ARBONIA
IT SECURITY

# Политика информационной безопасности

# Политика осведомленности

| | |
|---|---|
| Версия: | 1.0 |
| Принято (дата): | 13.04.2022 |
| Статус: | RELEASED |
| Классификация: | RESTRICTED |
| Составлено (кем): | CISO |
| Принято (кем): | Arbonia IT Board |
| Политика: | IS-ISP-GROUP-006 -IT-SECURITY-AWARENESS-POLICY |
| Изменение: | н/д |

**Информация о политике**

| | |
|---|---|
| **Цель** | Политика осведомленности описывает и определяет программу осведомленности Arbonia Group в области информационной безопасности. |
| **Пользователи / получатели** | Все сотрудники Arbonia Group |
| **Электронное хранение документов** | https://security.arbonia.com |

**Лист регистрации изменений**

| **Версия** | **Дата** | **Статус** | **Изменение** | **(кем)** |
|---|---|---|---|---|
| 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 |

# Содержание

**Список сокращений**

| Термин | Описание |
|---|---|
| ИКТ | Информационно-коммуникационные технологии |
| ISMS | Система управления информационной безопасностью |
| | |

**Глоссарий**

| Термин | Описание |
|---|---|
| Системы управления информационной безопасностью | Система управления информационной безопасностью представляет собой ряд методов и правил внутри организации, предназначенных для долговременного обеспечения, управления, мониторинга, поддержания и дальнейшего улучшения информационной безопасности предприятия. |
| | |
| | |

# 1 Цель, область применения и круг пользователей

Политика описывает требования и спецификации программы осведомленности об информационной безопасности Arbonia Group и определяет их в обязательном порядке.

Политика распространяется на всю сферу действия системы управления информационной безопасностью (СУИБ), то есть на всех сотрудников Arbonia Group, и служит для разъяснения задач и требований каждого отдельного сотрудника по защите конфиденциальности, целостности и доступности информационных систем и данных.

Все сотрудники Arbonia Group являются пользователями и получателями данной политики.

# 2 Принципы управления

## 2.1 Важность программы повышения осведомленности в области информационной безопасности

Благодаря растущему сетевому взаимодействию, цифровизации и технологическим изменениям, вытекающим из этого, потенциальные злоумышленники также открывают новые возможности для кибер-атак. Информационная безопасность очень динамична и затрагивает практически все сферы деятельности Arbonia Group. Социально-технический аспект (взаимодействие между людьми и информационными системами) может создать уязвимости в этой информационной сети.

Поскольку адекватная защита информации не может быть достигнута только техническими мерами, а в значительной степени зависит от поведения сотрудников и их обращения с данными и информационными системами, программа повышения осведомленности в области информационной безопасности с разъяснением и рекомендациями по действиям в отношении киберугроз имеет важное значение.

Целью является создание постоянно растущей осведомленности о безопасности среди каждого сотрудника Arbonia Group в соответствии с девизом ***THINK BERFORE YOU Click.Post.Type*** и регулярное измерение этого показателя.

## 2.2 Обязанности сотрудников

Участие в программе повышения осведомленности об информационной безопасности является обязательным для всех сотрудников Arbonia Group и должно осуществляться соответствующим образом, добросовестно и всесторонне. Соответственно, в каждом случае должны быть выполнены все части обучения (учебный материал и оценка работы).

## 2.3 Анонимность / Соответствие

Проведение кампаний, а также хранение и оценка статистических данных осуществляются в соответствии с правовыми нормами конкретной страны. Соглашения о защите данных, если таковые имеются, должны быть заключены с соответствующими рабочими советами заранее.

Обработка персональных данных осуществляется только в том случае, если это разрешено нормами законодательства конкретной страны и/или голосованием соответствующего производственного совета, при этом можно утверждать, что обработка персональных данных обеспечивает большую добавленную стоимость, так как сотрудники могут быть специально поддержаны и обучены. Если правовая норма или мнение не приведены, необходимо обеспечить анонимный сбор и обработку статистических данных. Анонимизация обеспечивается программным обеспечением, используемым для платформы фишинга и осведомленности. Группы получателей должны быть разделены в соответствии с требованиями анонимизации.

## 2.4 Новые поступления / выбытия (прием / увольнение) компаний и сотрудников

Новые, приобретенные компании должны быть учтены в следующей кампании с момента закрытия. Это также относится ко всем новым сотрудникам. Кроме того, новые сотрудники должны в течение 30 дней пройти начальный курс обучения по информационной безопасности. Ответственные ИТ- и кадровые службы должны принять соответствующие меры предосторожности для этого. Для сотрудников продаваемых компаний участие в программе является обязательным до момента закрытия или до окончания оговоренной в контракте службы. В любом случае, однако, до тех пор, пока инфраструктура клиента остается в сфере деятельности Arbonia Group. Исключения из этого правила должны быть согласованы с ИТ-менеджерами и CISO, а соответствующие сотрудники должны быть проинформированы.

# 3 Программа повышения осведомленности в области информационной безопасности

## 3.1 Определение

Политика осведомленности поддерживает СУИБ Arbonia Group, в обязательном порядке определяя требования и спецификации программы осведомленности об информационной безопасности. Благодаря регулярным тренингам и аттестациям сотрудники информируются о рисках и угрозах информационной безопасности и обращают внимание на них, что позволяет постоянно повышать осведомленность всех сотрудников в вопросах информационной безопасности. Программа повышения осведомленности в области информационной безопасности в основном состоит из двух частей (кампаний):

- Информационная кампания
- Фишинговая кампания

Кампании обычно проводятся ежеквартально, но не реже трех раз в год. Фишинговые кампании могут проводиться 6-8 раз в год, в зависимости от потребностей и требований.

Кроме того, программа повышения осведомленности об информационной безопасности включает следующие меры:

- Плакатные кампании
- Инструменты / Программное обеспечение (Фишинговая кнопка Outlook)
- Дополнительные кампании для сотрудников, подверженных риску (HR, FI / CO, IT и т.д.)
- Дополнительные кампании для сотрудников, нуждающихся в дополнительном обучении по результатам тренинга

Результаты отдельных кампаний обрабатываются статистически и используются для управления программой повышения осведомленности в области информационной безопасности.

## 3.2 Информационные кампании

Информационные кампании проводятся в соответствии с определением и затрагивают актуальные темы, связанные с информационной безопасностью.

Информационные кампании проводятся с помощью центральной фишинговой и информационной платформы для всех компаний группы Arbonia и включают следующие пункты:

- Определение темы осведомленности
- Обновление списков получателей (включение/выключение)
- Создание и настройка кампаний
- Испытания и проверка качества
- Реализация
- Сбор/подготовка основных статистических данных

Приглашение на соответствующую информационную кампанию рассылается непосредственно сотрудникам по электронной почте. Приглашение является персональным и не может быть передано другим сотрудникам. Как правило, информационная кампания состоит из двух частей - учебного материала и аттестации. В любом случае, все части должны быть заполнены. Поскольку участие в информационных кампаниях является обязательным для каждого сотрудника, работникам напоминают об этом как минимум один раз в течение информационной кампании.

## 3.3 Фишинговые кампании

Фишинговые кампании проводятся в соответствии с определением и направлены на имитацию фишинговых атак.

Фишинговые кампании проводятся с помощью центральной фишинговой и информационной платформы для всех компаний группы Arbonia и включают следующие пункты:

- Определение фишинговых шаблонов
- Обновление списков получателей (включение/выключение)
- Создание и настройка кампаний
- Испытания и проверка качества
- Реализация
- Сбор/подготовка основных статистических данных

Имитированные фишинговые атаки рассылаются непосредственно сотрудникам по электронной почте или другим соответствующим каналам. Имитация фишинговой атаки может принимать различные формы. Если сотрудник неправильно реагирует на имитацию фишинговой атаки, он автоматически получает уведомление.

## 3.4 Роли и обязанности

Команда информационной безопасности Arbonia Group отвечает за определение, подготовку, внедрение и оценку программы повышения осведомленности в области информационной безопасности. Изменения, оказывающие влияние на всю программу, обсуждаются с Советом по ИТ и рассматриваются CISO.

Местные HR-команды отвечают за своевременное информирование местной IT-команды обо всех кадровых изменениях (ввод / вывод / перевод). Таким образом, местные ИТ-команды обеспечивают работу текущей базы данных (мастер сотрудников в центральной службе каталогов Active Directory). Группы получателей обновляются командой информационной безопасности Arbonia Group перед каждым внедрением на основе состава групп Active Directory. Местная ИТ-команда также отвечает за включение (начальное обучение по информационной безопасности в течение 30 дней) новых сотрудников, уведомляя их об этом по электронной почте training@arbonia.com. Команда информационной безопасности Arbonia Group приглашает новых сотрудников пройти начальное обучение по повышению осведомленности после получения данного уведомления.

# 4 Подотчетность

Как описано в главе 2.2, участие в программе повышения осведомленности об информационной безопасности является обязательным для всех сотрудников Arbonia Group и должно осуществляться соответствующим образом, добросовестно и в полном объеме. В случае повторных неудач могут быть

определены дополнительные меры по обучению. В случае принципиального несоблюдения или недостаточного участия ответственное руководство оставляет за собой право принять дополнительные меры.

# 5 Справочные документы

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

# 6 Вступление в силу

| Фамилия | Подразделение | Должность | Дата | Подпись |
|---|---|---|---|---|
| Patrick Langenegger | Corporate IT | CIO Arbonia Group / CIO Division Doors | 2021-04-13 | n/a |
| Michael Kreter | Division HVAC | Head of IT Kermi<br>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 Соответствующие приложения

| № | Описание | Имя файла |
|---|---|---|
| 1 | IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE | IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE |