ARBONIA

IT SECURITY

Information Security Policy

Bewustzijnsbeleid

Versie:	1.0
Goedgekeurd:	13.04.2022
Status:	RELEASED
Classificatie:	RESTRICTED
Opgesteld door:	CISO
Goedgekeurd door:	Arbonia IT Board
Richtlijn:	IS-ISP-GROUP-006 -IT-SECURITY-AWARENESS-POLICY
Revisie:	n.v.t.

Informatiebeleid

Doel	Het bewustmakingsbeleid beschrijft en definieert het informatiebeveiligingsbewustmakingsprogramma van de Arbonia-groep.
Gebruikers/ontvangers	Alle werknemers van de Arbonia Groep
Elektronische documentarchivering	https://security.arbonia.com

Bewijs van wijziging

Versie	Datum	Status	Wijziging	door
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

Inhoudsopgave

Lijst van afkortingen

Begrip	Beschrijving
ICT	Informatie- en communicatietechnologie
ISMS	Systeem voor informatieveiligheidsbeheer

Verklarende woordenlijst

Begrip	Beschrijving
Information Security Management Systeem (informatiebeveiligingsbeheersysteem)	Een informatiebeveiligingmanagementsysteem is de combinatie van procedures en regels binnen een organisatie die dienen om de informatiebeveiliging permanent te definiëren, beheersen, bewaken, onderhouden en continu te verbeteren.

1 Doel, toepassingsgebied en gebruikers

Het beleid beschrijft de eisen en specificaties van het informatiebeveiligingsbewustmakingsprogramma van de Arbonia-groep en legt deze op bindende wijze vast.

Het beleid is van toepassing op het gehele bereik van het Information Security Management System (ISMS), d.w.z. op alle werknemers van de Arbonia-groep, en dient ter verduidelijking van de taken en vereisten van elke individuele werknemer bij de bescherming van de vertrouwelijkheid, integriteit en beschikbaarheid van informatiesystemen en gegevens.

Alle werknemers van de Arbonia-groep zijn gebruikers en ontvangers van dit beleid.

2 Governance-principes

2.1 Belang van het programma voor informatieveiligheidsbewustmaking

Door de toenemende netwerkvorming, digitalisering en de technologische veranderingen die daarvan het gevolg zijn, krijgen potentiële aanvallers ook meer mogelijkheden voor cyberaanvallen. Informatiebeveiliging is zeer dynamisch en raakt bijna elk gebied van de Arbonia-groep. Het sociaal-technische aspect (interactie tussen mensen en informatiesystemen) kan kwetsbaarheden in dit informatienetwerk creëren.

Aangezien adequate informatiebeveiliging niet kan worden bereikt met technische maatregelen alleen, maar sterk afhangt van het gedrag van werknemers en hun omgang met gegevens en informatiesystemen, is een bewustmakingsprogramma inzake informatiebeveiliging met bewustmaking en aanbevelingen voor maatregelen tegen cyberdreigingen van essentieel belang.

Het doel is een voortdurend groeiend veiligheidsbewustzijn bij elke werknemer van de Arbonia-groep te creëren volgens het motto ***THINK BERFORE YOU Click.Post.Type*** en dit op regelmatige tijdstippen te meten.

2.2 Taken van de werknemers

Deelname aan het bewustmakingsprogramma voor informatiebeveiliging is verplicht voor alle werknemers van de Arbonia-groep en moet dienovereenkomstig op consciëntieuze en volledige wijze worden uitgevoerd. Bijgevolg moeten alle onderdelen van de opleiding (opleidingsmateriaal en evaluatie van de prestaties) in elk geval worden voltooid.

2.3 Anonimiteit / Naleving

De uitvoering van de campagnes en de opslag en evaluatie van de statistische gegevens geschieden volgens de landenspecifieke wettelijke normen. Eventuele afspraken over gegevensbescherming moeten vooraf met de respectieve ondernemingsraden worden gemaakt.

De verwerking van persoonsgegevens vindt alleen plaats indien de landspecifieke wettelijke norm en/of de stemming van de betrokken ondernemingsraad dit toestaat, waarbij kan worden gesteld dat de verwerking van persoonsgegevens een grotere toegevoegde waarde biedt, omdat werknemers specifiek kunnen worden ondersteund en opgeleid. Indien de wettelijke norm of het standpunt niet wordt gegeven, moet worden gezorgd voor anoniem verzamelen en verwerken van statistische gegevens. Anonimisering wordt gewaarborgd door de software die voor het phishing- en bewustmakingsplatform wordt gebruikt. De groepen ontvangers moeten worden onderverdeeld naar gelang van de anonimiseringseisen.

2.4 Nieuwe toetredingen / uittredingen (onboarding / offboarding) van bedrijven en werknemers

Nieuwe, overgenomen bedrijven moeten in aanmerking worden genomen voor de volgende campagne vanaf het moment van afsluiting. Dit geldt ook voor alle nieuwe werknemers. Bovendien moeten nieuwe werknemers binnen 30 dagen een eerste bewustmakingsopleiding over informatiebeveiliging volgen. De verantwoordelijke IT- en HR-afdelingen moeten hiervoor passende voorzorgsmaatregelen treffen. Voor werknemers van afgestoten ondernemingen is deelneming verplicht tot het tijdstip van sluiting of tot het einde van de contractueel overeengekomen diensttijd. In elk geval echter zolang de infrastructuur van de klant binnen de werkingssfeer van de Arbonia-groep blijft. Uitzonderingen op deze regel moeten worden overeengekomen met de IT-managers en de CISO en de betrokken werknemers moeten op de hoogte worden gebracht.

3 Informatieveiligheidsbewustzijnsprogramma

3.1 Definitie

Het bewustmakingsbeleid ondersteunt het ISMS van de Arbonia-groep door het bindend vastleggen van de eisen en specificaties van het bewustmakingsprogramma voor informatiebeveiliging. Door middel van periodieke opleidingen en functioneringsgesprekken worden de werknemers geïnformeerd over en gesensibiliseerd voor risico's en bedreigingen voor de informatiebeveiliging, zodat alle werknemers zich voortdurend bewust zijn van de informatiebeveiliging. Het bewustmakingsprogramma voor informatiebeveiliging bestaat in wezen uit twee delen (campagnes):

- Bewustwordingscampagne
- Phishing campagne

De campagnes vinden normaal gesproken elk kwartaal plaats, maar ten minste drie keer per jaar. Phishing-campagnes kunnen 6-8 keer per jaar worden uitgevoerd, afhankelijk van de behoeften en vereisten.

Voorts omvat het bewustmakingsprogramma inzake informatiebeveiliging de volgende maatregelen:

- Poster campagnes
- Gereedschap / Software (Outlook Phishing Button)
- Aanvullende campagnes voor blootgestelde werknemers (HR, FI/CO, IT, enz.)
- Aanvullende campagnes voor werknemers die naar aanleiding van de opleidingsresultaten een aanvullende opleiding nodig hebben

De resultaten van de afzonderlijke campagnes worden statistisch verwerkt en gebruikt om het bewustmakingsprogramma inzake informatiebeveiliging bij te sturen.

3.2 Bewustmakingscampagnes

De bewustmakingscampagnes worden volgens een definitie uitgevoerd en behandelen actuele onderwerpen in verband met informatiebeveiliging.

De bewustmakingscampagnes worden uitgevoerd met een centraal phishing- en bewustmakingsplatform voor alle bedrijven van de Arbonia-groep en omvatten de volgende punten:

- Bepaling van het bewustmakingsthema
- Bijwerken van de ontvangerslijsten (onboarding/offboarding)
- Aanmaken en configureren van campagnes
- Tests en kwaliteitscontrole
- Uitvoering
- Verzamelen/voorbereiden van statistische kerncijfers

De uitnodiging voor de bewustmakingscampagne wordt via e-mail rechtstreeks naar de werknemers gestuurd. De uitnodiging is persoonlijk en mag niet worden doorgegeven aan andere werknemers. Normaliter bestaat de bewustmakingscampagne uit twee delen, het opleidingsmateriaal en de prestatiebeoordeling. In ieder geval moeten alle onderdelen worden ingevuld. Aangezien deelname aan de bewustmakingscampagnes voor iedere werknemer verplicht is, worden de werknemers er tijdens de bewustmakingscampagne ten minste eenmaal aan herinnerd.

