ARBONIA

IT SECURITY

Information Security Policy
Política de Sensibilização

Versão:	1.0
Aprovado:	13.04.2022
Estado:	RELEASED
Classificação:	RESTRICTED
Elaborado por:	CISO
Aprovado por:	Arbonia IT Board
Política:	IS-ISP-GROUP-006 -IT-SECURITY-AWARENESS-POLICY
Revisão:	n/a

Informações sobre a política

Finalidade	A Política de Sensibilização descreve e define o programa de sensibilização para a segurança da informação do Grupo Arbonia.	A política d gestão e uti
Utilizador/destinatário	Todos os empregados do Grupo Arbonia	▪ Toc ▪ For par Arb
Armazenamento eletrónico de documentos	https://security.arbonia.com	https:\\secu

Histórico de alterações

Versão	Data	Estado	Alteração	por
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

Índice

Lista de abreviaturas

Termo	Descrição
ICT	Tecnologias de Informação e Comunicação
ISMS	Sistema de Gestão de Segurança da Informação

Glossário

Termo	Descrição
Sistemas de Gestão de Segurança da Informação	Um sistema de gestão de segurança da informação pressupõe o estabelecimento de procedimentos e regras dentro de uma organização, que servem para definir, gerir, controlar, manter e melhorar continuamente a segurança da informação.

1 Finalidade, âmbito de aplicação e utilizador

A política descreve os requisitos e especificações do programa de sensibilização do Grupo Arbonia para a segurança da informação e define-os de uma forma vinculativa.

A política aplica-se a todo o âmbito do Sistema de Gestão da Segurança da Informação (SGSI), ou seja, a todos os empregados do Grupo Arbonia, e serve para clarificar as tarefas e requisitos de cada empregado individual na protecção da confidencialidade, integridade e disponibilidade dos sistemas e dados de informação.

Todos os empregados do Grupo Arbonia são utilizadores e destinatários desta política.

2 Princípios de governança

2.1 Importância do Programa de Sensibilização para a Segurança da Informação

Devido à crescente ligação em rede, digitalização e à mudança tecnológica daí decorrente, os potenciais atacantes estão também a abrir mais oportunidades para ataques cibernéticos. A segurança da informação é altamente dinâmica e afecta quase todas as áreas do Grupo Arbonia. O aspecto sócio-técnico (interacção entre pessoas e sistemas de informação) pode criar vulnerabilidades nesta rede de informação.

Uma vez que a protecção adequada da informação não pode ser alcançada apenas através de medidas técnicas, mas depende muito do comportamento dos empregados e do seu tratamento dos dados e sistemas de informação, é essencial um programa de sensibilização para a segurança da informação com sensibilização e recomendações de acção sobre ameaças cibernéticas.

O objectivo é criar uma consciência de segurança em constante crescimento entre cada empregado do Grupo Arbonia, de acordo com o lema ***THINK BERFORE YOU Click.Post.Type*** e medir isto a intervalos regulares.

2.2 Deveres dos empregados

A participação no programa de sensibilização para a segurança da informação é obrigatória para todos os empregados do Grupo Arbonia e deve ser levada a cabo de forma consciente e abrangente. Consequentemente, todas as partes da formação (material de formação e análise de desempenho) devem ser completadas em cada caso.

2.3 Anonimato / Cumprimento

A implementação das campanhas, bem como o armazenamento e avaliação dos dados estatísticos, é realizada de acordo com as normas legais específicas do país. Os acordos sobre protecção de dados, se existirem, devem ser feitos previamente com os respectivos conselhos de empresa.

O tratamento de dados pessoais só é efectuado se a norma legal específica do país e/ou o voto do conselho de empresa em causa o permitir, podendo-se afirmar que o tratamento de dados pessoais oferece um maior valor acrescentado, uma vez que os trabalhadores podem ser especificamente apoiados e formados. Se a norma ou visão legal não for dada, deve ser assegurada a recolha e tratamento anónimo de dados estatísticos. A anonimização é assegurada pelo software utilizado para a plataforma de phishing e sensibilização. Os grupos beneficiários devem ser subdivididos de acordo com os requisitos de anonimização.

2.4 Novas adições / saídas (onboarding / offboarding) de empresas e empregados

As empresas novas e adquiridas devem ser tidas em conta na próxima campanha a partir do momento do encerramento. Isto também se aplica a todos os novos empregados. Além disso, os novos funcionários devem completar uma formação inicial de sensibilização para a segurança da informação no prazo de 30 dias. Os departamentos responsáveis de TI e RH devem tomar as precauções adequadas para o efeito. Para empregados de empresas alienadas, a participação é obrigatória até ao momento do encerramento ou até ao fim do serviço contratualmente acordado. Em qualquer caso, no entanto, enquanto a infra-estrutura do cliente permanecer no âmbito do Grupo Arbonia. As excepções a esta regra devem ser acordadas com os gestores de TI e a CISO e os funcionários envolvidos devem ser informados.

