ПОЛИТИКА

Информационной Безопасности

Версия 2

г. Москва
2016

Паспорт документа	
Инициатор	Руководитель департамента безопасности ООО «Софтлайн интеграция» Мельников А.Г.
Разработчик	Заместитель руководителя Аналитического отдела Департамента сервисных услуг и технической поддержки Управления сервисов ЗАО «СофтЛайн Солюшн» Мосягин А.А.
Введен	Взамен Политики ИБ от 19 марта 2013
Версия	2
Статус	Действует
Заменен на	Нет
Дата следующего пересмотра	До 01.06.2017
Пункты стандарта ISO 9001:2008, требования которых реализует данный документ	П. 6.3
Пункты стандарта ISO 27001:2013, требования которых реализует данный документ	П. 5.2
Вовлеченные подразделения/ должности	Все структурные подразделения и должности Группы Компаний Softline
Нормоконтроль и экспертиза (ФИО, дата)	Менеджер по качеству Отдела менеджмента качества Управления качества АО «СофтЛайн Трейд» Фонайлова Е.А., 10.05.2016
Согласовано (ФИО, дата)	Генеральный директор ООО «СК Софтлайн» Руководитель департамента безопасности ООО «Софтлайн интеграция» Мельников А.Г., 11.05.2016 Директор по информационным технологиям ЗАО «СофтЛайн Солюшн» Решетков. А.В., 10.05.2016
Утверждено (ФИО, дата)	Председатель совета директоров Группы Компаний Softline Боровиков И.П., 06.06.2016

СОДЕРЖАНИЕ

1. Назначение

1.1. Настоящая Политика является основополагающим документом, регулирующим деятельность Группы компаний Softline в области информационной безопасности

1.2. Корпоративные требования в сфере обеспечения информационной безопасности распространяются на все регионы деятельности и на все бизнес-подразделения Группы компаний Softline.

2. Термины и определения, сокращения и обозначения

2.1. Термины и определения

Аудит - систематический, независимый и документированный процесс получения свидетельств аудита и их объективного оценивания для определения степени соответствия критериям аудита.

Компания - любое юридическое лицо, входящее в Группу компаний Софтлайн или аффилированное с ними.

Корпоративная культура Компании – это свод важных положений деятельности Компании, определяемых ее миссией и стратегией развития и находящих выражение в совокупности социальных норм и ценностей, разделяемых всеми сотрудниками Компании.

Работник - физическое лицо, которое состоит в трудовых отношениях с Компанией на основании заключенного Трудового договора и работающее в Компании по основному месту работы, либо по совместительству.

Сотрудник – физическое лицо, вступившее в трудовые взаимоотношения с работодателем.

2.2. Сокращения и обозначения

ФИО – фамилия, имя, отчество. Имя и отчество указываются в виде инициалов.

3. Нормативные ссылки

ISO 9001:2008 Системы менеджмента качества. Требования;

ISO/IEC 27001:2013 Системы менеджмента информационной безопасности.

4. Общие положения

4.1. Под информационной безопасностью понимается состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, целостность и доступность информации при ее обработке техническими средствами.

4.2. Политика информационной безопасности разработана в соответствии с положениями международного стандарта ISO/IEC 27001:2013.

4.3. Политика информационной безопасности утверждается Председателем совета директоров Группы компаний Softline.

4.4. Пересмотр Политики проводится на регулярной основе не реже одного раз в год.

4.5. Ответственность за общий контроль содержания настоящего документа и внесение в него изменений возлагается на Руководителя Департамента безопасности.

5. Цели в области информационной безопасности

В области информационной безопасности Группой компаний Softline устанавливаются следующие стратегические цели:

5.1. Повышение конкурентоспособности бизнеса Группы компаний Softline;

5.2. Соответствие требованиям законодательства и договорным обязательствам в части информационной безопасности;

5.3. Повышение деловой репутации и корпоративной культуры Группы компаний Softline;

5.4. Эффективное управление информационной безопасностью и непрерывное совершенствование системы управления информационной безопасностью;

5.5. Достижение адекватности мер по защите от угроз информационной безопасности;

5.6. Обеспечение безопасности корпоративных активов Группы компаний Softline, включая персонал, материально-технические ценности, информационные ресурсы, бизнес-процессы.

6. Задачи обеспечения информационной безопасности

Система обеспечения информационной безопасности Группы компаний Softline должна решать следующие задачи:

6.1. Вовлечение высшего руководства Группы компаний Softline в процесс обеспечения информационной безопасности: деятельность по обеспечению информационной безопасности инициирована и контролируется высшим руководством Группы компаний Softline;

6.2. Соответствие требованиям законодательства РФ: Группа компаний Softline реализует меры обеспечения информационной безопасности в строгом соответствии с действующим законодательством и договорными обязательствами;

6.3. Согласованность действий по обеспечению информационной, физической и экономической безопасности: действия по обеспечению информационной, физической и экономической безопасности осуществляются на основе четкого взаимодействия заинтересованных подразделений Группы компаний Softline и согласованы между собой по целям, задачам, принципам, методам и средствам;

6.4. Применение экономически целесообразных мер: Группа компаний Softline стремится выбирать меры обеспечения информационной безопасности с учетом затрат на их реализацию, вероятности возникновения угроз информационной безопасности и объема возможных потерь от их реализации;

6.5. Проверка работников: все кандидаты на вакантные должности в Группе компаний Softline в обязательном порядке проходят проверку в соответствии с установленными процедурами;

6.6. Документированность требований информационной безопасности: в Группе компаний Softline все требования в области информационной безопасности фиксируются в разрабатываемых внутренних нормативных документах;

6.7. Повышение осведомленности в вопросах обеспечения информационной безопасности: документированные требования в области информационной безопасности доводятся до сведения работников всех бизнес-подразделений Группы компаний Softline и контрагентов в части их касающейся;

6.8. Реагирование на инциденты информационной безопасности: Группа компаний Softline стремится выявлять, учитывать и оперативно реагировать на действительные, предпринимаемые и вероятные нарушения информационной безопасности;

6.9. Оценка рисков: в Группе компаний Softline на постоянной основе реализуются мероприятия по оценке и управлению рисками информационной безопасности, повышению уровня защищенности информационных активов;

6.10. Учет требований информационной безопасности в проектной деятельности: помимо операционной деятельности, Группа компаний Softline стремится учитывать требования информационной безопасности в проектной деятельности. Разработка и документирование требований по обеспечению информационной безопасности осуществляется на начальных этапах реализации проектов, связанных с обработкой, хранением и передачей информации;

6.11. Постоянное совершенствование системы управления информационной безопасностью: совершенствование системы управления информационной безопасности является непрерывным процессом.

7. Принципы обеспечения информационной безопасности

7.1. Принцип системности

В Группе компаний Softline активы рассматриваются, как взаимосвязанные и взаимовлияющие компоненты единой системы. Учитывается максимально возможное количество сценариев поведения системы в случае возникновения угроз информационной безопасности. Система защиты строится с учетом не только всех известных каналов получения несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности;

7.2. Принцип полноты (комплексности)

Для обеспечения информационной безопасности используется широкий спектр мер, методов и средств защиты информации. Комплексное их использование предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающие все существующие каналы угроз и не содержащие слабых мест на стыках отдельных её компонентов;

7.3. Принцип эшелонированности

Нельзя полагаться на один защитный рубеж, каким бы надежным он ни казался. Система обеспечения информационной безопасности стоится таким образом, чтобы наиболее защищаемая зона безопасности находилась внутри других защищаемых зон;

7.4. Принцип равнопрочности

Эффективность защитных механизмов не должна быть сведена на нет слабым звеном, возникшим в результате недооценки реальных угроз либо применения неадекватных мер защиты;

7.5. Принцип непрерывности

В Группе компаний Softline обеспечение информационной безопасности является непрерывным целенаправленным процессом, предполагающим принятие соответствующих мер на всех этапах жизненного цикла активов.

7.6. Принцип разумной достаточности

Руководство Группы компаний Softline исходит из того, что создать «абсолютную» защиту активов невозможно. Поэтому выбор средств защиты активов, адекватных реально существующим угрозам (т.е. обеспечивающих допустимый уровень возможного ущерба в случае реализации угроз), осуществляется на основе проведения анализа рисков;

7.7. Принцип законности

При выборе и реализации мер и средств обеспечения информационной безопасности Группой компаний Softline строго соблюдается законодательство Российской Федерации, требования нормативных правовых и технических документов в области обеспечения информационной безопасности Группы компаний Softline;

7.8. Принцип управляемости

Все процессы управления и обеспечения информационной безопасностью в Группе компаний Softline должны быть управляемыми, т.е. должна быть возможность мониторинга и измерения процессов и компонентов, своевременного выявления нарушений информационной безопасности и принятия соответствующих мер;

7.9. Принцип персональной ответственности

Ответственность за обеспечение безопасности активов возлагается на каждого работника в пределах его полномочий.

