
- disinfectant levels;
- dosing chemical monitors.

#### **C.3.3 Sensors or process monitoring data**

- Data quality;
- digital system integrity.

STANDARDSISO.COM : Click to view the full PDF of ISO 24596:2024

## **Annex D** (informative)

### **Example of general protection elements for water and wastewater infrastructure**

#### **D.1 Physical protection of infrastructure**

##### **D.1.1 General**

This clause describes the key design aspects of gates and fences used in hardening a site.

##### **D.1.2 Welded mesh fence**

The purpose of the welded mesh fence is to prevent unauthorized access to the area surrounding the different elements of the system. The welded mesh fence should be hooked up to a series of pillars along the perimeter of the site.

##### **D.1.3 Posts**

Posts should be galvanized in hot zinc and covered by plastic covers at their top. The posts should be sufficiently high to prevent jumping or climbing over the fence.

The upper part of the post should be manufactured so that it is bent at the top and installed so that the bend is facing outwards from the site.

Posts should have supports where necessary. The posts and support should be installed on an appropriate concrete foundation.

##### **D.1.4 Paint work**

Exposed parts of the fence elements should be painted, including welding points. Steel areas that will be anchored in the concrete should not be painted.

The first layer of paint should be in an anti-corrosive primary colour and proceeded by two additional layers of paint.

Painting should be completed after any welding.

##### **D.1.5 Gates for vehicle entrance**

To allow for operation and maintenance of the water system elements in the site, access should be given to vehicles inside the perimeter of the element.

Therefore, the fence should include a gate to allow entrance and outlet of the service vehicles. The width of the gate should allow for the widest service vehicles to transit through the gate.

##### **D.1.6 Gates for pedestrians**

To allow for operation and maintenance of the water system elements in the site, access should be permitted to pedestrians inside the perimeter of the element.

Therefore, the fence should include a pedestrian gate.

## D.2 Physical protection for covered water storages with hatch access and their ladders

### D.2.1 General

This clause describes physical protective measures using doors and hatches against unauthorized intrusion inside the reservoir.

One of the main entries for the introduction of contaminants into a water storage reservoir is through the reservoir's openings.

All access points are to be considered and assessed for security and safety treatments.

These physical barriers associated with the reservoir openings should be designed and constructed in a manner commensurate with the risk. Openings should be designed to prevent the entry of the primary hazard, whether this is an environmental hazard such as ash from a fire or a human intruder.

For a human intruder, the level of barrier should depend on the criticality of the site and range from basic locks to covered locks to prevent bolt cutters, through to doors with additional shielding and barriers to delay ingress and allow response by the water facility.

In addition to the direct physical barrier, an early alert system may be used to detect motion within the site or around the hatches. This may be augmented by video surveillance and detection shields that send a notification if a door or hatch is being tampered with. Early detection of the intent will allow an appropriate and timely response.

### D.2.2 Levels of intrusion protection examples

Level of protection 1 – basic:

- estimated time for intrusion: 2 min to 4 min;
- smaller than level protection 2 thickness plate to cover the access point for the reservoir;
- around the reservoir openings, a square metal frame anchored by internal anchors;
- covert door hinges;
- latch lock to lock the door to the frame.

Level of protection 2 – high level of hardening:

- estimated time for intrusion: more than 5 min;
- protection with special door, for example small safe box door that saves the need for the top grill;
- thicker than level protection 1 metal plate covering access point for the reservoir;
- recessed frame into the safe box lintel anchored by internal anchors;
- covert door hinges;
- bolts system to locking of the door to the frame (3 to 4 bolts depending on door diameter), 30 mm diameter;
- bolts penetrating the frame and the concrete from both sides; lock and bolts;
- strong and secure lock inside a protected box;
- covert handle for opening and closing;
- opening supported by two hydraulic pistons.