«Утверждаю»

_____

«__» «_____» 20__ г.

ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА
ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Содержание

1 Назначение и область применения

1.1 Настоящая процедура определяет процессы и методы, используемые для обеспечения конфиденциальности данных в рамках информационных систем организации. Процедура охватывает мероприятия по защите персональной, корпоративной и конфиденциальной информации, циркулирующей в рамках информационных систем, включая физическую и логическую защиту, а также организационные меры для предотвращения несанкционированного доступа, утечек или утрат данных.

1.2 Процедура применяется ко всем информационным системам, включая серверы, базы данных, рабочие станции, а также приложения и сети, которые обрабатывают конфиденциальную информацию.

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 27018:2019	Защита персональных данных в облачных вычислениях.
……..	……
……..	……

3 Термины и определения

Конфиденциальность — свойство информации, при котором доступ к ней ограничен или контролируется.
Информационные системы — системы, обрабатывающие, хранящие или передающие информацию, в том числе компьютерные системы, сети, базы данных.
Данные — любые данные, включая личные, финансовые или коммерческие, относящиеся к организации или ее сотрудникам.
Неавторизованный доступ — доступ к данным или системе, осуществленный без разрешения или прав пользователя.

4 Сокращения и обозначения

ИС — информационные системы.
ПД — персональные данные.
ИБ — информационная безопасность.
КИ — конфиденциальная информация.

5 Ответственность и полномочия

Руководитель службы информационной безопасности отвечает за внедрение, контроль и регулярное обновление мероприятий по обеспечению конфиденциальности данных. Также он контролирует соответствие требованиям законодательства и стандартов ISO 27001.
Ответственные лица за обработку данных обязаны соблюдать правила доступа и защиты конфиденциальной информации, а также уведомлять о любых инцидентах, связанных с утечкой или компрометацией данных.
Администраторы информационных систем обеспечивают техническую защиту данных в рамках системы, включая шифрование, настройку прав доступа и мониторинг активности пользователей.

6 Требования

6.1 Оценка конфиденциальности данных

Проводится регулярная оценка данных на основе их конфиденциальности, включая идентификацию и классификацию данных по уровню важности и чувствительности.