Приложение 1
к приказу и.о.Ректора
ТОО «Astana IT University»
от «03» 02 2026 года
№ 46-П

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТОО «ASTANA IT UNIVERSITY»

ГЛАВА 1. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

1.1. Термины и определения:

1) Информационная безопасность (ИБ) - состояние защищенности информации и инфраструктуры от угроз, обеспечивающее конфиденциальность, целостность и доступность;

2) Система управления информационной безопасностью (СУИБ) - совокупность политик, процессов, ролей и мер, направленных на управление рисками ИБ и обеспечение выполнения требований ИБ;

3) Информационный актив - данные, информационные системы, сервисы, оборудование, носители, учетные записи, ключи и иные ресурсы, имеющие ценность для Университета и подлежащие защите;

4) Владелец актива - руководитель подразделения/уполномоченное лицо, ответственное за определение требований к защите актива и согласование доступа;

5) Инцидент ИБ - событие, приводящее или способное привести к нарушению требований ИБ (например, утечка, несанкционированный доступ, вредоносное ПО, отказ сервиса, компрометация учетной записи);

6) Персональные данные (ПДн) - сведения, относящиеся к определенному или определяемому субъекту персональных данных, в соответствии с законодательством РК;

7) Критически важные информационные системы - системы, нарушение доступности/целостности/конфиденциальности которых может существенно повлиять на деятельность Университета (например, LMS, DU, Learn, СЭД и т.п. - по перечню, установленному Университетом);

8) Доступ - разрешенные действия пользователя/процесса в отношении информационного актива (чтение, изменение, удаление, администрирование и др.);

9) Учетная запись - уникальная идентификационная запись пользователя/сервиса в информационной системе.

1.2. Сокращения:

1) AITU - ТОО «Astana IT University»;
2) ИБ - информационная безопасность;
3) СУИБ - система управления информационной безопасностью;
4) ПДн - персональные данные;
5) ОИБЦР - Офис информационной безопасности и цифровых рисков;
6) ДТОС - Департамент технического обеспечения и сопровождения;
7) ДЦРР - Департамент цифровых решений и разработки;
8) ЦОД - центр обработки данных;
9) СКУД - система контроля и управления доступом;
10) RBAC - Role-Based Access Control (ролевая модель управления доступом);
11) MFA - Multi-Factor Authentication (многофакторная аутентификация);
12) DLP - Data Loss Prevention (предотвращение утечек данных);
13) BYOD - Bring Your Own Device (использование личных устройств);
14) NGFW - Next-Generation Firewall (межсетевой экран нового поколения);
15) IPS - Intrusion Prevention System (предотвращение вторжений);
16) VPN - Virtual Private Network (виртуальная частная сеть);
17) TLS/SSL - протоколы криптографической защиты трафика;
18) ЭЦП - электронная цифровая подпись;
19) НУЦ РК - Национальный удостоверяющий центр Республики Казахстан.

ГЛАВА 2. ОБЩИЕ ПОЛОЖЕНИЯ.

2.1. Назначение документа:

Настоящая Политика информационной безопасности (далее - Политика) является документом первого уровня в иерархии внутренних нормативных документов ТОО «Astana IT University» (далее - Университет). Политика декларирует цели, задачи, принципы и требования к обеспечению информационной безопасности (ИБ), обязательные для исполнения всеми

сотрудниками, обучающимися и контрагентами Университета.

2.2. Нормативная база

Политика разработана в соответствии с требованиями:

1. Закона Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации».
2. Закона Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите».
3. Постановления Правительства РК от 20 декабря 2016 года № 832 «Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности» (далее – ЕТ №832).
4. Национального стандарта СТ РК ISO/IEC 27001-2022 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

2.3. Область действия (Периметр защиты)

Действие настоящей Политики распространяется на все информационные активы Университета, расположенные:

- В главном учебном корпусе (г. Астана, пр. Мангилик Ел, 55/11, БЦ EXPO, блок C1);
- В выставочном центре (учебный корпус, 3 этаж) пр. Мангилик Ел, 53/1;
- В общежитиях (Дома студентов №1, 2, 3, 4 по пр. Кабанбай батыра);
- В Центре обработки данных (ЦОД), расположенном по ул. Космонавтов, 62;
- В облачных инфраструктурах, используемых Университетом (Microsoft 365, хостинг ps.kz).

Субъектами Политики являются:

- Руководство Университета;
- Штатные сотрудники всех департаментов и школ;
- Профессорско-преподавательский состав (ППС);
- Обучающиеся (студенты, магистранты, докторанты);
- Третьи лица (поставщики услуг, партнеры), имеющие доступ к инфраструктуре AITU.

ГЛАВА 3. ЦЕЛИ И ЗАДАЧИ СИСТЕМЫ УПРАВЛЕНИЯ ИБ (СУИБ).

3.1. Стратегическая цель

Обеспечение устойчивого функционирования цифровой экосистемы Университета, защита репутации AITU как ведущего IT-вуза региона и гарантия безопасности данных студентов и сотрудников.

3.2. Основные свойства защищаемой информации

СУИБ Университета направлена на обеспечение:

- Конфиденциальности: защита от несанкционированного доступа к персональным данным (ПДн), экзаменационным материалам, финансовой отчетности и коммерческой тайне.
- Целостности: защита от несанкционированной модификации или уничтожения данных в ключевых системах (LMS Moodle, DU, My-DU, Learn, СЭД, Abitur,1С: Предприятие).
- Доступности: гарантия своевременного доступа авторизованных пользователей к сервисам (Web-сайт, электронная почта, Интернет) в режиме 24/7, особенно в критические периоды (приемная кампания, сессия).

3.3. Ключевые показатели эффективности (KPI) ИБ

Эффективность реализации Политики оценивается по следующим метрикам:

1. Отсутствие инцидентов ИБ, повлекших утечку ПДн более 10 субъектов — 0 случаев в год.
2. Время простоя критически важных систем (LMS, DU, Learn) по причине инцидентов ИБ — не более 4 часов в месяц.
3. Охват рабочих станций средствами антивирусной защиты и актуальными обновлениями — 100%.
4. Устранение критических уязвимостей периметра сети - в течение 72 часов с момента обнаружения.

3.4. Защита персональных данных

3.4.1. Университет, являясь собственником и оператором баз, содержащих персональные данные (далее - ПДн), обеспечивает их защиту от неправомерного доступа, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в соответствии с Законом РК № 94-V.

3.4.2. Обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора.

3.4.3. Эффективность процессов защиты ПДн оценивается по следующим ключевым показателям (KPI):

1) Обработка обращений: 100% обращений субъектов (студентов, сотрудников) и их законных представителей обрабатываются в сроки, установленные законодательством РК (не более 3 рабочих дней для ответа на запрос о наличии/состоянии ПДн).

2) Утечки данных: Полное отсутствие (0 инцидентов) подтвержденных фактов утечки, незаконной передачи или публикации ПДн третьим лицам.

3) Соблюдение законодательства: Отсутствие предписаний и штрафных санкций со стороны уполномоченного органа (МЦРИАП, КИБ) по фактам нарушения требований законодательства о защите ПДн.

ГЛАВА 4. ОРГАНИЗАЦИОННАЯ СТРУКТУРА И ОТВЕТСТВЕННОСТЬ.

4.1. Правление (Management Board)

- Утверждает стратегию развития ИТ и ИБ.
- Выделяет бюджет на обеспечение ИБ.
- Принимает решения по рискам, превышающим допустимый уровень.

4.2. Председатель Правления – Ректор

- Является владельцем системы управления информационной безопасностью (СУИБ) и несет персональную ответственность за состояние информационной безопасности в Университете в соответствии с Законом Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V и Постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832.
- Утверждает настоящую Политику и назначает ответственных лиц.

4.3. Советник ректора по обеспечению безопасности

- Участвует в работе коллегиальных органов и рабочих групп Университета по вопросам обеспечения безопасности, в том числе информационной безопасности и кибербезопасности.
- Координирует взаимодействие структурных подразделений Университета с уполномоченными государственными органами по вопросам ИБ, кибербезопасности и защиты персональных данных (в пределах компетенции Университета).
- Организует подготовку и согласование ответов на запросы государственных органов, а также сопровождение проверок и иных контрольных мероприятий по вопросам ИБ совместно с ОИБЦР.
- Информирует Ректора и Правление о значимых рисках и инцидентах ИБ, требующих управленческих решений.

