ARBONIA

IT SECURITY

Polityka bezpieczeństwa informacji

Polityka świadomości

Wersja:	1.0
Przyjęto dnia:	13.04.2022
Status:	RELEASED
Klasyfikacja:	RESTRICTED
Utworzył:	ICT Security Officer
Przyjęte przez:	Arbonia IT Board
Wytyczna:	IS-ISP-GROUP-006 -IT-SECURITY-AWARENESS-POLICY
Rewizja:	n/a

Informacje dotyczące wytycznych

Przeznaczenie	Polityka świadomości opisuje i definiuje program świadomości bezpieczeństwa informacji w Arbonia Group.
Użytkownik/odbiorca	Wszyscy pracownicy Grupy Arbonia
Elektroniczne przechowywanie dokumentów	https://security.arbonia.com

Dowód zmiany

Wersja	Data	Status	Zmiana	przez
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

Spis treści

Wykaz skrótów

Pojęcie	Opis
ICT	Technologie informacyjne i komunikacyjne
ISMS	System zarządzania bezpieczeństwem informacji

Glosariusz

Pojęcie	Opis
System zarządzania bezpieczeństwem informacji	System zarządzania bezpieczeństwem informacji to ustanowienie procedur i zasad w organizacji, które służą do stałego definiowania, kontrolowania, monitorowania, utrzymywania i ciągłego doskonalenia bezpieczeństwa informacji.

1 Cel, zakres zastosowania i użytkownik

Polityka opisuje wymagania i specyfikacje programu świadomości bezpieczeństwa informacji Grupy Arbonia oraz definiuje je w sposób wiążący.

Polityka ma zastosowanie do całego zakresu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), tj. do wszystkich pracowników Grupy Arbonia, i służy wyjaśnieniu zadań i wymagań każdego pracownika w zakresie ochrony poufności, integralności i dostępności systemów informacyjnych i danych.

Użytkownikami i odbiorcami niniejszej polityki są wszyscy pracownicy Arbonia Group.

2 Zasady zarządzania

2.1 Znaczenie programu podnoszenia świadomości w zakresie bezpieczeństwa informacji

Ze względu na coraz większe powiązania sieciowe, cyfryzację i wynikające z niej zmiany technologiczne, potencjalni napastnicy stwarzają sobie coraz więcej okazji do cyberataków. Bezpieczeństwo informacji jest bardzo dynamiczne i dotyczy niemal każdego obszaru działalności Grupy Arbonia. Aspekt socjotechniczny (interakcje między ludźmi a systemami informacyjnymi) może być przyczyną słabych punktów w tej sieci informacyjnej.

Ponieważ odpowiedniej ochrony informacji nie da się osiągnąć wyłącznie za pomocą środków technicznych, ale w dużej mierze zależy ona od zachowania pracowników i sposobu, w jaki obchodzą się oni z danymi i systemami informatycznymi, zasadnicze znaczenie ma program podnoszenia świadomości w zakresie bezpieczeństwa informacji, obejmujący uwrażliwianie na zagrożenia cybernetyczne i zalecenia dotyczące działań w tym zakresie.

Celem jest stworzenie stale rosnącej świadomości bezpieczeństwa wśród każdego pracownika Arbonia Group zgodnie z mottem ***THINK BERFORE YOU Click.Post.Type*** oraz regularne mierzenie tego stanu rzeczy.

2.2 Obowiązki pracowników

Udział w programie podnoszenia świadomości w zakresie bezpieczeństwa informacji jest obowiązkowy dla wszystkich pracowników Grupy Arbonia i musi być realizowany w sposób sumienny i kompleksowy. W związku z tym w każdym przypadku należy zrealizować wszystkie części szkolenia (materiały szkoleniowe i ocena wyników).

2.3 Anonimowość / Zgodność

Realizacja kampanii, a także przechowywanie i ocena danych statystycznych odbywa się zgodnie z normami prawnymi obowiązującymi w danym kraju. Ewentualne porozumienia w sprawie ochrony danych należy zawczasu zawrzeć z odpowiednimi radami zakładowymi.

Przetwarzanie danych osobowych odbywa się tylko wtedy, gdy zezwalają na to normy prawne danego kraju i/lub głosowanie danej rady zakładowej, przy czym można stwierdzić, że przetwarzanie danych osobowych oferuje większą wartość dodaną, ponieważ pracownicy mogą być specjalnie wspierani i szkoleni. Jeśli norma prawna lub pogląd nie są podane, należy zapewnić anonimowe gromadzenie i przetwarzanie danych statystycznych. Anonimowość jest zapewniana przez oprogramowanie wykorzystywane do obsługi platformy phishingowej i świadomościowej. Grupy odbiorców muszą być podzielone zgodnie z wymogami anonimizacji.

2.4 Dodawanie i odchodzenie nowych firm i pracowników (onboarding / offboarding)

Nowe, przejęte firmy muszą być uwzględnione w następnej kampanii od momentu zamknięcia. Dotyczy to również wszystkich nowych pracowników. Ponadto nowi pracownicy muszą w ciągu 30 dni ukończyć wstępne szkolenie w zakresie świadomości bezpieczeństwa informacji. Odpowiedzialne działy IT i HR muszą podjąć odpowiednie środki ostrożności w tym zakresie. W przypadku pracowników sprzedanych przedsiębiorstw uczestnictwo jest obowiązkowe do czasu zamknięcia lub do końca okresu zatrudnienia przewidzianego w umowie. W każdym jednak przypadku, tak długo, jak infrastruktura klienta pozostaje w zakresie działania Grupy Arbonia. Wyjątki od tej zasady muszą być uzgodnione z kierownikami działów IT i CISO, a zainteresowani pracownicy muszą być o nich poinformowani.

3 Program podnoszenia świadomości w zakresie bezpieczeństwa informacji

3.1 Definicja

Polityka świadomościowa wspiera ISMS Arbonia Group poprzez wiążące określenie wymagań i specyfikacji programu świadomościowego w zakresie bezpieczeństwa informacji. Dzięki cyklicznym szkoleniom i ocenom wyników pracy pracownicy są informowani o ryzyku i zagrożeniach związanych z bezpieczeństwem informacji i uwrażliwiani na nie, a tym samym wśród wszystkich pracowników ma być stale rozwijana świadomość bezpieczeństwa informacji. Program podnoszenia świadomości w zakresie bezpieczeństwa informacji składa się zasadniczo z dwóch części (kampanii):

- Kampania informacyjna
- Kampania phishingowa

Kampanie są zwykle przeprowadzane raz na kwartał, ale co najmniej trzy razy w roku. Kampanie phishingowe mogą być przeprowadzane 6-8 razy w roku, w zależności od potrzeb i wymagań.

Ponadto program podnoszenia świadomości w zakresie bezpieczeństwa informacji obejmuje następujące działania:

- Kampanie plakatowe
- Narzędzia / Oprogramowanie (Przycisk phishingu w programie Outlook)
- Dodatkowe kampanie dla pracowników narażonych na ryzyko (HR, FI / CO, IT, itp.)
- Dodatkowe kampanie dla pracowników, którzy potrzebują dodatkowego szkolenia w związku z wynikami szkolenia

Wyniki poszczególnych kampanii są przetwarzane statystycznie i wykorzystywane do sterowania programem zwiększania świadomości w zakresie bezpieczeństwa informacji.

3.2 Kampanie uświadamiające

Kampanie uświadamiające są prowadzone zgodnie z definicją i dotyczą aktualnych tematów związanych z bezpieczeństwem informacji.

Kampanie uświadamiające są prowadzone za pomocą centralnej platformy phishingowej i uświadamiającej dla wszystkich spółek Grupy Arbonia i obejmują następujące punkty:

- Określenie tematu dotyczącego świadomości
- Aktualizowanie list odbiorców (onboarding/offboarding)
- Tworzenie i konfiguracja kampanii
- Testy i kontrola jakości
- Wdrożenie
- Zbieranie / przygotowywanie kluczowych danych statystycznych

Zaproszenie do udziału w kampanii informacyjnej jest wysyłane bezpośrednio do pracowników pocztą elektroniczną. Zaproszenie jest imienne i nie może być przekazywane innym pracownikom. Zwykle kampania uświadamiająca składa się z dwóch części: materiałów szkoleniowych i oceny wyników. W każdym przypadku należy wypełnić wszystkie części. Ponieważ udział w kampaniach świadomościowych jest obowiązkowy dla każdego pracownika, przypomina się o tym pracownikom przynajmniej raz w czasie trwania kampanii.

3.3 Kampanie phishingowe

Kampanie phishingowe są przeprowadzane zgodnie z definicją i dotyczą symulowanych ataków phishingowych.

Kampanie phishingowe są prowadzone za pomocą centralnej platformy phishingowej i świadomościowej dla wszystkich spółek Grupy Arbonia i obejmują następujące punkty:

- Określanie szablonów phishingu
- Aktualizowanie list odbiorców (onboarding/offboarding)
- Tworzenie i konfiguracja kampanii
- Testy i kontrola jakości
- Wdrożenie
- Zbieranie / przygotowywanie kluczowych danych statystycznych

Symulowane ataki phishingowe są wysyłane bezpośrednio do pracowników za pośrednictwem poczty elektronicznej lub innych odpowiednich kanałów. Symulowany atak phishingowy może przybierać różne formy. Jeśli pracownik zareaguje niepoprawnie na symulowany atak phishingowy, jest o tym automatycznie powiadamiany.

3.4 Role i obowiązki

Zespół ds. bezpieczeństwa informacji Grupy Arbonia jest odpowiedzialny za zdefiniowanie, przygotowanie, wdrożenie i ocenę programu podnoszenia świadomości w zakresie bezpieczeństwa informacji. Zmiany mające wpływ na cały program są omawiane z Radą Informatyki i uwzględniane przez CISO.

Lokalne zespoły HR są odpowiedzialne za terminowe przekazywanie informacji o wszystkich zmianach personalnych (wejście, wyjście, przeniesienie) do lokalnego zespołu IT. Lokalne zespoły informatyków dbają w ten sposób o aktualną bazę danych (główna baza danych pracowników w centralnej usłudze katalogowej Active Directory). Grupy odbiorców są aktualizowane przez zespół ds. bezpieczeństwa informacji Arbonia Group przed każdym wdrożeniem w oparciu o przynależność do grup Active Directory. Lokalny zespół IT jest również odpowiedzialny za wprowadzenie nowych pracowników na rynek pracy (wstępne szkolenie w zakresie świadomości bezpieczeństwa informacji w ciągu 30 dni) poprzez powiadomienie ich o tym pocztą elektroniczną na adres training@arbonia.com. Zespół ds. bezpieczeństwa informacji Arbonia Group zaprasza nowych pracowników na wstępne szkolenie uświadamiające po otrzymaniu tego powiadomienia.

4 Odpowiedzialność

Jak opisano w rozdziale 2.2, udział w programie podnoszenia świadomości w zakresie bezpieczeństwa informacji jest obowiązkowy dla wszystkich pracowników Grupy Arbonia i musi być realizowany w sposób sumienny i w pełni kompleksowy. W przypadku powtarzających się niepowodzeń można określić dodatkowe środki szkoleniowe. W przypadku zasadniczych niezgodności lub niewystarczającego uczestnictwa, dyrekcja odpowiedzialna zastrzega sobie prawo do podjęcia dalszych kroków.

5 Dokumenty źródłowe

- IS-ISS-GROUP-001-STRATEGIA BEZPIECZEŃSTWA INFORMACJI
- IS-GISP-GROUP-001-GENERAL-INFORMATION-SECURITY-POLICY
- IS-ISP-GROUP-004-IT-SECURITY-POLICY

6 Wejście w życie

Nazwa	**Jednostka biznesowa**	**Funkcja**	**Data**	**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 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 Odpowiednie załączniki

Nr	**Opis**	**Nazwa pliku**
1	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE