ARBONIA

IT SECURITY

Information Security Policy

Awareness Policy

Version:	1.0
Adopted:	2023-04-13
Status:	RELEASED
Classification:	RESTRICTED
Created by:	CISO
Adopted by:	Arbonia IT Board
Guideline:	IS-ISP-GROUP-006 -IT-SECURITY-AWARENESS-POLICY
Revision:	n/a

Policy information

Purpose	The Awareness Policy describes and defines the information security awareness program of the Arbonia Group.
User / recipient	All employees of the Arbonia Group
Electronic document storage	https://security.arbonia.com

Modification history

Version	Date	Status	Modification	by
0.1	10.01.2022	Draft	Draft of the policy	CISO
0.9	12.04.2022	Draft	Draft for adoption	CISO
0.9	13.04.2022	Review		Arbonia IT Board
1.0	13.04.2022	Adoption		Arbonia IT Board

Table of contents

Abbreviations

Term	Description
ICT	Information and Communications Technology
ISMS	Information Security Management System

Glossary

Term	Description
Information Security Management System	An information security management system is a list of procedures and rules within an organisation that serve to permanently define, manage, control, maintain, and continuously improve information security.

1 Purpose, scope of application, and users

The policy describes the requirements and specifications of the Arbonia Group's information security awareness program and defines them in a binding manner.

The policy applies to the entire scope of the Information Security Management System (ISMS), i.e. to all employees of the Arbonia Group, and serves to clarify the tasks and requirements of each individual employee in protecting the confidentiality, integrity and availability of information systems and data.

Users and recipients of this policy are all employees of the Arbonia Group.

2 Governance principles

2.1 Importance of the information security awareness program

Due to increasing networking, digitalization and the resulting technological change, potential attackers are also opening up further opportunities for cyber attacks. Information security is highly dynamic and affects almost every area of the Arbonia Group. The socio-technical aspect (interaction between people and information systems) can create vulnerabilities in this information network.

Since adequate information protection cannot be achieved by technical measures alone, but depends heavily on the behavior of employees and their handling of data and information systems, an information security awareness program with sensitization and recommendations for action regarding cyber threats is essential.

The goal is to create a steadily growing safety awareness among every employee of the Arbonia Group in accordance with the motto ***THINK BERFORE YOU Click.Post.Type*** and to measure this at regular intervals.

2.2 Duties of the employees

Participation in the information security awareness program is mandatory for all employees of the Arbonia Group and must be carried out accordingly in a conscientious and comprehensive manner. Accordingly, all parts of the training (training material and performance review) must be completed in each case.

2.3 Anonymity / Compliance

The implementation of the campaigns and the storage and evaluation of the statistical data are carried out in accordance with the country-specific legal standards. Agreements on data protection, if any, must be made in advance with the respective works councils.

Personal data processing is only carried out if the country-specific legal norm and/or the vote of the works council concerned permits this, whereby it can be stated that personal data processing offers greater added value, as employees can be provided with targeted support and training. If the legal norm or view is not given, anonymized collection and processing of the statistical data must be ensured. Anonymization is ensured by the software used for the phishing and awareness platform deployed. The recipient groups are to be subdivided according to the anonymization specifications.

2.4 New additions / departures (onboarding / offboarding) of companies and employees

New, acquired companies must be included in the next campaign from the time of closing. This also applies to all new employees. In addition, new employees must complete initial information security awareness training within 30 days. The responsible IT and HR departments must make appropriate arrangements for this. For employees of divested companies, participation is mandatory until the time of closing or until the end of the contractually agreed service. In any case, however, for as long as the client infrastructure remains within the scope of the Arbonia Group. Exceptions to this rule must be agreed with the IT managers and the CISO and the employees concerned must be informed.

3 Information Security Awareness Program

3.1 Definition

The awareness guideline supports the ISMS of the Arbonia Group by bindingly defining the requirements and specifications of the information security awareness program. With the recurring training and performance reviews, employees are informed about and sensitized to information security risks and threats and thus a constant information security awareness is to be generated among all employees. The information security awareness program basically consists of two parts (campaigns):

- Awareness campaign
- Phishing campaign

The campaigns are normally carried out quarterly, but at least three times a year. The phishing campaigns can be carried out 6-8 times a year, depending on the needs and requirements.

In addition, the information security awareness program includes the following measures:

- Poster campaigns
- Tools / Software (Outlook Phishing Button)
- Additional campaigns for exposed employees (HR, FI / CO, IT etc.)

- Additional campaigns for employees for whom additional training is required as a result of the training results

The results of each campaign are statistically processed and used to drive the information security awareness program.

3.2 Awareness campaigns

Awareness campaigns are conducted as defined and address current issues related to information security.

Awareness campaigns are conducted with a central phishing and awareness platform for all Arbonia Group companies and include the following:

- Determination of the awareness topic
- Updating the recipient lists (onboarding/offboarding)
- Campaign creation and configuration
- Tests and quality inspection
- Implementation
- Collection / preparation of statistical key figures

The invitation to the respective awareness campaign is sent directly to the employee via email. The invitation is personalized and may not be passed on to other employees. Normally, the awareness campaign consists of two parts, the training material and the performance review. In any case, all parts must be completed. Since participation in the awareness campaigns is mandatory for every employee, employees are reminded at least once during the course of the awareness campaign.

3.3 Phishing campaigns

The phishing campaigns are carried out according to definition and address simulated phishing attacks.

Phishing campaigns are conducted with a central phishing and awareness platform for all Arbonia Group companies and include the following:

- Definition of the phishing templates
- Updating the recipient lists (onboarding/offboarding)
- Campaign creation and configuration
- Tests and quality inspection
- Implementation
- Collection / preparation of statistical key figures

The simulated phishing attacks are sent directly to employees via email or other appropriate channels. A simulated phishing attack can take various forms. If an employee reacts incorrectly to a simulated phishing attack, he or she is automatically notified.

3.4 Roles and responsibilities

The Arbonia Group Information Security Team is responsible for defining, preparing, implementing and evaluating the Information Security Awareness Program. Changes with an impact on the entire program are discussed with the IT Board and addressed by the CISO.

The local HR teams are responsible for the timely communication of all personnel mutations (entry / exit / transfer) to the local IT team. The local IT teams thereby ensure the current database (employee master in the central Active Directory directory service). The recipient groups are updated by the Arbonia Group's information security team prior to each implementation based on the Active Directory group membership. The local IT team is also responsible for the onboarding (initial information security awareness training within 30 days) of new employees by notifying new employee hires via email to training@arbonia.com. The Arbonia Group Information Security Team invites new employees to initial awareness training after receiving this notification.

4 Accountability

As described in chapter 2.2, participation in the information security awareness program is mandatory for all Arbonia Group employees and must be carried out accordingly in a conscientious and fully comprehensive manner. In the event of repeated failures, additional training measures may be defined. In the event of fundamental non-compliance or insufficient participation, the responsible management reserves the right to take further measures.

5 Reference documents

- IS-ISS-GROUP-001-INFORMATION-SECURITY-STRATEGY
- IS-GISP-GROUP-001-GENERAL-INFORMATION-SECURITY-POLICY
- IS-ISP-GROUP-004-IT-SECURITY-POLICY

6 Effective date

Name	Business unit	Function	Date	Signature
Patrick Langenegger	Corporate IT	CIO Arbonia Group / CIO Division Doors	2021-04-13	n/a
Michael Kreter	Division HVAC	Head of IT Kermi Bereichleiter Informationsverarbeitung	2021-04-13	n/a
Reto Knechtle	Corporate IT	Head of IT Infrastructure	2021-04-13	n/a
Thomas Zehnder	Corporate IT	CISO	2021-04-13	n/a

7 Relevant enclosures

No.	Description	File name
1	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE