en.dwa.de

DWA
Clear Concepts. Clean Environment.

DWA Set of Rules

Guideline DWA-M 1060E

IT-Security – Standard for Water Supply/Wastewater Utilities

August 2017

IT-Sicherheit – Branchenstandard Wasser/Abwasser
August 2017

DVGW

en.dwa.de

DWA
Clear Concepts. Clean Environment.

DWA Set of Rules

Guideline DWA-M 1060E

IT-Security – Standard for Water Supply/Wastewater Utilities

August 2017

IT-Sicherheit – Branchenstandard Wasser/Abwasser
August 2017

Warning

This English-language version is an informal translation from the German original. Only the original German language version has been exclusively authorised by the Technical Committees of DVGW and DWA.

Users are responsible for the proper implementation and the use of further related rules.The German Association for Water, Wastewater and Waste (DWA) is strongly committed to the development of secure and sustainable water and waste management. As a politically and economically independent organisation it is professionally active in the field of water management, wastewater, waste and soil protection.

In Europe DWA is the association with the largest number of members within this field. Therefore it takes on a unique position in connection with professional competence regarding standardisation, professional training and information. The approximately 14,000 members represent specialists and executives from municipalities, universities, engineering offices, authorities and companies.

Imprint

Publisher and marketing:
German Association for
Water, Wastewater and Waste (DWA)
Theodor-Heuss-Allee 17
53773 Hennef, Germany
Tel.: +49 2242 872-333
Fax: +49 2242 872-100
E-Mail: info@dwa.de
Internet: www.dwa.de

Translation:
WORTWECHSEL, Doris Mann, Karlsruhe

Print:
Bonner Universitäts-Buchdruckerei

ISBN:
978-3-88721-772-3 (Print)
978-3-88721-773-0 (E-Book)

Printed on 100 % recycled paper

© Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V. (DWA), Hennef 2018
German Association for Water, Wastewater and Waste

All rights, in particular those of translation into other languages, are reserved. No part of this Advisory Guideline may be reproduced in any form – by photocopy, digitalisation or any other process – or transferred into a language usable in machines, in particular data processing machines, without the written approval of the publisher.

Foreword

This Guideline has been elaborated by a project group of the DVGW Joint Technical Committee on "IT Security" in cooperation with the DWA Working Group on "Cyber Security".

Article 8a (2) of the Act to Strengthen the Security of Federal Information Technology (*BSIG*) offers industry sectors an opportunity to develop an industry-specific IT security standard (B3S) for IT system security, in particular for the security of information technology systems, components or processes that are indispensable for maintaining the operation of critical infrastructures and/or critical services. In conjunction with the DVGW/DWA IT Security Code of Practice and the DVGW/DWA Regulations on the Procedures of Furnishing Proof pursuant to Article 8a (3) BSIG, this Guideline at hand represents the industry-specific IT Security Standard for the water industry sector, i.e. the drinking water supply and wastewater disposal industries. After consultation with the Federal Office for Civil Protection and Disaster Assistance (*Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK*), the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik, BSI*) has recognised the suitability of the IT Security Standard for the water industry sector.

The IT Security Standard for the water industry sector serves as a basis for assessing risks and carrying out controls designed to protect the information technology systems, components, processes and data of water supply and wastewater installations, regardless of whether or not an installation falls within the scope of critical infrastructures in accordance with the Ordinance on Critical Infrastructures of the Federal Office for Information Security *(BSI-KritisV).*

The Federal Office for Information Security *(Bundesamt für Informationssicherheit, BSI)* recommends joining UP KRITIS to operators of water supply installations that handle a total volume and/or a minimum volume of 2.2 million m^3 of abstracted, treated or distributed water and to operators of wastewater installations that service a minimum of 50,000 persons connected to a sewer system and/or a wastewater treatment plant or control centre with a design capacity of 50,000 population equivalents. UP KRITIS is a public-private cooperation between operators of Critical Infrastructures (*KRITIS*) and their associations and the BSI and BBK as responsible government authorities. The goal of the UP KRITIS cooperation is to maintain the supply of services provided by Critical Infrastructures in Germany.

Smaller operators of Critical Infrastructures are advised to join the *"Allianz für Cybersicherheit"* (Cyber Security Alliance), a platform that was initiated by the BSI and the German Association for IT, Telecommunications and New Media (*BITKOM*, a registered association) with the objective being to sustainably enhance cyber security in Germany.

Amendments:

All-new guideline

Earlier editions

None

Authors

This Guideline has been elaborated by a project group of the DVGW Joint Technical Committee on "IT Security" in cooperation with the DWA Working Group on "Cyber Security".

Project organizer within the DWA Head Office :

HETZEL, Friedrich Dr., Hennef
Department Wastewater and Water Protection

Content

List of Figures

User Notes

This Guideline has been produced by a group of technical, scientific and economic experts, working in an honorary capacity and applying the rules and procedures of the DWA and the Standard DWA-A 400. Based on judicial precedent, there exists an actual presumption that this document is textually and technically correct.

Any party is free to make use of this Guideline. However, the application of its contents may also be made an obligation under the terms of legal or administrative regulations, or of a contract, or for some other legal reason.

This Guideline is an important, but not the sole, source of information for solutions to technical problems. Applying information given here does not relieve the user of responsibility for his own actions or for correctly applying this information in specific cases. This holds true in particular when it comes to respecting the margins laid down in this Guideline.

Introduction

Water supply and wastewater installations are always considered Critical Infrastructures.

Operators of water supply and wastewater disposal installations (hereinafter referred to as "operators") shall have at their disposal high-performance equipment, sufficiently qualified staff – see DVGW W 1000 (A) and DWA-M 1000 – and robust quality assurance measures and/or, alternatively, subcontract qualified experts and monitor the execution of the subcontracted services. Furthermore, they shall be organised in such a way as to ensure the safe, reliable, environmentally compatible and economically efficient operation of their business – see DVGW W 1000 (A), DVGW W 400 Parts 1 through 3 (A), DWA-M 1000, DWA-M 1002 and DWA-A 100.

A risk-based, process-oriented management style with a focus on the individual drinking water supply and wastewater disposal process steps – as specified in the DVGW and DWA Sets of Rules – is target oriented in order to implement these requirements, see DIN EN 15975-2 and DWA-M 801.

The protection of information technology systems, components and processes against failure and/or manipulation constitutes an important risk management element in the operation of water supply and wastewater installations (hereinafter referred to as "installations"). The purposeful protection of the information technology systems, components and processes of installations helps to reduce and, consequently, control risks in the provision of public services. In conjunction with the IT Security Code of Practice, this Guideline at hand serves as an industry-specific security standard that helps identify necessary preventive action to avert threats against the information technology systems, components or processes of installations. Following the recommendations of both, this Guideline and of the IT Security Code of Practice, can help reduce the risk of impairment of public services caused by an abstract hazard, i.e. a hazard likely to occur in the light of actual findings. In the event of a concrete hazard, i.e. a hazard that actually exists in a specific situation, preventive action can be classified on the basis of efficacy.

Additionally, certain situations may arise that occur extremely rarely, are difficult to forecast and, therefore, impossible to make provisions for. Operators may not be able to control such crisis situations, which may also occur after taking IT security controls, on the basis of a conventional organisation structure. In such cases it will be necessary to take appropriate decisions, taking into account all operationally relevant framework conditions. DIN EN 15975-1 provides some guidance on that matter.

1 Scope

This Guideline applies to the identification of controls designed to protect the information technology systems, components or processes of installations that are required for providing drinking water supply and wastewater disposal services, which are Critical Services, in the framework of a risk management approach in accordance with DIN EN 15975-2 and DWA-M 801 and taking into account the BSIG and BSI-KritisV requirements, regardless of whether such installations are operated by a company or whether they have been subcontracted partially or as a whole to a service provider. The underlying approach is based on an all-risk approach.

This Guideline does not cover data protection aspects.

The recommendations of DVGW W 1050 cover property protection aspects and shall be followed in this regard. DVGW Water Information Bulletin No. 80 and DWA-M 213-1 provide additional guidance on security services.

This Guideline does not cover current reporting obligations pursuant to Art. 8b (4) BSIG.

2 Normative references

The following normative documents comprise definitions, which by being referenced in this text form an integral part of the part of the DVGW set of rules at hand. For dated references, later amendments or revisions of this publication shall not apply. However, parties making use of this part of the DVGW set of rules are encouraged to consider the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document, including all amendments, referred to shall apply. Listed DIN standards may be part of the DVGW set of rules.

DVGW W 400-1 (A), *Engineering Rules for Water Supply Systems; Part 1: Design*

DVGW W 400-2 (A), *Engineering Rules for Water Supply Systems; Part 2: Construction and Testing*

DVGW W 400-3 (A), *Engineering Rules for Water Supply Systems; Part 3: Operation and Maintenance*

DVGW W 1000 (A), *Requirements on the Qualification and Organisation of Drinking Water Utilities*

DVGW W 1050 (M), *Objektschutz von Wasserversorgungsanlagen* [*Property protection for Water Supply Utilities*]

DVGW Water Information Bulletin No. 80, *Security Services for Water Supply Utilities – Guidance on How to Draft a Security Service Concept*

DIN 4046, *Water supply; terms*

DIN EN 15975-1, *Security of drinking water supply – Guidelines for risk and crisis management – Part 1: Crisis management*

DIN EN 15975-2, *Security of drinking water supply – Guidelines for risk and crisis management – Part 2: Risk management*

DIN EN 16323, *Glossary of wastewater engineering terms*

DIN EN ISO 22301, *Societal security – Business continuity management systems – Requirements*