

«Утверждаю»

\_\_\_\_\_

«\_» «\_\_\_\_\_» 20\_\_ г.

**РУКОВОДСТВО ПО  
СИСТЕМЕ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

## Содержание

1 Назначение .....	4
2 Общие положения .....	4
2.1 Область применения .....	4
2.2 Нормативные ссылки .....	4
3 Термины и определения, сокращения .....	4
4 Контекст организации.....	5
4.1 Описание контекста Компании.....	5
4.2 Заинтересованные стороны. Потребности и ожидания .....	5
4.3 Область действия системы менеджмента информационной безопасности .....	6
4.4 Система менеджмента информационной безопасности.....	6
5 Лидерство.....	7
5.1 Лидерство и обязательства руководства .....	7
5.2 Политика в области информационной безопасности .....	7
5.3 Организационные функции, ответственность и полномочия .....	8
6 Планирование. ....	9
6.1 Действия по обработке рисков и реализации возможностей.....	9
6.1.3 Обработка рисков информационной безопасности .....	10
6.2 Цели в области информационной безопасности и планирование их достижения .....	10
7 Обеспечение.....	10
7.1 Ресурсы.....	10
7.2 Компетентность .....	10
7.3 Осведомленность.....	10
7.4 Коммуникация .....	11
7.5 Документированная информация .....	11
7.5.1 Общие положения .....	11
8 Функционирование .....	12
8.1 Оперативное планирование и управление .....	12
8.2 Оценка рисков информационной безопасности.....	12
8.3 Обработка рисков информационной безопасности .....	12
9 Оценка результатов деятельности .....	12
9.1 Мониторинг, измерение, анализ и оценка .....	12
9.2 Внутренний аудит .....	12
9.3 Анализ менеджмента .....	13
10 Улучшение. ....	13
10.2 Непрерывное улучшение .....	13

Приложения .....	14
Лист регистрации изменений .....	15
Лист ознакомления.....	16

## 1 Назначение

Настоящее Руководство устанавливает единые требования к порядку управления информационной безопасностью в Компании, закрепляет полномочия и ответственность работников Компании, устанавливает общие направления и принципы деятельности для реализации в Компании системы менеджмента информационной безопасности (далее-СМИБ) в соответствии с требованиями международного стандарта ISO/IEC 27001:2022.

Настоящее Руководство вводится в действие со дня его утверждения.

## 2 Общие положения

### 2.1 Область применения

Требования настоящего Руководства распространяются на структурные подразделения Компании, к информационным активам и процессам, подпадающим в область действия СМИБ, описанной в документе «Область действия системы управления информационной безопасностью Компании».

Контроль за выполнением требований настоящего Руководства несет руководитель Рабочей группы СМИБ.

Ответственность за управление и соответствие требований настоящего Руководства требованиям нормативных правовых актов Республики Казахстан, нормативных документов несет Менеджер информационной безопасности.

Руководители структурных подразделений, входящих в Область действия СМИБ, несут ответственность за выполнение требований настоящего Руководства.

## 2 Нормативные ссылки

2.1 В настоящем Руководстве по СМИБ приведены ссылки на внешние и внутренние нормативные документы в соответствии с:

- Перечнями внешней нормативной документации компании и ее структурных подразделений;
- Контрольным перечнем основной документации СМИБ /Контрольным перечнем внутренних нормативных документов Компании.

## 3 Термины и определения, сокращения

В настоящем руководстве использованы термины в соответствии с определениями предусмотренными Глоссарием интегрированной системы менеджмента.

В дополнение к ним в настоящем руководстве предусмотрены следующие термины, определения и сокращения:

**ВНД** – внутренний нормативный документ;

**ДУП** - Департамент по управлению персоналом;

**ИА** – информационный актив;

**ИБ** – информационная безопасность;

**ИС** – информационная система;

**КЦД** – конфиденциальность, целостность, доступность;

**РИБ** – риски информационной безопасности;

**СМИБ** – система управления информационной безопасностью

**ПРПД** – цикл «Планирование-Реализация-Проверка-Действие».