ARBONIA

IT SECURITY

Information Security Policy

Awareness Richtlinie

Version:	1.0
Verabschiedet:	13.04.2022
Status:	DRAFT
Klassifizierung:	RESTRICTED
Erstellt durch:	CISO
Verabschiedet durch:	Arbonia IT Board
Richtlinie:	IS-ISP-GROUP-006 -IT-SECURITY-AWARENESS-POLICY
Revision:	n/a

Richtlinieninformation

Zweck	Die Awareness Richtlinie beschreibt und definiert das Informationssicherheits-Awarenessprogramm der Arbonia Gruppe.
Anwender / Empfänger	Alle Mitarbeitenden der Arbonia Gruppe
Elektronische Dokumentenablage	https://security.arbonia.com

Änderungsnachweis

Version	Datum	Status	Änderung	Durch
0.1	10.01.2022	Draft	Entwurf der Richtlinie	ICT Security Specialist
0.9	12.04.2022	Draft	Entwurf zur Verabschiedung	CISO
0.9	13.04.2022	Review	Feedback Arbonia IT Board eingearbeitet	Arbonia IT Board
1.0	13.04.2022	Adoption		Arbonia IT Board

Inhaltsverzeichnis

Abkürzungsverzeichnis

Begriff	Beschreibung
ICT	Informations and Communications Technology (Informations- und Kommunikations-technik)
ISMS	Informationssicherheits-Managementsystems

Glossar

Begriff	Beschreibung
Informationssicher-heits-Management-system	Ein Informationssicherheits-Managementsystem ist die Aufstellung von Verfahren und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dau-erhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

1 Zweck, Anwendungsbereich und Anwender

Die Richtlinie beschreibt die Anforderungen und Vorgaben des Informationssicherheits-Awarenessprogrammes der Arbonia Gruppe und legt diese verbindlich fest.

Die Richtlinie gilt für den gesamten Anwendungsbereich des Informationssicherheits-Managementsystems (ISMS), d.h. für alle Mitarbeitende der Arbonia Gruppe und dient der Verdeutlichung der Aufgaben und Anforderungen jedes einzelnen Mitarbeiters beim Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen und Daten.

Anwender und Empfänger dieser Richtlinie sind alle Mitarbeitende der Arbonia Gruppe.

2 Governance Grundsätze

2.1 Wichtigkeit des Informationssicherheits-Awarenessprogrammes

Aufgrund der zunehmenden Vernetzung, Digitalisierung und des daraus abgeleiteten technologischen Wandels eröffnen sich auch potenziellen Angreifern weitere Möglichkeiten für Cyberangriffe. Die Informationssicherheit ist hochgradig dynamisch und betrifft nahezu jeden Bereich der Arbonia Gruppe. Durch den soziotechnischen Aspekt (Interaktion zwischen Mensch und Informationssystem) können Schwachstellen in diesem Informationsverbund entstehen.

Da ein angemessener Informationsschutz nicht nur durch technische Massnahmen erreicht werden kann, sondern stark vom Verhalten der Mitarbeitenden und deren Umgang mit Daten und Informationssystemen abhängt, ist ein Informationssicherheits-Awarenessprogramm mit Sensibilisierung und Handlungsempfehlungen zu Cyber-Bedrohungen essenziell.

Das Ziel ist es bei jedem Mitarbeitenden der Arbonia Gruppe ein stetig wachsendes Sicherheitsbewusstsein gemäss dem Motto ***THINK BERFORE YOU Click.Post.Type*** zu schaffen und dieses in regelmässigen Abständen zu messen.

2.2 Pflichten der Mitarbeitenden

Die Teilnahme an dem Informationssicherheits-Awarenessprogramm ist für alle Mitarbeitenden der Arbonia Gruppe verpflichtend und muss entsprechend gewissenhaft und vollumfassend erfolgen. Dementsprechend sind jeweils alle Teile der Schulung (Schulungsmaterial und Erfolgskontrolle) zu absolvieren.

2.3 Anonymität / Compliance

Die Durchführung der Kampagnen sowie die Speicherung und Auswertung der statistischen Daten erfolgt nach den Länderspezifischen Rechtsnormen. Absprachen zum Datenschutz müssen, falls vorhanden, mit den jeweiligen Betriebsräten im Vorfeld durchgeführt werden.

Eine personenbezogene Datenverarbeitung wird nur dann durchgeführt, wenn die länderspezifische Rechtsnorm und/oder die Abstimmung des betroffenen Betriebsrates dies zulässt, wobei festgehalten werden kann, dass eine personenbezogene Datenverarbeitung einen grösseren Mehrwert bietet, da die Mitarbeitenden gezielt unterstütz und geschult werden können. Ist die Rechtsnorm oder Ansicht nicht gegeben, muss eine anonymisierte Erfassung und Verarbeitung der statistischen Daten sichergestellt werden. Die Anonymisierung ist durch die verwendete Software für die eingesetzte Phishing und Awareness Plattform sichergestellt. Die Empfängergruppen sind entsprechend den Anonymisierungsvorgaben zu unterteilen.

2.4 Neuzugang / Ausscheiden (On-/Offboarding) von Gesellschaften und Mitarbeitenden

Neue, zugekaufte (akquirierte) Gesellschaften müssen ab dem Zeitpunkt des Closings für die nächste Kampagne mitberücksichtigt werden. Dies gilt ebenfalls für alle neueintretende Mitarbeitende. Zusätzlich müssen neue Mitarbeitende innerhalb von 30 Tagen ein initiales Inforationssicherheits-Awarenesstraining absolvieren. Hierzu müssen von der verantwortlichen IT und HR entsprechende Vorkehrungen getroffen werden. Für Mitarbeitende von veräusserten Gesellschaften ist die verbindliche Teilnahme bis zum Zeitpunkt des Closings oder bis zum Ende der vertraglich festgehaltenen Servicedienstleistung gegeben. In jedem Fall jedoch solange, wie die Client Infrastruktur im Anwendungsbereich der Arbonia Gruppe verbleibt. Ausnahmen zu dieser Regelung sind mit den IT Verantwortlichen und dem CISO abzusprechen und die betroffenen Mitarbeitenden sind zu informieren.

3 Informationssicherheits-Awarenessprogramm

3.1 Definition

Die Awareness Richtlinie unterstützt das ISMS der Arbonia Gruppe in dem diese Richtlinie die Anforderungen und Vorgaben des Informationssicherheits-Awarenessprogrammes verbindlich festlegt. Mit den wiederkehrenden Schulungen und Erfolgskontrollen werden die Mitarbeitenden über Informationssicherheits-Risiken und -Bedrohungen aufgeklärt und sensibilisiert und dadurch soll ein stetiges Informationssicherheitsbewusstsein bei allen Mitarbeitenden erzeugt werden. Das Informationssicherheits-Awarenessprogramm setzt sich grundsätzlich aus zwei Teilen (Kampagnen) zusammen:

- Awareness Kampagne
- Phishing Kampagne

Die Kampagnen werden im Normalfall quartalsweise, mindestens jedoch dreimal pro Jahr durchgeführt. Die Phishing Kampagnen können je nach Bedarf und Anforderungen 6-8 Mal pro Jahr durchgeführt werden.

Darüber hinaus umfasst das Informationssicherheits-Awarenessprogramm folgende Massnahmen:

- Poster-Kampagnen

- Tools / Software (Outlook Phishing-Button)
- Zusätzliche Kampagnen für exponierte Mitarbeitende (HR, FI / CO, IT u.w.)
- Zusätzliche Kampagnen für Mitarbeitende bei denen sich aufgrund der Trainingsergebnisse ein zusätzlicher Schulungsbedarf ergibt

Die Ergebnisse der einzelnen Kampagnen werden statistisch aufbereitet und zur Steuerung des Informationssicherheits-Awarenessprogrammes eingesetzt.

3.2 Awareness Kampagnen

Die Awareness Kampagnen werden gemäss Definition durchgeführt und adressieren aktuelle Themen im Zusammenhang mit der Informationssicherheit.

Die Awareness Kampagnen werden mit einer zentralen Phishing und Awareness Plattform für alle Gesellschaften der Arbonia Gruppe durchgeführt und umfassen folgende Punkte:

- Festlegung des Awareness Themas
- Aktualisierung der Empfängerlisten (On-/ Offboarding)
- Erstellung und Konfiguration der Kampagne
- Tests und Qualitätsprüfung
- Durchführung
- Erfassung / Aufbereitung statistischer Kennzahlen

Die Einladung zu der jeweiligen Awareness Kampagne erfolgt über Email direkt an die Mitarbeitende. Die Einladung ist personalisiert und darf nicht an andere Mitarbeitende weitergegeben werden. Im Normalfall setzt sich die Awareness Kampagne aus zwei Teilen, dem Schulungsmaterial und der Erfolgskontrolle, zusammen. In jedem Fall sind alle Teile zu absolvieren. Da die Teilnahme an den Awareness Kampagnen verbindlich für jeden Mitarbeitenden ist, werden die Mitarbeitenden im Verlauf der Awareness Kampagne mindestens einmal an die Teilnahme erinnert.

3.3 Phishing Kampagnen

Die Phishing Kampagnen werden gemäss Definition durchgeführt und adressieren simulierte Phishing-Angriffe.

Die Phishing Kampagnen werden mit einer zentralen Phishing und Awareness Plattform für alle Gesellschaften der Arbonia Gruppe durchgeführt und umfassen folgende Punkte:

- Festlegung der Phishing-Templates
- Aktualisierung der Empfängerlisten (On-/ Offboarding)
- Erstellung und Konfiguration der Kampagne
- Tests und Qualitätsprüfung
- Durchführung
- Erfassung / Aufbereitung statistischer Kennzahlen

Der Versand der simulierten Phishing-Angriffe erfolgt über Email oder andere geeignete Kanäle direkt an die Mitarbeitende. Ein simulierter Phishing-Angriff kann verschiedene Formen haben. Reagiert ein Mitarbeitender falsch auf einen simulierten Phishing Angriff, wird er automatisch darüber in Kenntnis gesetzt.

3.4 Rollen und Verantwortlichkeiten

Das Informationssicherheitsteam der Arbonia-Gruppe ist für die Definition, Vorbereitung, Durchführung und Auswertung des Informationssicherheits-Awarenessprogramm verantwortlich. Änderungen mit Auswirkung auf das gesamte Programm werden mit dem IT Board abgesprochen und durch den CISO adressiert.

Die lokalen HR Teams sind für die fristgerechte Kommunikation aller Personalmutationen (Eintritt / Austritt / Übertritt) an das lokale IT Team verantwortlich. Die lokalen IT Teams stellen dadurch die aktuelle Datenbasis (Mitarbeiterstamm im zentralen Verzeichnisdienst Active Directory) sicher. Die Empfängergruppen werden vor jeder Durchführung vom Informationssicherheitsteam der Arbonia-Gruppe anhand der Active Directory Gruppenzugehörigkeit aktualisiert. Das lokale IT Team ist ausserdem für das Onboarding (initiales Inforationssicherheits-Awarenesstraining innerhalb von 30 Tagen) von neuen Mitarbeitenden zuständig, indem sie Eintritte von neuen Mitarbeitenden per E-Mail an training@arbonia.com melden. Das Informationssicherheitsteam der Arbonia-Gruppe lädt neue Mitarbeitende nach Erhalt dieser Meldung zum initialen Awarenesstraining ein.

4 Rechenschaftspflicht

Wie im Kapitel 2.2 beschrieben, ist die Teilnahme an dem Informationssicherheits-Awarenessprogramm für alle Mitarbeitenden der Arbonia Gruppe verpflichtend und muss entsprechend gewissenhaft und vollumfassend erfolgen. Im Falle von wiederholten Misserfolgen können zusätzliche Schulungsmassnahmen definiert werden. Bei grundsätzlicher Nichteinhaltung bzw. ungenügender Teilnahme behält sich das zuständige Management weitere Massnahmen vor.

5 Referenzdokumente

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

6 Inkrafttreten

Name	Geschäftseinheit	Funktion	Datum	Unterschrift
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 Relevante Anhänge

Nr.	Beschreibung	Dateiname
1	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE