ARBONIA

IT SECURITY

Information Security Policy
Politica di sensibilizzazione

Versione:	1.0
Approvato:	13.04.2022
Stato:	RELEASED
Classificazione:	RESTRICTED
Creato da:	CISO
Approvato da:	Arbonia IT Board
Politica:	IS-ISP-GROUP-006 -IT-SECURITY-AWARENESS-POLICY
Revisione:	non disponibile

Informazioni sulla politica

Finalità	La politica di sensibilizzazione descrive e definisce il programma di sensibilizzazione alla sicurezza delle informazioni del Gruppo Arbonia.
Utente / destinatario	Tutti i dipendenti del Gruppo Arbonia
Archiviazione elettronica dei documenti	https://security.arbonia.com

Prova della modifica

Versione	Data	Stato	Modifica	da parte di
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

Indice

Elenco delle abbreviazioni

Termine	Descrizione
ICT	Tecnologia dell'informazione e della comunicazione
ISMS	Sistema di gestione della sicurezza delle informazioni

Glossario

Termine	Descrizione
Sistema di gestione della sicurezza delle informazioni	Un sistema di gestione della sicurezza delle informazioni è l'istituzione di procedure e regole all'interno di un'organizzazione che servono a definire, gestire, controllare, mantenere e migliorare continuamente la sicurezza delle informazioni in modo permanente.

1 Scopo, ambito e utenti

La politica descrive i requisiti e le specifiche del programma di consapevolezza della sicurezza delle informazioni del Gruppo Arbonia e li definisce in modo vincolante.

La politica si applica all'intero ambito del Sistema di Gestione della Sicurezza delle Informazioni (ISMS), cioè a tutti i dipendenti del Gruppo Arbonia, e serve a chiarire i compiti e i requisiti di ogni singolo dipendente nella protezione della riservatezza, dell'integrità e della disponibilità dei sistemi informativi e dei dati.

Tutti i dipendenti del Gruppo Arbonia sono utenti e destinatari di questa politica.

2 Principi di governance

2.1 Importanza del programma di sensibilizzazione sulla sicurezza delle informazioni

A causa del crescente collegamento in rete, della digitalizzazione e del cambiamento tecnologico che ne deriva, i potenziali aggressori stanno anche aprendo ulteriori opportunità per gli attacchi informatici. La sicurezza delle informazioni è molto dinamica e riguarda quasi tutti i settori del Gruppo Arbonia. L'aspetto socio-tecnico (interazione tra persone e sistemi informativi) può creare vulnerabilità in questa rete informativa.

Poiché un'adeguata protezione delle informazioni non può essere raggiunta solo con misure tecniche, ma dipende molto dal comportamento dei dipendenti e dalla loro gestione dei dati e dei sistemi informativi, è essenziale un programma di consapevolezza della sicurezza delle informazioni con sensibilizzazione e raccomandazioni di azione sulle minacce informatiche.

L'obiettivo è quello di creare una consapevolezza della sicurezza in costante crescita in ogni dipendente del Gruppo Arbonia secondo il motto ***PENSARE PRIMA DI VOI Click.Post.Type*** e di misurarla ad intervalli regolari.

2.2 Doveri degli impiegati

La partecipazione al programma di sensibilizzazione alla sicurezza delle informazioni è obbligatoria per tutti i dipendenti del Gruppo Arbonia e deve essere eseguita in modo coscienzioso e completo. Di conseguenza, tutte le parti della formazione (materiale didattico e revisione delle prestazioni) devono essere completate in ogni caso.

2.3 Anonimato / Conformità

L'implementazione delle campagne così come l'immagazzinamento e la valutazione dei dati statistici è effettuata secondo le norme legali specifiche del paese. Eventuali accordi sulla protezione dei dati devono essere stipulati in anticipo con i rispettivi comitati aziendali.

Il trattamento dei dati personali viene effettuato solo se la norma legale specifica del paese e/o il voto del consiglio di fabbrica interessato lo permette, per cui si può affermare che il trattamento dei dati personali offre un maggiore valore aggiunto, poiché i dipendenti possono essere supportati e formati in modo specifico. Se la norma legale o l'opinione non è data, la raccolta e l'elaborazione anonima dei dati statistici deve essere garantita. L'anonimizzazione è assicurata dal software utilizzato per la piattaforma di phishing e di sensibilizzazione. I gruppi di destinatari devono essere suddivisi in base ai requisiti di anonimizzazione.

2.4 Nuove aggiunte / partenze (onboarding / offboarding) di aziende e dipendenti

Le nuove aziende acquisite devono essere prese in considerazione per la prossima campagna dal momento della chiusura. Questo vale anche per tutti i nuovi dipendenti. Inoltre, i nuovi dipendenti devono completare una formazione iniziale di consapevolezza della sicurezza delle informazioni entro 30 giorni. I dipartimenti IT e HR responsabili devono prendere le opportune precauzioni per questo. Per i dipendenti delle aziende cedute, la partecipazione è obbligatoria fino al momento della chiusura o fino alla fine del servizio concordato contrattualmente. In ogni caso, però, finché l'infrastruttura del cliente rimane nell'ambito del Gruppo Arbonia. Le eccezioni a questa regola devono essere concordate con i responsabili IT e il CISO e i dipendenti interessati devono essere informati.

3 Programma di sensibilizzazione alla sicurezza delle informazioni

3.1 Definizione

La politica di sensibilizzazione sostiene l'ISMS del Gruppo Arbonia definendo in modo vincolante i requisiti e le specifiche del programma di sensibilizzazione alla sicurezza delle informazioni. Con i ricorrenti corsi di formazione e le revisioni delle prestazioni, i dipendenti sono informati e sensibilizzati sui rischi e le minacce alla sicurezza dell'informazione e quindi una costante consapevolezza della sicurezza dell'informazione deve essere generata tra tutti i dipendenti. Il programma di sensibilizzazione alla sicurezza delle informazioni consiste fondamentalmente in due parti (campagne):

- Campagna di sensibilizzazione
- Campagna di phishing

Le campagne sono normalmente effettuate trimestralmente, ma almeno tre volte all'anno. Le campagne di phishing possono essere effettuate 6-8 volte all'anno, a seconda delle necessità e dei requisiti.

Inoltre, il programma di sensibilizzazione alla sicurezza delle informazioni include le seguenti misure:

- Campagne di affissione
- Strumenti / Software (Outlook Phishing Button)
- Campagne aggiuntive per i dipendenti esposti (HR, FI / CO, IT, ecc.)
- Campagne aggiuntive per i dipendenti che hanno bisogno di ulteriore formazione a seguito dei risultati della formazione

I risultati delle singole campagne vengono elaborati statisticamente e utilizzati per orientare il programma di sensibilizzazione alla sicurezza delle informazioni.

3.2 Campagne di sensibilizzazione

Le campagne di sensibilizzazione sono realizzate secondo la definizione e affrontano temi attuali legati alla sicurezza dell'informazione.

Le campagne di sensibilizzazione si realizzano con una piattaforma centrale di phishing e sensibilizzazione per tutte le aziende del Gruppo Arbonia e comprendono i seguenti punti:

- Determinazione del tema della consapevolezza
- Aggiornamento delle liste di destinatari (onboarding/offboarding)
- Creazione e configurazione della campagna
- Test e ispezione della qualità
- Implementazione
- Raccolta / preparazione di dati statistici chiave

L'invito alla rispettiva campagna di sensibilizzazione viene inviato direttamente ai dipendenti via e-mail. L'invito è personalizzato e non può essere trasmesso ad altri dipendenti. Normalmente, la campagna di sensibilizzazione consiste di due parti, il materiale di formazione e la revisione delle prestazioni. In ogni caso, tutte le parti devono essere completate. Poiché la partecipazione alle campagne di sensibilizzazione è obbligatoria per ogni dipendente, i dipendenti vengono ricordati almeno una volta durante la campagna di sensibilizzazione.

3.3 Campagne di phishing

Le campagne di phishing sono effettuate secondo la definizione e affrontano attacchi di phishing simulati.

Le campagne di phishing sono realizzate con una piattaforma centrale di phishing e di sensibilizzazione per tutte le aziende del Gruppo Arbonia e comprendono i seguenti punti:

- Determinazione dei modelli di phishing

- Aggiornamento delle liste di destinatari (onboarding/offboarding)
- Creazione e configurazione della campagna
- Test e ispezione della qualità
- Implementazione
- Raccolta / preparazione di dati statistici chiave

Gli attacchi di phishing simulati sono inviati direttamente ai dipendenti via e-mail o altri canali appropriati. Un attacco di phishing simulato può assumere varie forme. Se un dipendente reagisce in modo errato a un attacco di phishing simulato, viene automaticamente avvisato.

3.4 Ruoli e responsabilità

Il team di sicurezza delle informazioni del Gruppo Arbonia è responsabile della definizione, preparazione, implementazione e valutazione del programma di sensibilizzazione alla sicurezza delle informazioni. I cambiamenti con un impatto sull'intero programma sono discussi con il consiglio IT e affrontati dal CISO.

I team HR locali sono responsabili della comunicazione tempestiva di tutti i cambiamenti del personale (entrata / uscita / trasferimento) al team IT locale. I team IT locali assicurano così il database attuale (master dei dipendenti nel servizio centrale di directory Active Directory). I gruppi di destinatari sono aggiornati dal team di sicurezza delle informazioni del Gruppo Arbonia prima di ogni implementazione in base all'appartenenza al gruppo di Active Directory. Il team IT locale è anche responsabile dell'onboarding (formazione iniziale di consapevolezza della sicurezza delle informazioni entro 30 giorni) dei nuovi dipendenti, notificando i nuovi assunti via e-mail a training@arbonia.com. Il team di sicurezza informatica del Gruppo Arbonia invita i nuovi dipendenti ad una formazione di sensibilizzazione iniziale dopo aver ricevuto questa notifica.

4 Responsabilità

Come descritto nel capitolo 2.2, la partecipazione al programma di sensibilizzazione alla sicurezza delle informazioni è obbligatoria per tutti i dipendenti del Gruppo Arbonia e deve essere svolta in modo coscienzioso e completo. In caso di fallimenti ripetuti, possono essere definite misure di formazione supplementari. In caso di inadempienza fondamentale o di partecipazione insufficiente, la direzione responsabile si riserva il diritto di prendere ulteriori misure.

5 Documenti di riferimento

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

6 Entrata in vigore

Cognome	Unità commerciale	Funzione	Data	Firma
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 Allegati rilevanti

N.	Descrizione	Nome del file
1	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE