ARBONIA
IT SECURITY

Politika bezpečnosti informací
Směrnice k zvyšování povědomí

Verze:	1.0
Schválena:	13.04.2022
Stav:	RELEASED
Klasifikace:	RESTRICTED
Zpracoval:	CISO
Schválena kým:	Arbonia IT Board
Směrnice:	IS-ISP-GROUP-006 -IT-SECURITY-AWARENESS-POLICY
Revize:	n/a

Informace ke směrnici

Účel	Politika informovanosti popisuje a definuje program skupiny Arbonia pro zvyšování povědomí o bezpečnosti informací.
Uživatel / příjemce	Všichni zaměstnanci skupiny Arbonia
Elektronická dokumentace	https://security.arbonia.com

Doklad o změně

Verze	Datum	Stav	Změna	provedena kým
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

Obsah

Seznam zkratek

Pojem	Popis
ICT	Informační a komunikační technologie
ISMS	Systém řízení bezpečnosti informací

Glosář

Pojem	Popis
Systém řízení bezpečnosti informací	Systém řízení bezpečnosti informací je vytvoření postupů a pravidel v rámci organizace, které slouží k trvalému definování, řízení, kontrole, udržování a neustálému zlepšování bezpečnosti informací.

1 Účel, rozsah použití a uživatelé

Politika popisuje požadavky a specifikace programu skupiny Arbonia pro zvyšování povědomí o bezpečnosti informací a závazně je definuje.

Tato politika se vztahuje na celý rozsah systému řízení bezpečnosti informací (ISMS), tj. na všechny zaměstnance skupiny Arbonia, a slouží k objasnění úkolů a požadavků jednotlivých zaměstnanců při ochraně důvěrnosti, integrity a dostupnosti informačních systémů a dat.

Uživateli a příjemci těchto zásad jsou všichni zaměstnanci skupiny Arbonia.

2 Zásady governance

2.1 Význam programu zvyšování povědomí o bezpečnosti informací

Vzhledem k rostoucímu propojení, digitalizaci a z toho vyplývajícím technologickým změnám se potenciálním útočníkům otevírají další možnosti kybernetických útoků. Bezpečnost informací je velmi dynamická a ovlivňuje téměř všechny oblasti skupiny Arbonia. Sociálně-technický aspekt (interakce mezi lidmi a informačními systémy) může v této informační síti vytvářet zranitelná místa.

Vzhledem k tomu, že odpovídající ochrany informací nelze dosáhnout pouze technickými opatřeními, ale do značné míry závisí na chování zaměstnanců a jejich zacházení s daty a informačními systémy, je nezbytný program zvyšování povědomí o informační bezpečnosti s osvětou a doporučeními pro opatření v oblasti kybernetických hrozeb.

Cílem je vytvářet neustále rostoucí povědomí o bezpečnosti u každého zaměstnance skupiny Arbonia v souladu s heslem ***THINK BERFORE YOU Click.Post.Type*** a v pravidelných intervalech to měřit.

2.2 Povinnosti zaměstnanců

Účast na programu zvyšování povědomí o bezpečnosti informací je povinná pro všechny zaměstnance skupiny Arbonia a musí být prováděna svědomitě a komplexně. V každém případě je proto nutné dokončit všechny části školení (školicí materiály a hodnocení výkonu).

2.3 Anonymita / dodržování předpisů

Provádění kampaní, jakož i uchovávání a vyhodnocování statistických údajů se provádí v souladu s právními normami platnými v dané zemi. Případné dohody o ochraně údajů musí být předem uzavřeny s příslušnými podnikovými radami.

Zpracování osobních údajů se provádí pouze tehdy, pokud to povoluje právní norma platná v dané zemi a/nebo hlasování příslušné podnikové rady, přičemž lze konstatovat, že zpracování osobních údajů přináší vyšší přidanou hodnotu, neboť zaměstnanci mohou být speciálně podporováni a školeni. Pokud není dána právní norma nebo stanovisko, musí být zajištěn anonymizovaný sběr a zpracování statistických údajů. Anonymizaci zajišťuje software používaný pro platformu pro phishing a informovanost. Skupiny příjemců musí být rozděleny podle požadavků na anonymizaci.

2.4 Nové příchody / odchody (nástupy / výstupy) společností a zaměstnanců

Nové, získané společnosti je třeba zohlednit v další kampani od okamžiku uzavření. To platí i pro všechny nové zaměstnance. Kromě toho musí noví zaměstnanci do 30 dnů absolvovat úvodní školení o bezpečnosti informací. Odpovědná oddělení IT a lidských zdrojů musí přijmout příslušná opatření. Pro zaměstnance odprodávaných společností je účast povinná až do okamžiku uzavření nebo do konce smluvně sjednané služby. V každém případě však po dobu, kdy infrastruktura klienta zůstává v působnosti skupiny Arbonia. Výjimky z tohoto pravidla musí být dohodnuty s vedoucími IT a ředitelem CISO a dotyční zaměstnanci o nich musí být informováni.

3 Program zvyšování povědomí o bezpečnosti informací

3.1 Definice

Politika zvyšování povědomí podporuje ISMS skupiny Arbonia tím, že závazně definuje požadavky a specifikace programu zvyšování povědomí o bezpečnosti informací. Díky opakovaným školením a hodnocením výkonnosti jsou zaměstnanci informováni o rizicích a hrozbách v oblasti bezpečnosti informací a jsou na ně upozorňováni, čímž se u všech zaměstnanců vytváří trvalé povědomí o bezpečnosti informací. Program zvyšování povědomí o bezpečnosti informací se v zásadě skládá ze dvou částí (kampaní):

- Osvětová kampaň
- Phishingová kampaň

Kampaně se obvykle provádějí čtvrtletně, nejméně však třikrát ročně. Phishingové kampaně lze provádět 6-8krát ročně v závislosti na potřebách a požadavcích.

Program zvyšování povědomí o bezpečnosti informací navíc zahrnuje následující opatření:

- Plakátové kampaně
- Nástroje / Software (Outlook Phishing Button)
- Další kampaně pro exponované zaměstnance (HR, FI / CO, IT atd.)
- Další kampaně pro zaměstnance, kteří na základě výsledků školení potřebují další školení.

Výsledky jednotlivých kampaní jsou statisticky zpracovávány a využívány k řízení programu zvyšování povědomí o bezpečnosti informací.

3.2 Informační kampaně

Osvětové kampaně probíhají podle definice a zabývají se aktuálními tématy souvisejícími s bezpečností informací.

Osvětové kampaně jsou prováděny pomocí centrální platformy pro phishing a osvětu pro všechny společnosti skupiny Arbonia a zahrnují následující body:

- Určení tématu povědomí
- Aktualizace seznamů příjemců (onboarding/offboarding)
- Vytvoření a konfigurace kampaně
- Testy a kontrola kvality
- Provádění
- Shromažďování / příprava klíčových statistických údajů

Pozvánka na příslušnou informační kampaň je zasílána přímo zaměstnancům e-mailem. Pozvánka je osobní a nesmí být předána dalším zaměstnancům. Obvykle se informační kampaň skládá ze dvou částí, a to ze školicího materiálu a z hodnocení výkonu. V každém případě je nutné vyplnit všechny části. Protože účast na osvětových kampaních je pro každého zaměstnance povinná, jsou zaměstnanci během osvětové kampaně alespoň jednou připomenuty.

3.3 Phishingové kampaně

Phishingové kampaně jsou prováděny podle definice a řeší simulované phishingové útoky.

Phishingové kampaně jsou prováděny pomocí centrální platformy pro phishing a zvyšování povědomí pro všechny společnosti skupiny Arbonia a zahrnují následující body:

- Určení šablon phishingu
- Aktualizace seznamů příjemců (onboarding/offboarding)
- Vytvoření a konfigurace kampaně
- Testy a kontrola kvality
- Provádění
- Shromažďování / příprava klíčových statistických údajů

Simulované phishingové útoky jsou zasílány přímo zaměstnancům prostřednictvím e-mailu nebo jiných vhodných kanálů. Simulovaný phishingový útok může mít různé podoby. Pokud zaměstnanec na simulovaný phishingový útok zareaguje nesprávně, je automaticky upozorněn.

3.4 Role a odpovědnosti

Tým pro bezpečnost informací skupiny Arbonia je odpovědný za definování, přípravu, provádění a vyhodnocování programu zvyšování povědomí o bezpečnosti informací. Změny s dopadem na celý program jsou projednávány s radou pro IT a řešeny ředitelem CISO.

Místní týmy lidských zdrojů jsou odpovědné za včasné oznamování všech změn zaměstnanců (nástup/výstup/přeložení) místnímu týmu IT. Místní týmy IT tak zajišťují aktuální databázi (master zaměstnanců v centrální adresářové službě Active Directory). Skupiny příjemců jsou před každou implementací aktualizovány týmem zabezpečení informací skupiny Arbonia Group na základě členství ve skupinách služby Active Directory. Místní tým IT je také zodpovědný za onboarding (úvodní školení o povědomí o bezpečnosti informací do 30 dnů) nových zaměstnanců, a to oznámením nově přijatých zaměstnanců prostřednictvím e-mailu na adresu training@arbonia.com. Tým informační bezpečnosti skupiny Arbonia Group po obdržení tohoto oznámení pozve nové zaměstnance na úvodní školení.

4 Odpovědnost

Jak je popsáno v kapitole 2.2, účast v programu zvyšování povědomí o bezpečnosti informací je povinná pro všechny zaměstnance skupiny Arbonia a musí být prováděna svědomitě a zcela komplexně. V případě opakovaných selhání mohou být stanovena další tréninková opatření. V případě zásadního nedodržení nebo nedostatečné účasti si odpovědné vedení vyhrazuje právo přijmout další opatření.

5 Referenční dokumenty

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

6 Nabytí platnosti

Jméno	Obchodní jednotka	Funkce	Datum	Podpis
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 Důležité přílohy

Č.	Popis	Název souboru
1	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE