КОРПОРАТИВНЫЙ УНИВЕРСИТЕТ
САМРУК-КАЗЫНА

ПОЛИТИКА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЧУ «Корпоративный университет «Самрук-Казына»

1. Введение

1.1. Корпоративный университет (далее – Учреждение) декларирует свою приверженность целям информационной безопасности при осуществлении своей деятельности, как во внутренних процессах, так и при взаимодействии с внешними сторонами.

1.2. В рамках обеспечения информационной безопасности поддерживаются главные атрибуты информации:

1) Конфиденциальность – это гарантия, что информация может быть прочитана и проинтерпретирована только теми людьми и процессами, которые авторизованы это делать. Обеспечение конфиденциальности включает процедуры и меры, предотвращающие раскрытие информации неавторизованными пользователями.

2) Целостность – это гарантия того, что информация остается неизменной, корректной и аутентичной. Обеспечение целостности предполагает предотвращение и определение неавторизованного создания, модификации или удаления информации.

3) Доступность – это гарантирование того, что авторизованные пользователи могут иметь доступ и работать с информационными активами, ресурсами и системами, которые им необходимы, при этом обеспечивается требуемая производительность. Обеспечение доступности включает меры для поддержания доступности информации, несмотря на возможность создания помех, включая отказ системы и преднамеренные попытки нарушения доступности.

2. Цели и измерения достижения целей

2.1. Целями информационной безопасности Учреждения являются:

1) обеспечение всесторонней защиты интересов Учреждения, его контрагентов, а также работников от угроз в сфере информационных технологий;

2) создание, поддержка, контроль и развитие эффективной системы менеджмента информационной безопасности (далее - СМИБ), основывающейся на сбалансированном комплексе организационных и технических мер по обеспечению информационной безопасности в соответствии с требованиями международного стандарта ISO/IEC 27001:2013;

3) защита интеллектуальной собственности, персональных данных и иной конфиденциальной информации;

4) минимизация возможных потерь и/или ущерба от инцидентов информационной безопасности;

5) развитие корпоративной культуры в области информационной безопасности.

6) обеспечение непрерывного и результативного подхода к управлению инцидентами информационной безопасности, включая сообщения о событиях безопасности и слабые стороны;

7) уменьшение до приемлемого уровня возможного ущерба Учреждения при реализации угроз информационной безопасности, в том числе сокращение времени восстановления бизнес-процессов после возможных прерываний;

8) обеспечить как минимум 99,5% времени безотказной работы;

9) минимизировать количество срабатываний ложных инцидентов до 5%;

2.2. Для достижения целей обеспечения информационной безопасности Учреждение обеспечивает эффективное решение следующих задач:

1) разработка мер по управлению рисками информационной безопасности (включая как методологические, ручные, так и автоматизированные средства контроля);

2) внедрение и настройка средств защиты информации;

3) мониторинг и обработка событий и инцидентов информационной безопасности;

4) своевременное выявление и устранение уязвимостей активов Компании и тем самым предупреждение возможности нанесения ущерба и нарушения нормального функционирования бизнес-процессов Компании в результате реализации угроз информационной безопасности;

5) обучение персонала Учреждения в области информационной безопасности;

5) проведение ежегодного анализа и оценки результатов измерений на предмет достижения поставленных целей ИБ;

6) пересмотр целей ИБ периодичносью в год;

2.3. При обеспечении информационной безопасности Корпоративный университет руководствуется следующими принципами:

1) законность;
2) процессный подход;
3) комплексное использование способов, методов и средств защиты;
4) следование лучшим практикам;
5) разумная достаточность;
6) персональная ответственность.

3. Роли и обязанности

3.1. **Руководство Учреждения** обеспечивает СМИБ всеми необходимыми ресурсами;

3.2. **Менеджер по информационной безопасности во главе с Руководством Учреждения** обеспечивают:

работоспособность СМИБ в соответствии с настоящей Политикой;

распространение Политики, ознакомление всех сотрудников Учреждения, а также всех соответствующих внешних сторон с настоящей Политикой;

пересмотр СМИБ не реже чем один раз в год или каждый раз, когда происходят значительные изменения с целью установления пригодности, адекватности и эффективности СМИБ.

3.3. **Руководители структурных подразделений** обеспечивают адаптацию и реализацию Плана обучения и повышения осведомлённости сотрудников.

3.4. **Владельцы активов** обеспечивают защиту конфиденциальности, целостности и доступности своих активов.

Иные роли, распределение обязанностей и ответственность определены в документах СМИБ.

4. Поддержка СМИБ

Настоящим Руководство Учреждения заявляет, что внедрение и постоянное улучшение СМИБ будет поддерживаться адекватным ресурсами с целью достижения всех заявленных в данной Политике целей, а также с целью соблюдения всех идентифицированных технологий.

5. Непрерывность бизнеса

Процесс управления непрерывностью бизнеса определен в документе **МИБ-ПР-07** «Правила обеспечения непрерывности деятельности».

6. Меры безопасности

Выбранные меры безопасности и статус их внедрения определены в «Положении о применимости».

7. Требования информационной безопасности

Настоящая политика, как и СМИБ в целом, должны соответствовать правовыми и нормативными требованиями, имеющими отношение в сфере информационной безопасности, а также договорным обязательствами.

Список правовых и нормативных требований:

1) Международный стандарт ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. (Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования.);

2) Международный стандарт ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls. (Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации.);

3) Методология COBIT (Control Objectives for Information and Related Technologies), (Задачи управления для информационных и смежных технологий);

4) РК-02 - Руководство по ИБ;

5) МИБ-ПК-01 - Процедура «Оценка и улучшение СМИБ» с двумя приложениями (анализ со стороны руководства и аудит СМИБ);

6) ПРК-ПР-07 – Правила управления рисками;
7) МИБ-ПР-01 (В) – Правила ИБ;
8) МИБ-ПР-02 – Управление сетевыми устройствами;
9) МИБ-ПР-03 - Правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации;
10) МИБ-ПР-04 - Правила управления доступом в информационные системы;
11) МИБ-ПР-05 - Правила организации физического доступа;
12) МИБ-ПР-06 - Правила управления инцидентами;
13) МИБ-ПР-07 - Правила обеспечения непрерывности деятельности;
14) МИБ-ПР-08 - Правила управления изменениями;
15) МИБ-ПР-09 - Правила обеспечения информационной безопасности при работе с поставщиками.

Директор **А. Кадырбаева**

12.07.2021г.