Утверждаю
Директор ООО «Мосье Башмаков»
Мулик М.Н. _____
Дата: 17/01/2017

Политика

информационной безопасности ООО «Мосье Башмаков»

для размещения в сети интернет

Содержание

1. Общие положения

Обеспечение информационной безопасности является, необходимым условием для осуществления деятельности ООО «Мосье Башмаков» (далее по тексту – Компания). Нарушение информационной безопасности может привести к серьезным последствиям для ООО «Мосье Башмаков», включая потерю доверия со стороны клиентов, партнеров, поставщиков и снижение конкурентоспособности.

1.1 Цель документа

Целью Политики информационной безопасности ООО «Мосье Башмаков» для размещения в сети интернет (далее – Политика) является декларация основных целей и положений по организации процессов обеспечения и управления информационной безопасностью ООО «Мосье Башмаков» (далее – Компания).

1.2 Область применения

Политика предназначена для:

- опубликования на сайте Компании;
- декларирует подход компании к обеспечению информационной безопасности.

1.3 Для кого предназначен документ

Политика является общедоступной и предназначена для всех, кто пожелает ознакомиться с подходом Компании к обеспечению информационной безопасности.

2. Цели обеспечения и управления информационной безопасностью ООО «Мосье Башмаков»

Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность – в случае внесения в данные исключительно авторизированных изменений, доступность – при обеспечении возможности получения доступа к данным авторизированным лицам в нужное для них время.

Основными целями в области обеспечения и управления информационной безопасностью Компании являются:

- Обеспечение целостности, доступности и конфиденциальности критичной информации, а также обеспечение доступности критичных ИТ-сервисов Компании.
- Применение обоснованных, экономически эффективных организационных и технических мер по обеспечению информационной безопасности.
- Соответствие Компании требованиям действующего законодательства и регуляторов в области ИБ.
- Соответствие процессов обеспечения информационной безопасности бизнес-требованиям Компании.
- Обеспечение доверия клиентов и партнеров Компании.
- Установление ответственности сотрудников по вопросам обеспечения информационной безопасности и повышение их осведомленности.

3. Подход к обеспечению информационной безопасности

1. Информация является важным активом Компании и ее защита является обязанностью каждого сотрудника.

2. Доступ к информации предоставляется только лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально возможном объеме.
3. Для каждого информационного ресурса определяется владелец, отвечающий за предоставление к нему доступа и эффективное функционирование мер защиты информации.
4. Сотрудники Компании проходят регулярное обучение в области информационной безопасности.
5. В компании регулярно проводится независимый аудит информационной безопасности.
6. Специалисты информационной безопасности отвечают за определение детальных требований информационной безопасности и контролируют их исполнение в Компании.
7. Меры защиты информации внедряются по результатам проведения оценки рисков информационной безопасности.
8. Меры защиты персональных данных внедряются согласно требованиям Федерального закона №152 «О защите персональных данных» и других нормативных документов, регламентирующих обработку персональных данных в автоматизированных и неавтоматизированных информационных системах.
9. Оценка рисков информационной безопасности проводится ежегодно, а также в случае значительных изменений в структуре Компании и ее бизнес-процессах.
10. При оценке рисков учитывается влияние реализации угроз информационной безопасности на финансовое положение Компании и ее репутацию на рынке.
11. Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.
12. Система управления информационной безопасностью в Компании строится на основе международных стандартов ISO 27001. Компания сертифицирована по международному стандарту ISO 27001:2005 со следующей областью регистрации: Система управления информационной безопасностью в отношении обеспечения защиты информации в информационных системах и при осуществлении информационного обмена в рамках бизнес-процессов закупки цифровой, компьютерной техники и сопутствующих товаров, процесса управления продажами, включая продажи через интернет магазин, процесса управления предоставления сервиса, процесса управления логистическими операциями, процесса обеспечения маркетинговых операций, включая программу лояльности, процесса осуществления финансовых и бухгалтерских операций в соответствии с положением о применимости средств контроля ЗП-9 от 13.03.2012.
13. Успешное достижение целей настоящей политики возможно только при выполнении положений детальных регламентов информационной безопасности.

4. Порядок пересмотра Политики

Политика должна пересматриваться при наступлении существенных событий, но не реже, чем один раз в три года.