3.3 Phishing-campagnes

De phishing-campagnes worden volgens de definitie uitgevoerd en zijn gericht op gesimuleerde phishing-aanvallen.

De phishing-campagnes worden uitgevoerd met een centraal phishing- en bewustmakingsplatform voor alle bedrijven van de Arbonia-groep en omvatten de volgende punten:

- Bepaling van de phishing-sjablonen
- Bijwerken van de ontvangerslijsten (onboarding/offboarding)
- Aanmaken en configureren van campagnes
- Tests en kwaliteitscontrole
- Uitvoering
- Verzamelen/voorbereiden van statistische kerncijfers

Gesimuleerde phishingaanvallen worden rechtstreeks naar de werknemers gestuurd via e-mail of andere geschikte kanalen. Een gesimuleerde phishing-aanval kan verschillende vormen aannemen. Als een werknemer verkeerd reageert op een gesimuleerde phishing-aanval, wordt hij of zij automatisch op de hoogte gebracht.

3.4 Rollen en verantwoordelijkheden

Het informatiebeveiligingsteam van de Arbonia-groep is verantwoordelijk voor het definiëren, voorbereiden, uitvoeren en evalueren van het bewustmakingsprogramma voor informatiebeveiliging. Wijzigingen met gevolgen voor het gehele programma worden besproken met de IT-raad en aangepakt door de CISO.

De plaatselijke HR-teams zijn verantwoordelijk voor het tijdig doorgeven van alle personeelsmutaties (indiensttreding/vertrek/overplaatsing) aan het plaatselijke IT-team. De lokale IT-teams zorgen daarbij voor het huidige gegevensbestand (employee master in de centrale Active Directory directory service). De ontvangende groepen worden vóór elke implementatie bijgewerkt door het informatiebeveiligingsteam van de Arbonia Group op basis van het lidmaatschap van de Active Directory-groepen. Het lokale IT-team is ook verantwoordelijk voor de onboarding (initiële informatiebeveiligingsbewustmakingstraining binnen 30 dagen) van nieuwe werknemers door de aanwerving van nieuwe werknemers per e-mail te melden op training@arbonia.com. Het informatiebeveiligingsteam van de Arbonia-groep nodigt nieuwe werknemers uit voor een eerste bewustmakingsopleiding na ontvangst van deze kennisgeving.

4 Verantwoordingsplicht

Zoals beschreven in hoofdstuk 2.2 is deelname aan het bewustmakingsprogramma voor informatiebeveiliging verplicht voor alle werknemers van de Arbonia-groep en moet dit programma op consciëntieuze en volledig omvattende wijze worden uitgevoerd. In geval van herhaalde mislukkingen kunnen aanvullende opleidingsmaatregelen worden vastgesteld. In geval van fundamentele niet-naleving of onvoldoende deelname behoudt de verantwoordelijke directie zich het recht voor verdere maatregelen te nemen.

5 Referentiedocumenten

- IS-ISS-GROEP-001-INFORMATIEVEILIGHEIDSSTRATEGIE
- IS-GISP-GROEP-001-ALGEMEEN INFORMATIEBEVEILIGINGSBELEID
- IS-ISP-GROEP-004-IT-SECURITY-POLICY

6 Inwerkingtreding

Naam	**Bedrijfseen-heid**	**Functie**	**Datum**	**Handtekening**
Patrick Langenegger	Corporate IT	CIO Arbonia Group / CIO Division Doors	2021-04-13	n/a
Michael Kreter	Division HVAC	Head of IT Kermi Bereichleiter Informa-tionsverarbeitung	2021-04-13	n/a
Reto Knechtle	Corporate IT	Head of IT Infrastruc-ture	2021-04-13	n/a
Thomas Zehnder	Corporate IT	CISO	2021-04-13	n/a

7 Relevante bijlagen

Nr.	**Beschrijving**	**Bestandsnaam**
1	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE