Технологии ОФС

Элемент: Глобальный
Тип документа: Политика
Номер документа: TOFS-IS-RU-000017
Редакция: 1
Дата вступления: 24 июля 2023 г.

Политика информационной безопасности АО «Технологии ОФС»

Содержание

Перечень редакций					
Ред.	RDR	Содержание изменений	Подготовил	Утвердил	Дата вступления
Текущая редакция					
1	-	Первоначальный выпуск	Ойтов А.	Аникеев А.	24 июля 2023 г.
Предыдущие редакции					

Авторское право 2023 компании Технологии ОФС. Информация, которая содержится в настоящем документе, относится к конфиденциальной и является собственностью компании Технологии ОФС и её подразделений. Данная информация предназначена для использования только в интересах компании Технологии ОФС. Распространение, пересылка, воспроизведение, изменение или использование информации в любых целях без явно выраженного письменного разрешения компании Технологии ОФС запрещается.

Экземпляры, распечатанные или переданные в электронном виде, являются неконтролируемыми

1 Цель

Информационные ресурсы АО «Технологии ОФС» (далее – «Компания») являются одними из ее ценнейших активов.

Управление и обеспечение информационной безопасности Компании ориентировано на достижение следующих целей:

- Предоставление безопасной информационной среды для функционирования и развития бизнеса;
- Повышение конкурентоспособности, деловой репутации и ценности бизнеса для акционеров путем снижения уровня риска в области информационной безопасности;
- Соответствие требованиям законодательства в области информационной безопасности и защиты персональных данных, а также соблюдение договорных обязательств в сфере защиты информации;
- Повышение корпоративной культуры обработки и защиты информации;
- Предотвращение инцидентов информационной безопасности;
- Эффективное управление процессами информационной безопасности и непрерывное совершенствование системы управления информационной безопасностью.

В Компании могут применяться иные документы, которые регулируют те или иные специализированные аспекты информационной безопасности.

В случае выявления противоречий между настоящим документом и иным локальными нормативными актами Компании, необходимо задать уточняющий вопрос представителю отдела информационной безопасности или юристу Компании.

2 Область применения

Настоящая политика применяется ко всем информационным ресурсам, принадлежащим Компании или находящимся в пользовании.

Все Работники Компании должны следовать установленной Политике при взаимодействии с информационными ресурсами Компании.

Компания приветствует соблюдение положений политики информационной безопасности при использовании личных информационных ресурсов.

3 Основные положения

1 Компания должна осуществлять учет информационных ресурсов, принадлежащих ей.

2 Компания должна быть осведомлена о том, какие информационные ресурсы нуждаются в защите, произведена ли классификация данных ресурсов и определена ли степень их важности.

3 При выборе и применении мер по обеспечению информационной безопасности, Компания соблюдает требования применимого законодательства.

4 Компания всегда предупреждает об используемых мерах безопасности. Использование скрытых мер безопасности недопустимы.

5 Каждому информационному ресурсу должен быть назначен владелец, который является ответственным за его правильную классификацию и защиту.

6 Деятельность Компании в области информационной безопасности должна соотноситься с целями Компании.

7 Определение мер по обеспечению информационной безопасности в Компании осуществляется на основе анализа угроз и оценке рисков безопасности информационных ресурсов.

~~8~~ Компания расследует все инциденты, связанные с нарушением безопасности информации и принимает меры по предотвращению подобных инцидентов в будущем.

9 Вся информация, используемая в Компании, должна быть валидирована, а источник информации должен быть аутентифицирован.

10 Информация должна быть использована в объеме, необходимом для достижения поставленных целей. По достижении целей необходимо обеспечить безопасное уничтожение информации.

4 Ожидания

Положения данной Политики должны учитываться при разработке локальных нормативных актов Компании.
Нарушение требований нормативных актов Компании по обеспечению ИБ является инцидентом и будет служить поводом и основанием для проведения служебного расследования.
Работники Компании обязаны сообщать обо всех инцидентах, связанных с информационной безопасностью в отдел информационной безопасности.

5 Ответственность

Работники Компании несут ответственность за нарушение требований настоящей Политики в соответствии с локальными нормативными актами Компании и действующим законодательством.
Линейные руководители несут ответственность за обеспечение соблюдения требований политики своими подчиненными.
Отдел информационной безопасности несет ответственность за расследование инцидентов относящихся к информационной безопасности, разработку документации по информационной безопасности и поддержание положений настоящей Политики в актуальном состоянии, а также за информирование работников Компании об актуальных угрозах и принципах безопасного поведения в сфере информационной безопасности.

6 Термины, определения и сокращения

- **Аутентификация – обеспечение гарантии того, что заявленные характеристики объекта являются подлинными.**
- **Валидация — процесс определения точности, полноты или соответствия данных установленным критериям.**
- **Доступность – обеспечение доступа к информации авторизированным пользователям, когда это необходимо (по требованию).**
- **Информационная безопасность (ИБ)** – обеспечение доступности, целостности и конфиденциальности информационных ресурсов.
- **Информационный ресурс** – совокупность информации, определяемая и управляемая как единое целое, которую можно понять, разделить, защитить и эффективно использовать. К информационным ресурсам также относятся средства, методы, используемые для обработки информации, а также сотрудники участвующие в процессе обработке информации.
- **Инцидент информационной безопасности (Инцидент ИБ) – единичное или серия нежелательных или неожиданных событий информационной безопасности, которые со значительной вероятностью могут поставить под угрозу бизнес-операции и угрожать информационной безопасности.**
- **Конфиденциальность** – обеспечение доступности информации только для тех, кто имеет соответствующие полномочия (авторизированные пользователи).
- **Оборудование Компании** – рабочие компьютеры (портативные, стационарные и планшеты) и телефоны (мобильные, стационарные и факсы), а также сервера, коммутационное оборудование, оборудование по видеонаблюдению и иное оборудование, используемое Компанией в процессе своей деятельности.
- **Целостность -** обеспечение точности и полноты информации, а также методов ее обработки.

7 Ссылки

Настоящая Политика разработана с учетом положений следующих законодательных и нормативных правовых актов:

- ГОСТ Р ИСО/МЭК 27000-2021 Информационные технологии (ИТ). Методы и средства обеспечения безопасности;
- Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информатизации и защите информации»;
- Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»;
- «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;
- «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 года;
- «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом ФСБ от 9 февраля 2005 № 66;
- Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ;
- Закон РФ «О недрах» от 21.02.1992 № 2395-1 (последняя редакция).