«Утверждаю»

_____

«__» «_____» 20__ г.

ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА
УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Содержание

1 Назначение и область применения

1.1 Настоящая документированная процедура определяет порядок управления инцидентами информационной безопасности в Компании. Включает этапы от идентификации инцидента до его полного разрешения и принятия превентивных мер. Процесс охватывает все аспекты реагирования на инциденты, связанные с нарушением конфиденциальности, целостности и доступности информации, а также восстанавливает функционирование информационных систем в случае инцидентов.

1.2 Процедура применяется ко всем инцидентам, затрагивающим информационные активы организации, независимо от их источника (внутренний или внешний), включая события, влияющие на IT-инфраструктуру, данные, сети и бизнес-процессы..

2 Нормативные ссылки

2.1 В настоящей документированной процедуре использованы ссылки на следующие нормативные документы:

ISO/IEC 27001:2022	Информационные технологии, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования
ISO/IEC 27002:2022	Информационная безопасность, кибербезопасность и защита конфиденциальности. Управление информационной безопасностью
ISO/IEC 27035-1:2016	Управление инцидентами информационной безопасности. Часть 1: Принципы и процессы.
……..	……
……..	……

3 Термины и определения

Инцидент информационной безопасности (ИБ) — любое событие или серия событий,которые ставят под угрозу безопасность информационных активов, нарушая или пытаясь нарушить конфиденциальность, целостность или доступность информации.

Инцидент ИБ может включать:

- Несанкционированный доступ к информации.
- Потерю или повреждение данных.
- Атаки на информационные системы (например, вирусные или DDoS-атаки).
- Нарушение норм функционирования ИТ-систем.

Управление инцидентами ИБ — совокупность действий, направленных на выявление, регистрацию, классификацию, расследование, реагирование на инцидент и устранение его последствий.

Реагирование на инциденты — набор мер, направленных на нейтрализацию угрозы, минимизацию ущерба и восстановление нормального функционирования информационной системы.

Постинцидентное расследование — анализ инцидента для выяснения его причин и последствий с целью минимизации рисков возникновения подобных инцидентов в будущем**..**

4 Сокращения и обозначения

ИС — Информационная безопасность
ИБ — Инцидент информационной безопасности
СМИБ — Система менеджмента информационной безопасности
ЦОД — Центр обработки данных
ЗРК — Запрос на восстановление работы системы
CISO — Chief Information Security Officer (Руководитель службы информационной безопасности)
Служба ТП — Служба технической поддержки