Appendix Information Security
(Handling of Viega Information)

Version 1.0
01.10.2023

Table of contents

Change history

Date of change		old version	new version	Editing	Release
17.10.2023		*-*	*1.0*	*M. Kirchmaier*	*B. Heintel*
Chapter		Change			
-	-	Preparation of the Annex			

1 Introduction

This appendix describes the regulations relating to the handling of data and information of Viega to consistently ensure compliance with all information security-relevant aspects in procurement and in the use of external service providers.
In order to be able to protect data and information comprehensively, suppliers, external service providers and subcontractors must be included in information security.

2 Scope

The regulations in this appendix apply to all persons who come into contact with Viega data and information in the life cycle of the contractor-client relationship.
The further contents of the technical delivery specification remain binding for the contractor or deviations are to be released by the respective Viega project manager.

All deviations from this appendix must be requested in writing from the Viega project manager or the CISO (Chief Information Security Officer) of Viega. Approval of the deviations can only be given with the consent of the specialist department placing the order before conclusion of the contract. The acceptance of our order includes the express acknowledgement of these delivery specifications with the waiver of contradictory, own terms and conditions of sale. They supplement the respectively valid General Terms and Conditions of Purchase of Viega.

If orders are passed on to subcontractors, the contractor is responsible for ensuring that this appendix is complied with.

3 Data and information

In the world of information security, data and information are two different concepts, but they are closely linked.

Data: Data are raw, unstructured facts or signs that do not yet have meaning. They are the basic units of information and can exist in various forms, such as text, numbers, images or sounds. Data alone has no context and no specific meaning.

Information: Information is created when data is put into context and interpreted. Information is data that has been organised, processed or structured to have a specific meaning or provide a benefit. It is relevant to decision-making and helps people develop an understanding of a specific situation.

Both data and information exist in different forms. However, they are usually exchanged electronically or in paper form.

It is important to ensure that both data and information are adequately protected. To this end, Viega attaches great importance to the integrity, availability and confidentiality of the data exchanged. This may mean restricting access to sensitive data, using encryption technologies, carrying out regular security checks and ensuring that information is only accessible to authorised persons in order to guarantee the confidentiality, integrity and availability of data and information.

4 Information classes

Viega classifies all information according to its protection needs in terms of confidentiality, integrity, availability and authenticity.

It is the task of every Viega employee to help ensure that information is used in accordance with its classification and that violations of this are reported to the information owner and, in serious cases, to the CISO. This principle also applies in the supplier relationship.

Information within the Viega Group is divided into four protection classes according to their requirements. These are divided into classes A-D. Personal information is subject to data protection and must therefore be treated with appropriate specificity.

Class	Characterisation	Examples of company information
A	**Strictly confidential information** and **business secrets**, the uncontrolled publication of which could mean damage to Viega's existence.	• Strategy papers • Innovation documents • Patent applications • Business secrets according to GeschGehG
B	**Confidential information** intended only for a group of employees, e.g. a department, the disclosure of which could cause damage to Viega's operations.	• Production and shipping information • Characteristics of new products before distribution • Treaties of particular importance • Orders • Transaction data • Construction drawings
C	**Internal information which is** intended for the company's employees or contractual partners and the publication of which would not cause any damage to Viega's business operations.	• Invoices, credit notes • Project portfolio • Process descriptions • Meeting minutes • House messages • Intranet content (if not otherwise classified)
D	**Information** prepared for customers and the interested public and published accordingly and may be passed on **without restriction.**	• Internet presences • Social media content • Brochures, leaflets • Presentations for trade fairs and events

The marking of the protection class is independent of the classification. This is done by printing the **confidentiality class** ("unrestricted", "internal", "confidential", "strictly confidential") on each page of the document.

The English terms "unrestricted", "internal", "confidential" and "strictly confidential" are also permissible.

5 Dealing with information

Depending on the protection class of an item of information, Viega has different rules for handling it. A distinction is made between how this information must be used, printed, transmitted, stored and destroyed.

5.1 Protection class A (Strictly confidential)

General handling	Information classified as *strictly confidential is* for the use of designated persons. Care must be taken to ensure that this information is never left unlocked and unattended. Disclosure to external parties is only permitted with a valid Non-Disclosure Agreement (NDA). It is recommended to document the transfer.
Expression/Multiplication	Unattended printing and copying of *highly confidential* information is not permitted. Printouts, originals and copies must not remain in the printer after printing. The printer option "Confidential Printing" must be used.
Data transmission	If possible, postal delivery should be avoided. If there is no other possibility, make sure that a specific recipient is indicated and that the delivery is made by registered mail. For this purpose, the delivery instruction "registered mail, personal delivery" must be entered in the first address line. The recipient must ensure that the item arrives intact. Otherwise, the CISO of Viega must be notified. Electronic transmission is only permitted in encrypted form. Exceptions are to be approved by the CISO of Viega.
Storage	In order to protect *highly confidential* information, it may only be stored in locked offices, archives, safes or locked cabinets. Roll containers are not sufficiently secured and therefore not suitable for storing *highly confidential* information. If *strictly confidential* information is stored outside the Viega data centres, the data must be encrypted. In addition, access authorisation must be verified with single sign-on or multi-factor authentication.
Disposal	The disposal is done by shredding.
Destruction/Deletion	Destruction takes place via multiple overwriting or physical destruction of the data carrier.

5.2 Protection class B (Confidential)

General handling	*Confidential* classified information is intended for use within a defined group (department, specialist area, project team, etc.). The owner of the information decides whether it is to be passed on to external parties. Disclosure to external parties is only permitted with a valid non-disclosure agreement (NDA).
Expression/Multiplication	Unattended printing and copying of *confidential* information must be avoided. Printouts, originals and copies must not remain in the printer after printing. If possible, use the printer option "Confidential Printing".
Data transmission	When sending by post, it must be ensured that a specific recipient is indicated, and the delivery instruction "personal" must also be indicated in the first address line. The recipient must ensure that the consignment arrives undamaged. Otherwise, the CISO of Viega must be notified. Electronic transmission is only permitted in encrypted form. Exceptions are to be approved by the CISO of Viega.
Storage	*Confidential* information must be kept locked up after the end of work. Archiving must be done in a locked and secured room. If *confidential* information is stored outside the Viega data centres, the data must be encrypted. In addition, access authorisation must be verified with single sign-on or multi-factor authentication.
Disposal	The disposal is done by shredding.
Destruction/Deletion	Destruction is done by multiple overwriting.

For access to information in protection classes A (strictly confidential) and B (confidential), the "need-to-know" principle applies, i.e. the information owner must ensure that access to this information is authorised to the extent necessary for the performance of the work. It follows that information that can be viewed may be viewed. In case of doubt, the CISO of Viega must be informed.

5.3 Protection class C (internal)

General handling	*Internally* classified information is for use within the project group. Sharing with colleagues and external parties involved in projects is permitted.
Expression/Multiplication	Printing and copying of *internal* information is generally permitted. Printed documents and copies should be removed from the printers promptly.
Data transmission	No special security measures are prescribed for data transmission. However, encryption should be used where possible.
Storage	*Internal* information should be kept locked away at workplaces after the end of work. Storage may only take place on approved storage media, network drives and websites. If Class C personal information is stored outside the Viega data centres, the data should be encrypted. In addition, access authorisation must be verified with single sign-on or multi-factor authentication.
Disposal	Disposal may be done via the waste paper basket; shredding is recommended.
Destruction/Deletion	Destruction is done by simple deletion.

5.4 Protection class D (Unrestricted)

general handling	*Unrestricted* information is not subject to any restrictions in handling. It may and should be used and disseminated in compliance with the legal regulations.
Expression/Multiplication	Printing and copying of *unrestricted* information is generally permitted.
Data transmission	No special security measures are prescribed for data transmission.
Storage	There are no requirements for storage or warehousing.
Disposal	Disposal is via the wastepaper bin.
Destruction/Deletion	Destruction is done by (simple) deletion.

6 Release and return of data and information

Upon termination of the contractual relationship, all measures defined for this purpose in the contract shall be fulfilled. The contractor is responsible for the proper implementation and provides corresponding evidence for control.

The Contractor undertakes to surrender all data and information of Viega in the Contractor's possession after termination of the contractual relationship.

The Contractor shall ensure that all data handed over are treated securely and confidentially in the handover process and are only accessible to authorised personnel.

The Contractor undertakes to return all transferred data securely and definitively.

The return of the data includes the secure deletion or destruction of all electronic and physical data carriers on which the data are stored so that it is impossible to recover the data. The Client may also request the destruction of the data and information instead of the surrender/return.

The Contractor shall provide the Client with a written confirmation of the proper return of the data.

7 Sensitisation of employees

The Contractor shall ensure that all employees who come into contact with Viega data and information are informed about this Annex and have sufficient training in the handling of data and information per protection class.

8 Review of information security at the partner

The contractor agrees to grant the client access to its technical and organisational measures. This applies in particular to data and information of protection classes "A" and "B".

The Client reserves the right to conduct reviews of the Contractor's information security measures. These reviews shall ensure that the Contractor has taken appropriate technical, organisational and physical security measures to ensure the confidentiality, integrity and availability of the Client's data.

The controls may include, where necessary, aspects such as access control, encryption, data backup, incident response plans and staff training. The Contractor undertakes to provide all relevant information and documentation required to carry out these checks. These checks may be carried out at regular intervals or as required.

After each inspection, the Contractor shall submit a report to the Client on the results of the inspections. Should vulnerabilities be identified during the checks, the contractor undertakes to take appropriate measures to remedy these vulnerabilities and improve information security. The Client may set reasonable deadlines for the implementation of these measures and has the right to review the effectiveness of these measures again.
Both parties agree that all information disclosed during the information security controls will be kept confidential. Neither the Client nor the Contractor shall disclose or use any confidential information for any purpose other than the performance of the Controls without the prior written consent of the other party.