8. Распределение ролей и ответственности

Для эффективного внедрения процессов управления информационной безопасностью в Группе компаний Softline внедряется система управления информационной безопасностью на основе требований Международного стандарта ISO/IEC 27001:2013. Система управления информационной безопасностью регламентируется отдельными положениями и стандартами, принятыми в Группе компаний Softline.

8.1. Подразделения информационной безопасности:

- совместно с представителями бизнес-подразделений и подразделений Департамента информационных технологий, включая обособленные подразделения Компании, занимающиеся поддержкой и внедрением информационных сервисов (далее ИТ), проводят оценку рисков, связанных с защитой информации, и осуществляют управление этими рисками;

- совместно с подразделениями ИТ разрабатывают и внедряют политики и стандарты информационной безопасности, основанные на признанных в мире стандартах информационной безопасности;

- разрабатывают планы и технические спецификации для внедрения систем информационной безопасности;

- определяют требования по информационной безопасности для существующих и внедряемых информационных систем;

- обосновывают и совместно с ИТ защищают общий бюджет ИТ в части, касающейся информационной безопасности Группы компаний Softline, с целью выделения достаточных средств для функционирования и развития систем информационной безопасности;

- участвуют в разработке стандартов, инструкций и иных нормативных документов в сфере ИТ, выборе контрагентов и утверждении технических решений в части информационной безопасности;

- проводят аудит информационных систем с целью выявления потенциальных уязвимостей в корпоративных информационных системах, используют предоставленные ИТ возможности и инструменты, организуют оповещение пользователей о попытках вторжения в информационные системы;

- могут привлекать ресурсы сторонних фирм для проведения аудита информационных систем с точки зрения информационной безопасности;

- организуют и проводят обучение сотрудников Компании по информационной безопасности, проверяют знания и навыки информационной безопасности сотрудников Компании;

- принимают активное участие в процессе изменения информационных систем для обеспечения требуемого уровня информационной безопасности;

- согласовывают и контролируют доступ пользователей к информационным ресурсам;

- проводят постоянную работу с пользователями информационных ресурсов Компании по разъяснению им основных требований информационной безопасности.

8.2. Подразделения Информационных технологий:

- внедряют новые информационные системы и инструменты, обеспечивающие реализацию совместно разработанных политик, стандартов информационной безопасности;

- обеспечивают работоспособность и доступность информационных систем;

- соблюдают все совместно разработанные требования информационной безопасности;

- разрабатывают и внедряют планы развития информационных систем, обеспечивают финансирование и осуществляют все виды технической деятельности в корпоративных информационных системах;
- следуют совместно принятым корпоративным политикам, стандартам и инструкциям по информационной безопасности, равно как и своим функциональным обязанностям;
- следуют совместно разработанным требованиям и рекомендациям подразделений информационной безопасности на всех стадиях реализации новых проектов: от предложения и планирования до осуществления;
- управляют процессом изменения информационных систем Группы компаний Softline;
- незамедлительно информируют подразделения информационной безопасности о любых нарушениях, уязвимостях, обнаруженных в корпоративных информационных системах и попытках незаконного проникновения в них;
- обеспечивают доступ пользователей к компьютерным системам;
- являются держателем бюджета ИТ, включая статьи расходов на информационную безопасность, и обеспечивают финансирование утвержденных проектов информационной безопасности;
- обеспечивают техническую эксплуатацию систем безопасности.

9. Ответственность за нарушение Политики информационной безопасности

В случае нарушения установленных правил работы с информационными активами работник может быть ограничен в правах доступа к таким активам, а также привлечен к ответственности в соответствии с Трудовым кодексом, Кодексом об административных правонарушениях и Уголовным кодексом РФ.

Лист регистрации изменений

Номер отмененной версии	Номера пунктов, рисунков, таблиц, приложений			Дата утверждения отмененной версии
	Измененных	Введенных вновь	Удаленных	
1	Полностью изменен формат документа	Нет	Нет	19.03.2016