ARBONIA
IT SECURITY

Information Security Policy
Política de sensibilización

Versión:	1.0
publicada el:	13.04.2022
Status:	RELEASED
Clasificación:	RESTRICTED
Redactado por:	CISO
Publicado por:	Arbonia IT Board
Directiva:	IS-ISP-G IS-ISP-GROUP-006 -IT-SECURITY-AWARENESS-POLICY
Revisión:	s/i

Información de directivas

Finalidad	La política de concienciación describe y define el programa de concienciación sobre la seguridad de la información del Grupo Arbonia.
Usuarios/Destinatarios	Todos los empleados del Grupo Arbonia
Archivo electrónico de documentos	https://security.arbonia.com

Registro de cambios

Versión	Fecha	Status	Modificación	realizada 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

Registro de abreviaturas

Término	Explicación
TIC	Tecnología de la información y las comunicaciones
ISMS	Sistema de gestión de la seguridad de la información

Glosario

Término	Explicación
Sistemas de gestión de seguridad de información	Un sistema de gestión de la seguridad de la información está formado por un compendio de procedimientos y reglas dentro de una organización que sirven para establecer, gestionar, controlar, mantener y mejorar continuamente y de forma duradera la seguridad de la información.

1 Finalidad, campo de aplicación y usuarios

La política describe los requisitos y especificaciones del programa de concienciación sobre la seguridad de la información del Grupo Arbonia y los define de forma vinculante.

La política se aplica a todo el ámbito del Sistema de Gestión de la Seguridad de la Información (SGSI), es decir, a todos los empleados del Grupo Arbonia, y sirve para aclarar las tareas y los requisitos de cada empleado a la hora de proteger la confidencialidad, la integridad y la disponibilidad de los sistemas de información y los datos.

Todos los empleados del Grupo Arbonia son usuarios y destinatarios de esta política.

2 Fundamentos de gobierno

2.1 Importancia del programa de concienciación sobre la seguridad de la información

Debido a la creciente interconexión, la digitalización y el cambio tecnológico derivado de ello, los posibles atacantes también están abriendo nuevas oportunidades para los ciberataques. La seguridad de la información es muy dinámica y afecta a casi todas las áreas del Grupo Arbonia. El aspecto sociotécnico (interacción entre las personas y los sistemas de información) puede crear vulnerabilidades en esta red de información.

Dado que una adecuada protección de la información no puede lograrse sólo con medidas técnicas, sino que depende en gran medida del comportamiento de los empleados y de su manejo de los datos y los sistemas de información, es esencial un programa de concienciación sobre la seguridad de la información con sensibilización y recomendaciones de actuación sobre las ciberamenazas.

El objetivo es crear una conciencia de seguridad cada vez mayor entre todos los empleados del Grupo Arbonia, de acuerdo con el lema ***THINK BERFORE YOU Click.Post.Type*** y medirlo a intervalos regulares.

2.2 Funciones de los empleados

La participación en el programa de concienciación sobre la seguridad de la información es obligatoria para todos los empleados del Grupo Arbonia y debe llevarse a cabo de forma concienzuda y exhaustiva. Por lo tanto, todas las partes de la formación (material de formación y revisión del rendimiento) deben completarse en cada caso.

2.3 Anonimato/Conformidad

La realización de las campañas, así como el almacenamiento y la evaluación de los datos estadísticos, se llevan a cabo de acuerdo con las normas legales específicas del país. Los acuerdos sobre la protección de datos, si los hay, deben realizarse previamente con los respectivos comités de empresa.

El tratamiento de datos personales sólo se lleva a cabo si la norma legal específica del país y/o el voto del comité de empresa correspondiente lo permiten, por lo que se puede afirmar que el tratamiento de datos personales ofrece un mayor valor añadido, ya que se puede apoyar y formar específicamente a los empleados. Si no se da la norma legal o el punto de vista, debe garantizarse la recogida y el tratamiento anónimos de los datos estadísticos. La anonimización está garantizada por el software utilizado para la plataforma de phishing y sensibilización. Los grupos de destinatarios deben subdividirse en función de los requisitos de anonimización.

2.4 Nuevas incorporaciones / salidas (onboarding / offboarding) de empresas y empleados

Las nuevas empresas adquiridas deben tenerse en cuenta para la siguiente campaña desde el momento del cierre. Esto también se aplica a todos los nuevos empleados. Además, los nuevos empleados deben realizar una formación inicial de concienciación sobre la seguridad de la información en un plazo de 30 días. Los departamentos de TI y RRHH responsables deben tomar las precauciones adecuadas para ello. Para los empleados de las empresas enajenadas, la participación es obligatoria hasta el momento del cierre o hasta el final del servicio acordado contractualmente. En cualquier caso, mientras la infraestructura del cliente permanezca en el ámbito del Grupo Arbonia. Las excepciones a esta norma deben acordarse con los responsables de TI y el CISO, y los empleados afectados deben ser informados.

3 Programa de concienciación sobre la seguridad de la información

3.1 Definición

La política de concienciación apoya el SGSI del Grupo Arbonia al definir de forma vinculante los requisitos y las especificaciones del programa de concienciación sobre la seguridad de la información. Con los cursos de formación recurrentes y las revisiones de rendimiento, los empleados son informados y sensibilizados sobre los riesgos y amenazas a la seguridad de la información, por lo que se debe generar una conciencia constante de seguridad de la información entre todos los empleados. El programa de concienciación sobre la seguridad de la información consta básicamente de dos partes (campañas):

- Campaña de sensibilización
- Campaña de phishing

Las campañas suelen realizarse trimestralmente, pero al menos tres veces al año. Las campañas de phishing pueden llevarse a cabo entre 6 y 8 veces al año, en función de las necesidades y los requisitos.

Además, el programa de concienciación sobre la seguridad de la información incluye las siguientes medidas:

- Campañas de carteles
- Herramientas / Software (Botón de suplantación de identidad de Outlook)
- Campañas adicionales para los empleados expuestos (RRHH, FI / CO, IT, etc.)
- Campañas adicionales para los empleados que necesiten formación adicional como consecuencia de los resultados de la formación

Los resultados de las campañas individuales se procesan estadísticamente y se utilizan para dirigir el programa de concienciación sobre la seguridad de la información.

3.2 Campañas de sensibilización

Las campañas de sensibilización se llevan a cabo según la definición y abordan temas de actualidad relacionados con la seguridad de la información.

Las campañas de concienciación se realizan con una plataforma central de phishing y concienciación para todas las empresas del Grupo Arbonia e incluyen los siguientes puntos:

- Determinación del tema de sensibilización
- Actualización de las listas de destinatarios (altas y bajas)
- Creación y configuración de campañas
- Pruebas e inspección de calidad
- Aplicación
- Recogida/preparación de ratios estadísticos

La invitación a la campaña de sensibilización correspondiente se envía directamente a los empleados por correo electrónico. La invitación es personalizada y no puede ser transmitida a otros empleados. Normalmente, la campaña de concienciación consta de dos partes, el material de formación y la revisión del rendimiento. En cualquier caso, todas las partes deben ser completadas. Como la participación en las campañas de sensibilización es obligatoria para todos los empleados, se les recuerda al menos una vez durante la campaña de sensibilización.

3.3 Campañas de phishing

Las campañas de phishing se llevan a cabo según la definición y abordan ataques de phishing simulados.

Las campañas de phishing se llevan a cabo con una plataforma central de phishing y concienciación para todas las empresas del Grupo Arbonia e incluyen los siguientes puntos

- Determinación de las plantillas de phishing
- Actualización de las listas de destinatarios (altas y bajas)
- Creación y configuración de campañas
- Pruebas e inspección de calidad
- Aplicación
- Recogida/preparación de ratios estadísticos

Los ataques de phishing simulados se envían directamente a los empleados por correo electrónico u otros canales apropiados. Un ataque de phishing simulado puede adoptar varias formas. Si un empleado reacciona de forma incorrecta a un ataque de phishing simulado, se le notifica automáticamente.

3.4 Funciones y responsabilidades

El equipo de seguridad de la información del Grupo Arbonia se encarga de definir, preparar, aplicar y evaluar el programa de concienciación sobre la seguridad de la información. Los cambios que tienen un impacto en todo el programa se discuten con el Consejo de TI y son abordados por el CISO.

Los equipos locales de RRHH son responsables de la comunicación oportuna de todos los cambios de personal (entrada/salida/transferencia) al equipo local de TI. Los equipos informáticos locales aseguran así la base de datos actual (maestro de empleados en el servicio de directorio central Active Directory). El equipo de seguridad de la información de Arbonia Group actualiza los grupos de destinatarios antes de cada implementación basándose en la pertenencia a grupos de Active Directory. El equipo local de TI también es responsable de la incorporación (formación inicial de concienciación sobre la seguridad de la información en un plazo de 30 días) de los nuevos empleados, notificándolo por correo electrónico a training@arbonia.com. El equipo de seguridad de la información de Arbonia Group invita a los nuevos empleados a una formación inicial de concienciación tras recibir esta notificación.

4 Rendición de cuentas

Tal y como se describe en el capítulo 2.2, la participación en el programa de concienciación sobre la seguridad de la información es obligatoria para todos los empleados del Grupo Arbonia y debe llevarse a cabo de forma concienzuda y completa. En caso de que se repitan los fallos, se podrán definir medidas de formación adicionales. En caso de incumplimiento fundamental o de participación insuficiente, la dirección responsable se reserva el derecho de tomar otras medidas.

5 Documentos de referencia

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

6 Entrada en vigor

Nombre	División	Función	Fecha	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 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 Anexos relevantes

N.º	Explicación	Nombre del archivo
1	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE