ARBONIA

IT SECURITY

Information Security Policy
Politique de sensibilisation

Version:	1.0
Votée:	13.04.2022
Statut:	RELEASED
Classification:	RESTRICTED
Auteur:	CISO
Votée par:	Arbonia IT Board
Directive:	IS-ISP-GROUP-006 -IT-SECURITY-AWARENESS-POLICY
Révision:	n/a

Informations relatives à la directive

Objectif	La directive Awareness décrit et définit le programme de sensibilisation à la sécurité de l'information du groupe Arbonia.
Utilisateurs/destinataires	Tous les collaborateurs du Groupe Arbonia
Enregistrement électronique des documents	https://security.arbonia.com

Justificatif de modification

Version	Date	Statut	Modification	par
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 des matières

Table des abréviations

Concept	Description
ICT	Informations and Communications Technology (Technologie de l'information et de la communication)
ISMS	Système de gestion de la sécurité de l'information

Glossaire

Concept	Description
Système de gestion de la sécurité des informations	Un système de gestion de la sécurité des informations consiste à établir des procédures et des règles au sein d'une organisation qui servent à définir, gérer, contrôler, maintenir et améliorer en permanence la sécurité des informations.

1 Objet, domaine d'application et utilisateurs

La directive décrit les exigences et les prescriptions du programme d'évaluation de la sécurité de l'information du groupe Arbonia et les rend obligatoires.

La directive s'applique à l'ensemble du champ d'application du système de gestion de la sécurité de l'information (ISMS), c'est-à-dire à tous les collaborateurs du Groupe Arbonia, et sert à clarifier les tâches et les exigences de chaque collaborateur en matière de protection de la confidentialité, de l'intégrité et de la disponibilité des systèmes d'information et des données.

Les utilisateurs et destinataires de cette directive sont tous les collaborateurs du groupe Arbonia.

2 Principes de gouvernance

2.1 Importance du programme de sensibilisation à la sécurité de l'information

En raison de la mise en réseau croissante, de la numérisation et de l'évolution technologique qui en découle, de nouvelles possibilités de cyber-attaques s'ouvrent également aux agresseurs potentiels. La sécurité de l'information est très dynamique et concerne presque tous les domaines du groupe Arbonia. En raison de l'aspect sociotechnique (interaction entre l'homme et le système d'information), des points faibles peuvent apparaître dans ce réseau d'information.

Étant donné qu'une protection adéquate de l'information ne peut pas être obtenue uniquement par des mesures techniques, mais dépend fortement du comportement des collaborateurs et de leur utilisation des données et des systèmes d'information, un programme de sensibilisation à la sécurité de l'information comprenant une sensibilisation et des recommandations d'action sur les cybermenaces est essentiel.

L'objectif est de créer chez chaque collaborateur du groupe Arbonia une conscience de la sécurité en constante augmentation selon la devise ***THINK BERFORE YOU Click.Post.Type*** et de la mesurer à intervalles réguliers.

2.2 Obligations des collaborateurs

La participation au programme de sensibilisation à la sécurité de l'information est obligatoire pour tous les collaborateurs du groupe Arbonia et doit donc être consciencieuse et complète. En conséquence, toutes les parties de la formation (matériel de formation et contrôle des résultats) doivent être suivies.

2.3 Anonymat / Conformité

La réalisation des campagnes ainsi que l'enregistrement et l'évaluation des données statistiques se font conformément aux normes juridiques spécifiques à chaque pays. Des accords sur la protection des données doivent être conclus au préalable avec les comités d'entreprise concernés, s'ils existent.

Un traitement de données à caractère personnel n'est effectué que si la norme juridique spécifique au pays et/ou l'accord du comité d'entreprise concerné l'autorisent, étant entendu qu'un traitement de données à caractère personnel offre une plus grande valeur ajoutée, car les collaborateurs peuvent être soutenus et formés de manière ciblée. Si la norme juridique ou l'avis n'est pas donné, il faut garantir une saisie et un traitement anonymisés des données statistiques. L'anonymisation est assurée par le logiciel utilisé pour la plateforme de phishing et de sensibilisation mise en place. Les groupes de destinataires doivent être subdivisés en fonction des exigences d'anonymisation.

2.4 Entrée / sortie (on/offboarding) de sociétés et de collaborateurs

Les nouvelles sociétés rachetées (acquises) doivent être prises en compte pour la prochaine campagne à partir de la date de clôture. Cela vaut également pour tous les nouveaux collaborateurs. En outre, les nouveaux collaborateurs doivent suivre une formation initiale de sensibilisation à la sécurité de l'information dans un délai de 30 jours. Les responsables IT et RH doivent prendre les dispositions nécessaires à cet effet. Pour les collaborateurs des sociétés vendues, la participation est obligatoire jusqu'au moment de la clôture ou jusqu'à la fin de la prestation de service prévue par le contrat. Dans tous les cas, tant que l'infrastructure client reste dans le domaine d'application du groupe Arbonia. Les exceptions à cette règle doivent être discutées avec les responsables informatiques et le CISO et les collaborateurs concernés doivent en être informés.

3 Programme de sensibilisation à la sécurité de l'information

3.1 Définition

La directive Awareness soutient l'ISMS du groupe Arbonia dans la mesure où cette directive fixe de manière contraignante les exigences et les prescriptions du programme de sensibilisation à la sécurité de l'information. Les formations récurrentes et les contrôles d'efficacité permettent d'informer et de sensibiliser les collaborateurs aux risques et aux menaces en matière de sécurité de l'information et de générer ainsi une prise de conscience constante de la sécurité de l'information chez tous les collaborateurs. Le programme de sensibilisation à la sécurité de l'information se compose en principe de deux parties (campagnes) :

- Campagne de sensibilisation
- Campagne d'hameçonnage

Les campagnes sont normalement menées tous les trimestres, mais au moins trois fois par an. Les campagnes de phishing peuvent être menées 6 à 8 fois par an, selon les besoins et les exigences.

En outre, le programme de sensibilisation à la sécurité de l'information comprend les mesures suivantes :

- Campagnes d'affichage
- Outils / logiciels (bouton d'hameçonnage Outlook)
- Campagnes supplémentaires pour les collaborateurs exposés (RH, FI / CO, IT, etc.)
- Campagnes supplémentaires pour les collaborateurs qui ont besoin d'une formation supplémentaire sur la base des résultats de la formation.

Les résultats des différentes campagnes sont traités statistiquement et utilisés pour piloter le programme de sensibilisation à la sécurité de l'information.

3.2 Campagnes de sensibilisation

Les campagnes de sensibilisation sont menées conformément à la définition et abordent des thèmes actuels en rapport avec la sécurité de l'information.

Les campagnes de sensibilisation sont menées avec une plate-forme centrale de phishing et de sensibilisation pour toutes les sociétés du groupe Arbonia et comprennent les points suivants :

- Définition du thème de la sensibilisation
- Mise à jour des listes de destinataires (onboarding/offboarding)
- Création et configuration de la campagne
- Tests et contrôle de qualité
- Mise en œuvre
- Saisie / préparation de ratios statistiques

L'invitation à la campagne de sensibilisation est envoyée par e-mail directement aux collaborateurs. L'invitation est personnalisée et ne doit pas être transmise à d'autres collaborateurs. En règle générale, la campagne de sensibilisation se compose de deux parties : le matériel de formation et le contrôle des résultats. Dans tous les cas, toutes les parties doivent être suivies. Comme la participation aux campagnes de sensibilisation est obligatoire pour chaque collaborateur, les collaborateurs sont rappelés au moins une fois au cours de la campagne de sensibilisation.

3.3 Campagnes d'hameçonnage

Les campagnes de phishing sont menées conformément à la définition et s'adressent à des attaques de phishing simulées.

Les campagnes de phishing sont menées avec une plate-forme centrale de phishing et de sensibilisation pour toutes les sociétés du groupe Arbonia et comprennent les points suivants :

- Définition des modèles d'hameçonnage
- Mise à jour des listes de destinataires (onboarding/offboarding)
- Création et configuration de la campagne
- Tests et contrôle de qualité
- Mise en œuvre
- Saisie / préparation de ratios statistiques

L'envoi des attaques de phishing simulées se fait par e-mail ou par d'autres canaux appropriés directement aux collaborateurs. Une attaque de phishing simulée peut prendre différentes formes. Si un collaborateur réagit mal à une attaque de phishing simulée, il en est automatiquement informé.

3.4 Rôles et responsabilités

L'équipe de sécurité de l'information du Groupe Arbonia est responsable de la définition, de la préparation, de la mise en œuvre et de l'évaluation du programme d'évaluation de la sécurité de l'information. Les changements ayant un impact sur l'ensemble du programme sont discutés avec l'IT Board et adressés par le CISO.

Les équipes RH locales sont responsables de la communication dans les délais de toutes les mutations de personnel (entrée / sortie / transfert) à l'équipe informatique locale. Les équipes IT locales garantissent ainsi la base de données actuelle (base des collaborateurs dans le service d'annuaire central Active Directory). Les groupes de destinataires sont mis à jour avant chaque exécution par l'équipe de sécurité de l'information du groupe Arbonia sur la base de l'appartenance à un groupe Active Directory. L'équipe informatique locale est en outre responsable de l'onboarding (formation initiale de sensibilisation à la sécurité de l'information dans un délai de 30 jours) des nouveaux collaborateurs, en signalant les entrées de nouveaux collaborateurs par e-mail à training@arbonia.com. L'équipe de sécurité de l'information du groupe Arbonia invite les nouveaux collaborateurs à la formation initiale de sensibilisation après réception de cette annonce.

4 Responsabilité

Comme décrit au chapitre 2.2, la participation au programme de sensibilisation à la sécurité de l'information est obligatoire pour tous les collaborateurs du Groupe Arbonia et doit donc être consciencieuse et complète. En cas d'échecs répétés, des mesures de formation supplémentaires peuvent être définies. En cas de non-respect fondamental ou de participation insuffisante, la direction compétente se réserve le droit de prendre d'autres mesures.

5 Documents de référence

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

6 Entrée en vigueur

Nom	Unité	Fonction	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 Informations-verarbeitung	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 Annexes pertinentes

N°	Description	Nom du fichier
1	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE