ПЛАН РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

Дата утверждения: _____

Дата начала действия: _____

Цель:
Обеспечение эффективного и быстрого реагирования на различные инциденты ИБ и минимизации потенциальных ущербов, сохранения конфиденциальности целостности и доступности данных.

Определения и сокращения:
Компания – компания ООО «АВС»
Руководитель – руководитель компании ООО "АВС" (председатель правления)
ИБ – информационная безопасность
инцидент ИБ – инцидент информационной безопасности
отдел ИБ – отдел информационной безопасности **Компании**
сотрудник – сотрудник **Компании**

Общий порядок:

1. Выявление **инцидента ИБ**
   Инцидент ИБ может быть выявлен (обнаружен) SIEM-системой или сотрудником **Компании**

2. Регистрация и уведомление об **инциденте ИБ**
   В случаем выявления потенциального **инцидента ИБ** SIEM-системой событие регистрируется автоматически и уведомление об **инциденте ИБ** автоматически формируется для ответственного за **ИБ** (начальник **отдела ИБ**)
   В случае выявления потенциального **инцидента ИБ** сотрудником, обнаруживший обязан зарегистрировать данное событие (при наличии соответствующих прав или возможностей) либо сообщить в **отдел ИБ** (уведомить ответственного за **ИБ** (начальник **отдела ИБ**))

3. Оценка **инцидента ИБ**
   Оценка инцидента ИБ необходима для формирования рабочей группы для расследования и работы с **инцидентом ИБ**
   В случаем выявления **инцидента ИБ** SIEM-системой первичная оценка, классификация и формирование документа об **инциденте ИБ** происходит автоматически.
   В случае выявления **инцидента ИБ сотрудником Компании** после уведомления **отдела ИБ** ответственный за **ИБ** обязан дать первичную оценку, классификацию и подготовить документ о выявленном **инциденте ИБ**

4. Рабочая группа
   В зависимости от классификации инцидента и его характера, назначается ответственный сотрудник или рабочая группа
   Работа по реагированию на инцидент проводится в соответствии с предварительно разработанными процедурами.

5. Анализ и меры по управлению рисками
   Рабочей группой проводится анализ **инцидента ИБ**, определяются причины, масштаб и меры реагирования по управлению **инцидентом ИБ** для его пресечения, устранения и предотвращения повторения.

6. Документирование работы по управлению **инцидентом ИБ**
   Рабочая группа проводит анализ инцидента, фиксирует все детали и результаты реагирования;
   Предлагает меры улучшения для будущих ситуаций

Порядок реагирования на некоторые виды инцидентов:

- При выявлении вредоносного ПО на серверах компании
  - Инфицированные серверы должны быть немедленно изолированы от сети;
  - Процедура сканирования и удаления вредоносного ПО с зараженных серверов;
  - Восстановление данные с резервных копий;
  - Анализ причин инцидента;
  - Принятие мер для предотвращения повторных инцидентов.

Рабочая группа:

1. Ответственный за информационную безопасность (начальник отдела ИБ).
2. IT-специалисты **отдела ИБ**
3. IT-специалисты других отделов **Компании** (при необходимости)
4. Представители юридического и HR-отделов (при необходимости).

Данный план вступает в силу с момента его утверждения **Руководителем**.

Руководитель компании: _____
(подпись) (Иванов А. Г.)

Ответственный за исполнение: _____
(подпись) (Петров Б. В.)