Иванов Егор БИСО-03-19

**Политика информационной безопасности**

Компания ООО «Донви»

Штат — 25 сотрудников.

3 - руководство, 3 - бухгалтерия, 5 — IT-отдел, 10 — менеджеры по работе с клиентами, 5 - отдел кадров, 4 — отдел безопасности.

Руководство компании использует телефонную связь, MS Office, 1С: Предприятие и т. д.

Бухгалтерия использует MS Office, 1С: Бухгалтерия. Занимается формированием полной и достоверной информации о деятельности организации и ее имущественном положении.

IT-отдел обеспечивает функционирование внутренней сети организации, а также сайта компании и личных кабинетов клиентов. Использует интернет, MS Office, 1С, сайт, языки программирования.

Менеджеры по работе с клиентами осуществляют работу с ними посредством Интернет. Телефонной связи и др.

Отдел кадров использует MS Office, 1С: Зарплата и Кадры. Обеспечивает предприятие необходимыми кадрами и эффективным использованием потенциала работников.

Отдел безопасности обеспечивает информационную безопасность компании, клиентам и работникам компании, используя MS Office, 1С, задействует различные ресурсы интернета.

**1. Общее положение**

Обеспечение информационной безопасности является необходимым условием для осуществления деятельности Компании. Нарушение информационной безопасности может привести к серьезным последствиям для Компании, включая потерю доверия со стороны партнеров, клиентов, поставщиков и снижение конкурентоспособности.

**1.1 Цель документа**

Целью политики информационной безопасности ООО «Донви» для размещения в сети интернет является декларация основных целей и положений по организации процессов обеспечения и управления информационной безопасностью Компании.

**2. Цели обеспечения и управления информационной безопасностью**

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 авторизованных изменений, доступность – при обеспечении возможности получения доступа к данным авторизованным 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**

- информация является важным активом Компании, ее защита является обязанностью каждого сотрудника.

- доступ к информации предоставляется только лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально возможном объеме.

- сотрудники Компании проходят регулярное обучение в области информационной безопасности.

- в Компании регулярно проводится независимый аудит информационной безопасности.

- специалисты информационной безопасности отвечают за определение детальных требований информационной безопасности и контролируют их исполнение в Компании.

- меры защиты информации внедряются по результатам проведения оценки рисков информационной безопасности.

- меры защиты персональных данных внедряются согласно требованиям Федерального закона «О защите персональных данных» и других нормативных документов, регламентирующих обработку персональных данных в автоматизированных и неавтоматизированных информационных системах.

- оценка рисков информационной безопасности проводится ежегодно, а также в случае значительных изменений в структуре Компании и ее бизнес-процессах.

- при оценке рисков учитывается влияние реализации угроз информационной безопасности на финансовое положение Компании и ее репутацию на рынке.

- стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.

- успешное достижение целей настоящей политики возможно только при выполнении положений регламентов информационной безопасности.

**4. Порядок пересмотра Политики**

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

**5. Технический регламент для отдела безопасности**

1) Исключение возможности доступа третьих лиц к документам, содержащим конфиденциальную информацию.

2) Контроль за соблюдением установленного уровня доступа внутри компании.

3) Соблюдение требований и правил по работе со средствами технической защиты, в том числе со средствами криптографической защиты.

4) Контроль состояния автоматизированной системы и реагирование на ситуации, имеющие характер инцидентов ИБ, а именно: нарушения целостности пломб, свидетельствующие о попытке проникнуть в охраняемую зону, некорректном срабатывании антивирусной защиты, нарушения в работе программного обеспечения, выявленных изменениях файлов, выходе из строя периферийных устройств.

5) Исключение копирования любых файлов или текстовой информации в любых целях без получения санкции руководителя.

6) Обеспечение антивирусной безопасности.

7) Обеспечение безопасности персональных данных. А именно:

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер.

- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.