4.4. Проректор по цифровизации

- Курирует вопросы цифровой трансформации и кибербезопасности.
- Курирует деятельность профильных ИТ-подразделений и ОИБЦР в части реализации требований информационной безопасности.
- Представляет отчеты по состоянию ИБ на заседаниях Правления.

4.5. Департамент технического обеспечения и сопровождения (ДТОС)

- Обеспечение бесперебойной работы и эксплуатация инфраструктуры.
- Сопровождение цифровых платформ и сервисов.
- Обеспечивает резервное копирование и восстановление данных.
- Ведение учета компьютерной техники, периферии и участие в инвентаризации.
- Установка, настройка рабочих мест сотрудников, обновление ПО и замена оборудования.

4.6. Офис информационной безопасности и цифровых рисков (ОИБЦР)

- Обеспечивает независимый контроль, мониторинг и методологическое сопровождение (вторая линия защиты) по вопросам информационной безопасности.
- Организует и координирует процесс управления рисками ИБ (методология, критерии, контроль исполнения), совместно с владельцами активов и профильными подразделениями.

- Осуществляет мониторинг событий/инцидентов ИБ и координирует расследование и реагирование (в пределах компетенции Университета).
- Определяет требования к управлению учетными записями и правами доступа; техническое создание/изменение учетных записей выполняется ДТОС по согласованным заявкам.
- Организует обучение сотрудников вопросам ИБ.
- Контролирует корректность предоставления и актуальности прав доступа; согласует исключения и повышенные права доступа в установленном порядке.

4.7. Департамент цифровых решений и разработки (ДЦРР)

- Безопасная разработка, управление изменениями, устранение уязвимостей в ПО/сервисах.
- Разработка и цифровизация внутренних сервисов и платформ Университета
- Устранение выявленных уязвимостей и ошибок в разрабатываемых системах
- Обеспечение корректной интеграции цифровых сервисов с внутренними и внешними информационными системами

4.8. Владельцы бизнес-процессов (информационных активов)

Руководители структурных подразделений (владельцы информационных активов и бизнес-процессов: офис регистратора, бухгалтерия, академические и административные подразделения, школы и др.) несут ответственность за определение требований к доступу и конфиденциальности информации в рамках своей зоны ответственности.

- Определяют требования к конфиденциальности своих данных.
- Согласовывают предоставление доступа сотрудникам к своим системам.
- Руководители структурных подразделений (владельцы ресурсов) оформляют и согласовывают заявки на предоставление/изменение/отзыв доступа к своим системам и данным; учетные записи и роли в корпоративных сервисах (например, AD, Microsoft 365 и др.) предоставляются по принципу минимально необходимого доступа.
- Департамент управления человеческими ресурсами (HR) обязан уведомлять ОИБЦР и ДТОС о кадровых событиях (прием, увольнение,

перевод, длительное отсутствие) не позднее 1 рабочего дня с момента издания кадрового приказа/распоряжения, чтобы обеспечить своевременное предоставление или отзыв прав доступа.

Отзыв/блокирование/аннулирование прав доступа выполняется по основанию кадрового события или по заявке владельца актива; ОИБЦР контролирует корректность и полноту отзыва, ДТОС обеспечивает техническое исполнение.

Контроль полноты и своевременности отзыва прав доступа осуществляется ОИБЦР в рамках реализации требований настоящей Политики.

ГЛАВА 5. КЛАССИФИКАЦИЯ ИНФОРМАЦИИ И УПРАВЛЕНИЕ АКТИВАМИ.

5.1. Все информационные ресурсы Университета подлежат классификации по трем уровням конфиденциальности:

1. «Общедоступная информация»: Данные, предназначенные для неограниченного круга лиц (информация на сайте astanait.edu.kz, расписание занятий, новости). Потеря конфиденциальности ущерба не несет.

2. «Для служебного пользования» (ДСП): Внутренняя документация, методические материалы, переписка, проекты решений. Доступ разрешен только сотрудникам. Утечка может нанести репутационный или незначительный материальный ущерб.

3. «Конфиденциальная информация»: Персональные данные, сведения о заработной плате, содержание экзаменационных билетов до экзамена, пароли администраторов, закрытые ключи ЭЦП. Доступ строго ограничен. Утечка влечет юридическую ответственность и значительный ущерб.

5.2. Инвентаризация активов

5.2.1. ДТОС ведет и поддерживает в актуальном состоянии Реестр активов, включающий аппаратное обеспечение (серверы, АРМ), программное обеспечение (лицензии) и информационные ресурсы. Владельцы активов (руководители структурных подразделений) обязаны своевременно (в срок не позднее 3 рабочих дней) уведомлять ДТОС о любых изменениях в составе, местоположении или статусе вверенных им активов (приобретение,

перемещение, списание, модернизация) для внесения изменений в Реестр. Плановая инвентаризация информационных активов проводится не реже 1 раза в год.

ГЛАВА 6. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ: ОСНОВНЫЕ ДОМЕНЫ.

6.1. Управление доступом

6.1.1. Доступ к информационным системам предоставляется на основе ролевой модели (RBAC) по принципу «минимально необходимых привилегий».

6.1.2. Процедура предоставления доступа: Заявка руководителя -> Согласование (ОИБЦР/Владелец ресурса) -> Исполнение (ДТОС).

6.1.3. Парольная политика:

- Минимальная длина пароля — 10 символов;
- Обязательное наличие букв в разном регистре, цифр и спецсимволов;
- Смена пароля — не реже 1 раза в 90 дней;
- Блокировка учетной записи после 5 неудачных попыток ввода.
- Периодический пересмотр прав доступа проводится владельцами ресурсов совместно с ОИБЦР не реже 1 раза в квартал; результаты фиксируются (журнал/акт).
- При переводе/изменении функциональных обязанностей выполняется пересмотр прав: удаление неактуальных ролей и назначение новых — в срок не позднее 24 часов с момента кадрового решения.
- Отзыв (деактивация) учетных записей и прав доступа при увольнении/расторжении договора выполняется автоматически по уведомлению HR и/или заявке руководителя — в срок не позднее 24 часов; для критических систем и удаленного доступа — немедленно (в день увольнения).
- Для обучающихся деактивация, изменение или предоставление учетных записей и прав доступа осуществляется на основании официальных уведомлений Студенческого департамента и/или Департамента академической деятельности о зачислении, отчислении, переводе, восстановлении или изменении статуса студента.

Предоставление доступа выполняется в день зачисления, а отзыв (деактивация) учетных записей и прав доступа — в день отчисления или перевода, при этом доступ к критическим системам и внешним ресурсам подлежит немедленному прекращению.

- Выдача и изменение доступа выполняются только на основании заявки руководителя и/или кадрового события (прием, перевод, временное замещение) с согласованием владельца ресурса и ОИБЦР

6.1.4. Многофакторная аутентификация (MFA) является обязательной для:

- Всех административных учетных записей (доменных и локальных администраторов);
- Удаленного доступа (VPN, VDI);
- Доступа к корпоративной электронной почте и облачным сервисам извне периметра сети;
- Критически важных информационных систем.

6.2. Сетевая безопасность и защита от вредоносного ПО

6.2.1. Периметр сети защищается межсетевыми экранами нового поколения (NGFW) с функциями IPS (предотвращение вторжений) и веб-фильтрации.

6.2.2. Доступ к категориям интернет-ресурсов «Азартные игры», «Порнография», «Вредоносное ПО», «Анонимайзеры/прокси», «Торренты (P2P)» запрещается и подлежит технической блокировке средствами защиты/фильтрации. По решению (согласованию) Ректора и на основании служебной необходимости может быть установлен дополнительный запрет на иные информационные ресурсы (в т.ч. отдельные сайты/домены/сервисы) в целях обеспечения информационной безопасности и снижения рисков.

6.2.3. Беспроводная сеть (Wi-Fi) сегментирована на отдельные логические/сетевые сегменты (VLAN/VRF) с межсетевым разделением (FW/ACL) и запретом lateral movement:

• AITU-Staff — для сотрудников (желательно 802.1X), доступ к внутренним ресурсам по принципу минимальных привилегий;

• AITU-Student — изолированный сегмент, доступ только в Интернет и утвержденные учебные сервисы (LMS/DU/Learn); доступ Student → Staff и к внутренним сервисам запрещен;

• AITU-Guest — полностью изолированный сегмент, только Интернет (captive portal при необходимости). Для BYOD применяются базовые меры

контроля (актуальные обновления, пароль/биометрия, при возможности — MDM/условный доступ).

6.2.4. На всех рабочих станциях и серверах в обязательном порядке используется централизованная антивирусная защита. Отключение антивируса пользователями запрещено.

6.2.5. По решению Руководства Университета/Ректора могут быть внедрены информационные системы класса DLP (Data Loss Prevention) для предотвращения утечек и контроля передачи служебной (ДСП) и/или конфиденциальной информации, включая персональные данные, через электронную почту, веб-сервисы, мессенджеры, съемные носители и иные каналы. Порядок внедрения и эксплуатации DLP определяется отдельными внутренними регламентами в соответствии с требованиями ЕТ №832 и законодательства РК.

6.3. Криптографическая защита

6.3.1. Передача конфиденциальной информации по открытым каналам связи (Интернет) допускается только в зашифрованном виде (протоколы SSL/TLS, IPsec VPN).

6.3.2. Веб-ресурсы Университета должны быть защищены сертификатами TLS. Использование устаревших и небезопасных версий протоколов (SSL 2.0/3.0, TLS < 1.2) запрещено.

6.3.3. Для обеспечения юридической значимости электронных документов и строгой аутентификации используются ключи ЭЦП НУЦ РК. Ключи руководства и главного бухгалтера хранятся на защищенных носителях (токенах).

6.3.4. Шифрование данных «на хранении» (encryption at rest): базы данных, серверные диски/тома и резервные копии, содержащие ПДн, ДСП или конфиденциальную информацию, должны быть защищены шифрованием (TDE/шифрование томов/хранилищ, шифрование backup) и разграничением доступа к ключам. Ключи шифрования хранятся в защищенных хранилищах и доступны только уполномоченным администраторам.

6.4. Физическая безопасность

6.4.1. Доступ в критически важные помещения (ЦОД, серверные, кроссовые) строго ограничен. Вход осуществляется по электронным пропускам (СКУД) только для сотрудников ДТОС и ОИБЦР.

6.4.2. Серверные помещения оборудуются системами кондиционирования, бесперебойного питания, пожаротушения и видеонаблюдения.

6.4.3. Вынос компьютерной техники за пределы территории Университета осуществляется только по оформленному материальному пропуску.

6.4.4 Вынос служебных портативных устройств (ноутбуки, планшеты, внешние носители), содержащих информацию категории «Для служебного пользования» (ДСП) и/или «Конфиденциальная информация» (включая персональные данные), допускается только при условии использования полного дискового шифрования (BitLocker, FileVault и аналоги) и применения средств контроля доступа к устройству (PIN/пароль/биометрия).

6.5. Резервное копирование и непрерывность

6.5.1. Резервному копированию по расписанию (Full + Incremental) подлежат все критически важные данные Университета, включая, но не ограничиваясь:

- Базы данных систем (1С, СЭД, LMS);
- Конфигурационные файлы сетевого оборудования и серверов;
- Иные программные продукты и информационные системы, введенные в эксплуатацию, которые содержат служебную, конфиденциальную информацию или персональные данные.
- Файловые хранилища подразделений.

6.5.2. Используется специализированная система резервного копирования виртуальных средств. Глубина хранения оперативных копий — не менее 7–14 дней; архивных (долгосрочных) копий — не менее 30–90 дней (в зависимости от критичности системы и требований регулятора/бизнеса). Рекомендуется наличие как минимум одной неизменяемой (immutable) или офлайн-копии для защиты от вирусов-шифровальщиков.

6.5.3. Резервные копии должны храниться изолированно от основной продуктивной сети для защиты от вирусов-шифровальщиков.

6.6. Мобильные устройства и BYOD (Bring Your Own Device)

6.6.1. Использование личных устройств (смартфонов, ноутбуков) сотрудников и обучающихся для доступа к информационным ресурсам Университета (почта, LMS, Teams) допускается при соблюдении базовых требований безопасности:

1) Наличие пароля/PIN-кода или биометрической аутентификации для разблокировки устройства;

2) Использование поддерживаемых версий ОС с актуальными

обновлениями безопасности.

6.6.2. В случае утери или кражи личного устройства, имеющего доступ к корпоративным данным, пользователь обязан незамедлительно уведомить ОИБЦР для блокировки доступа и удаленного стирания корпоративных данных (при наличии технической возможности).

6.7. Взаимодействие с поставщиками и использование облачных услуг

6.7.1. При выборе поставщиков ИТ-услуг, облачных провайдеров и разработчиков ПО учитываются требования информационной безопасности.

6.7.2. В договорах с поставщиками, имеющими доступ к инфраструктуре или данным Университета, должны быть зафиксированы:

1) Обязательства по соблюдению конфиденциальности (NDA);
2) Требования к обеспечению безопасности данных;
3) Право Университета на проведение аудита ИБ поставщика;
4) Ответственность за инциденты ИБ, произошедшие по вине поставщика.

6.7.3. Использование облачных сервисов (IaaS, PaaS, SaaS) допускается только после оценки рисков и согласования с ОИБЦР.

6.8. Безопасность разработки и управления изменениями

6.8.1. Департамент цифровых решений и разработки (ДЦРР) обеспечивает жизненный цикл ПО (LMS, порталы, приложения) в соответствии с принципами «Secure by Design». В исходном коде обязательны: валидация данных (защита от инъекций), запрет передачи сессий в URL, использование защищенных хранилищ секретов (Vault) вместо hardcode, проверка прав доступа на стороне сервера и детальное журналирование событий безопасности.

6.8.2. Среды разработки, тестирования и промышленной эксплуатации должны быть логически разделены. Для тестирования запрещено использование реальных персональных данных; должны применяться только обезличенные (маскированные) или синтетические данные.

6.8.3. Любые изменения в продуктивных системах производятся только после успешного тестирования. Приемка ПО в промышленную эксплуатацию без прохождения сканирования на уязвимости и устранения критических замечаний ОИБЦР запрещена.

ГЛАВА 7. УПРАВЛЕНИЕ РИСКАМИ И ИНЦИДЕНТАМИ.

7.1. Управление рисками

7.1.1. Университет применяет качественную методику оценки рисков ИБ.

7.1.2. Оценка рисков проводится на регулярной основе (раз в год), а также при внедрении новых систем.

7.1.3. Риски уровней «Высокий» и «Критический» подлежат обязательной обработке (внедрению мер защиты).

7.2. Управление инцидентами

7.2.1. Любой сотрудник или студент, обнаруживший признаки нарушения ИБ (вирус, странное поведение ПК, утеря пропуска, фишинг), обязан незамедлительно сообщить об этом напрямую в ОИБЦР.

7.2.2. Сокрытие факта инцидента влечет дисциплинарную ответственность.

7.2.3. В случае выявления фактов намеренного нарушения ИБ студентами (попытки взлома, несанкционированный доступ, деструктивные действия в сети), ОИБЦР инициирует процедуру немедленного отчисления указанных студентов в соответствии с Уставом Университета.

7.2.4. ОИБЦР ведет Журнал регистрации инцидентов, проводит детальный анализ причин и разрабатывает обязательные к исполнению рекомендации для предотвращения повторения инцидентов.

ГЛАВА 8. КОНТРОЛЬ И АУДИТ.

8.1. Внутренний аудит ИБ проводится не реже одного раза в год по утвержденному плану. Аудит организует ОИБЦР; при необходимости может привлекаться комиссия, назначенная Ректором, и/или внешние аудиторы по решению Правления.

8.2. Внешний аудит и аттестация на соответствие требованиям ИБ проводятся в случаях, предусмотренных законодательством РК.

8.3. Руководители подразделений обязаны оказывать содействие

аудиторам и предоставлять необходимую информацию.

ГЛАВА 9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ.

9.1. Настоящая Политика вступает в силу с момента ее утверждения.

9.2. Ознакомление всех сотрудников с Политикой производится отделом кадров (HR) при приеме на работу под роспись.

9.3. Актуализация Политики производится по мере необходимости, но не реже одного раза в два года.