3 Programa de Sensibilização para a Segurança da Informação

3.1 Definição

A política de sensibilização apoia o SGSI do Grupo Arbonia ao definir de forma vinculativa os requisitos e especificações do programa de sensibilização para a segurança da informação. Com os cursos de formação e revisões de desempenho recorrentes, os funcionários são informados e sensibilizados para os riscos e ameaças à segurança da informação e, assim, é gerada uma consciência constante da segurança da informação entre todos os funcionários. O programa de sensibilização para a segurança da informação é composto basicamente por duas partes (campanhas):

- Campanha de Sensibilização
- Campanha de Phishing

As campanhas são normalmente realizadas trimestralmente, mas pelo menos três vezes por ano. As campanhas de phishing podem ser levadas a cabo 6-8 vezes por ano, dependendo das necessidades e exigências.

Além disso, o programa de sensibilização para a segurança da informação inclui as seguintes medidas:

- Campanhas de cartazes

- Ferramentas / Software (Botão Phishing do Outlook)
- Campanhas adicionais para funcionários expostos (RH, FI / CO, IT, etc.)
- Campanhas adicionais para funcionários que necessitam de formação adicional em resultado dos resultados da formação

Os resultados das campanhas individuais são processados estatisticamente e utilizados para orientar o programa de sensibilização para a segurança da informação.

3.2 Campanhas de sensibilização

As campanhas de sensibilização são realizadas de acordo com a definição e abordam temas actuais relacionados com a segurança da informação.

As campanhas de sensibilização são realizadas com uma plataforma central de phishing e sensibilização para todas as empresas do Grupo Arbonia e incluem os seguintes pontos:

- Determinação do tema da sensibilização
- Actualização das listas de destinatários (onboarding/offboarding)
- Criação e configuração da campanha
- Testes e inspecção de qualidade
- Implementação
- Recolha / preparação de números-chave estatísticos

O convite para a respectiva campanha de sensibilização é enviado directamente para os funcionários através de correio electrónico. O convite é personalizado e não pode ser transmitido a outros empregados. Normalmente, a campanha de sensibilização é constituída por duas partes, o material de formação e a revisão do desempenho. Em qualquer caso, todas as peças devem ser preenchidas. Como a participação nas campanhas de sensibilização é obrigatória para cada empregado, os empregados são lembrados pelo menos uma vez durante a campanha de sensibilização.

3.3 Campanhas de Phishing

As campanhas de phishing são levadas a cabo de acordo com a definição e abordam ataques simulados de phishing.

As campanhas de phishing são realizadas com uma plataforma central de phishing e sensibilização para todas as empresas do Grupo Arbonia e incluem os seguintes pontos:

- Determinação dos modelos de phishing
- Actualização das listas de destinatários (onboarding/offboarding)
- Criação e configuração da campanha
- Testes e inspecção de qualidade
- Implementação

- Recolha / preparação de números-chave estatísticos

Os ataques simulados de phishing são enviados directamente aos empregados através de correio electrónico ou outros canais apropriados. Um ataque de phishing simulado pode assumir várias formas. Se um empregado reagir incorrectamente a um ataque de phishing simulado, ele ou ela é automaticamente notificado.

3.4 Papéis e responsabilidades

A equipa de segurança da informação do Grupo Arbonia é responsável pela definição, preparação, implementação e avaliação do programa de sensibilização para a segurança da informação. As alterações com impacto em todo o programa são discutidas com o Conselho TI e abordadas pela CISO.

As equipas locais de RH são responsáveis pela comunicação atempada de todas as mudanças de pessoal (entrada / saída / transferência) para a equipa local de TI. As equipas informáticas locais asseguram assim a base de dados actual (mestre de empregados no serviço central de directório activo). Os grupos destinatários são actualizados pela equipa de segurança da informação do Grupo Arbonia antes de cada implementação, com base nos membros do grupo Active Directory. A equipa local de TI é também responsável pela formação inicial de sensibilização para a segurança da informação no prazo de 30 dias) dos novos empregados, notificando as novas contratações de empregados através de e-mail para training@arbonia.com. A equipa de segurança da informação do Grupo Arbonia convida novos funcionários para uma formação inicial de sensibilização após receberem esta notificação.

4 Prestação de contas

Conforme descrito no capítulo 2.2, a participação no programa de sensibilização para a segurança da informação é obrigatória para todos os trabalhadores do Grupo Arbonia e deve ser levada a cabo de forma consciente e totalmente abrangente. Em caso de falhas repetidas, podem ser definidas medidas de formação adicionais. Em caso de incumprimento fundamental ou de participação insuficiente, a direcção responsável reserva-se o direito de tomar outras medidas.

5 Documentos de referência

- IS-ISS-GROUP-001-ESTRATÉGIA DE INFORMAÇÃO-SEGURANÇA
- IS-GISP-GROUP-001-GENERAL-INFORMATION-SECURITY-POLICY
- IS-ISP-GROUP-004-IT-SECURITY-POLICY

6 Entrada em vigor

Nome	Unidade de negócios	Cargo	Data	Assinatura
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 Anexos relevantes

N.º	Descrição	Nome do ficheiro
1	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE