Политика информационной безопасности ОО «ACCREDITATION CENTER FOR QUALITY IN HEALTHCARE» (ACQH)»

Разработчик	Должность	Ф.И.О.	Подпись
	Руководитель Центра корпоративной поддержки и ресурсного обеспечения	Султангожина Д.К.	
Согласовано	Исполнительный директор	Жаркенов Е.А.	

Утверждено приказом Председателя Объединения Каупбаевой Б.Т. от 10 декабря 2024 года № 198

Дата	Номер регистрации	Версия	Дата пересмотра
10.12.2024	2024-017 (1)	4	10.12.2027

г. Астана, 2024 год

1. Общие положения

1. Политика информационной безопасности (далее–Политика) разработана в соответствии с Постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» и внутренними нормативными документами (далее–ВНД) ОО «ACCREDITATION CENTER FOR QUALITY IN HEALTHCARE» (ACQH)» (далее – Объединение).

2. В настоящей политике информационной безопасности (далее - ИБ) определен комплекс мер по предотвращению, обнаружению и решению проблем с целью защиты целостности, конфиденциальности и доступности обрабатываемых данных на объектах информатизации Объединении.

3. Политика является документом первого уровня технической документации по ИБ и определяет цели, задачи, руководящие принципы и практические приемы в области обеспечения ИБ.

4. Настоящая Политика разработана в соответствии с:

1) Законом Республики Казахстан от 24 ноября 2015 года «Об информатизации»;

2) Законом Республики Казахстан от 21 мая 2013 года «О персональных данных и их защите»;

3) Законом Республики Казахстан от 16 ноября 2015 года «О доступе к информации»;

4) Законом Республики Казахстан от 7 января 2003 года «Об электронном документе и электронной цифровой подписи»;

5) Постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении Единых требований в области информационно-коммуникационных технологий и обеспечении информационной безопасности» и другими нормативно-правовыми и техническими актами в области ИБ.

2. Термины и определения

5. В Политике используются следующие основные термины и определения:

1) информационная безопасность в сфере информатизации (далее – информационная безопасность) – состояние защищенности электронных

информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

2) ответственный сотрудник за информационную безопасность (далее – ответственный за ИБ) – сотрудник Объединения, назначенный приказом и занимающийся вопросами обеспечения информационной безопасности объектов информатизации Объединении и подчиняющийся непосредственно Председателю Объединения;

3) объекты информатизации – электронные информационные ресурсы, программное обеспечение, интернет-ресурс и информационно-коммуникационная инфраструктура Объединении;

4) инцидент информационной безопасности – отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов;

5) журналирование событий – процесс записи информации о происходящих с объектом информатизации программных или аппаратных событиях в журнал регистрации событий;

6) внутренний аудит информационной безопасности – объективный, документированный процесс контроля качественных и количественных характеристик текущего состояния информационной безопасности объектов информатизации в Объединении.

7) пользователь – субъект информатизации, использующий объекты информатизации для выполнения конкретной функции и (или) задачи.

3. Цель политики

6. Целью Политики является:

1) определение технических и процедурных мер для обеспечения исполнения нормативно-правовых актов и ВНД в области ИБ;

2) определение средств, позволяющих обеспечить безопасность, а также предотвратить несанкционированный доступ, изменение, публикацию, удаление и повреждение обрабатываемых данных;

3) обеспечение непрерывности основных процессов Объединении для сохранения стабильности функционирования объектов информатизации;

4) минимизация возможных потерь и ущерба от нарушений в области ИБ.

7. Основными направлениями обеспечения ИБ являются: