SAMRUK BUSINESS ACADEMY	**Положение о конфиденциальных данных**
ПП SBA 011-2024	**Редакция первая**

Утверждено
приказом директора
частного учреждения
«Samruk Business Academy»
от «12» 02 2024 года №03-01/14-00

1. Общие положения

1.1. Целью настоящего Положения о конфиденциальных данных (далее - Положение) является установление порядка сбора, обработки и охраны конфиденциальных данных в частном учреждении «Samruk Business Academy» (далее - Учреждение).

1.2.Охрана конфиденциальных данных осуществляется в целях предотвращения несанкционированного доступа к ним.

Сбор, обработка и охрана конфиденциальных данных (нераскрытая информация) Учреждения осуществляется в соответствии с Гражданским кодексом Республики Казахстан, настоящим Положением посредством применения комплекса мер, в том числе правовых, организационных и технических.

1.3. Положение применимо к деятельности всех структурных подразделений и работников Учреждения.

Все работники Учреждения должны быть ознакомлены с настоящим Положением.

2. Применяемые формы

Применяемых форм нет.

3. Термины и определения. Обозначения и сокращения

Для целей настоящего Положения в документе используются следующие сокращения и определения:

Учреждение - частное учреждение «Samruk Business Academy»;

Руководитель - директор Учреждения или иное лицо, исполняющее обязанности директора на основании соответствующего приказа и доверенности;

работник Учреждения - физическое лицо, состоящее в трудовых отношениях с Учреждением и непосредственно выполняющее работу по трудовому договору;

ИТ-служба - структурное подразделение и/или лица, осуществляющие в рамках своей компетенции ИТ-сопровождение деятельности Учреждения;

конфиденциальные данные (информация, сведения) - нераскрытая информация, информация об управленческой, финансово-хозяйственной, иной организационной деятельности Учреждения, коммерческая тайна Учреждения;

коммерческая тайна - бухгалтерская информация, иная информация, относимая к предпринимательской деятельности Учреждения, осуществляемой в соответствии с его уставной целью, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к

которой нет свободного доступа на законном основании, и Учреждение принимает меры к охране е конфиденциальности, если иное не установлено законодательством Республики Казахстан;

общедоступная информация - обобщенная информация, не раскрывающая сведений о деятельности Учреждения или конкретного лица, информация, относимая законодательством Республики Казахстан к общедоступной;

Перечень - Перечень конфиденциальных данных - перечень управленческой, финансово-хозяйственной, иной организационной информации, коммерческой тайны Учреждения, подлежащей охране (приложение к настоящему Положению);

охрана конфиденциальных данных - комплекс мер, в том числе правовых, организационных и технических, осуществляемых в целях защиты от незаконного получения, распространения либо использования информации.

4. Нормативные ссылки

Гражданский Кодекс Республики Казахстан (общая часть) от 27 декабря 1994 года №268-XIII;

Гражданский Кодекс Республики Казахстан (особенная часть) от 1 июля 1999 года №409-1;

Трудовой Кодекс Республики Казахстан от 23 ноября 2015 года №414-V;

Кодекс об административных нарушениях от 5 июля 2014 года №235-V;

Уголовный Кодекс Республики Казахстан от 3 июля 2014 года №226-V;

Закон Республики Казахстан от 24 ноября 2015 года №418-V «Об информатизации»;

Закон Республики Казахстан от 19 марта 2010 года №257-IV «О государственной статистике».

5. Ответственность

Функциональная ответственность:

5.1. Руководитель Учреждения несет ответственность за:

5.1.1. принятие/обеспечение принятия мер по охране конфиденциальных данных, предусмотренных законодательством Республики Казахстан и настоящим Положением;

5.1.2. материально-техническое оснащение деятельности ответственных лиц и ИТ-службы в целях обеспечения хранения и сохранности конфиденциальных данных.

5.2. Руководители структурных подразделений несут ответственность за контроль соблюдения работниками подразделений требований, предусмотренных законодательством Республики Казахстан и настоящим Положением.

5.3. ИТ-служба Учреждения несет ответственность за обеспечение физической защиты электронных информационных ресурсов и информационных систем, содержащих конфиденциальные данные, с использованием средств защиты информации, а также систем контроля доступа и регистрации фактов доступа к информации.

5.4. Все работники Учреждения, допущенные к сведениям, составляющим коммерческую тайну и иную конфиденциальную информацию, несут ответственность за соблюдение установленного порядка учета, пользования, размножения, хранения и уничтожения документов, содержащих конфиденциальные данные, аз выполнение требований настоящего Положения и законодательства Республики Казахстан.

Ответственность за разглашение:

5.5. Работник, разгласивший конфиденциальные данные, которому они были доверены по работе, несет дисциплинарную ответственность вплоть до расторжения трудового договора, а также уголовную, административную, гражданско-правовую ответственность, предусмотренную законодательством Республики Казахстан.

Работник, разгласивший конфиденциальные данные, обязан возместить вред, причиненный Учреждению в полном объеме.

Прекращение трудового договора после причинения работником ущерба (вреда) Учреждению, в результате разглашения конфиденциальных данных, не влечет за собой освобождения работника от материальной ответственности по возмещению причиненного ущерба (вреда) Учреждению.

5.6. Лицо(-а), совершившее(-ие) умышленные действия по сбору (получению) конфиденциальных данных путем хищения документов, подкупа или угроз в отношении лиц(-а), владеющих(-его) информацией или их близких, перехвата в средствах связи, незаконного проникновения в информационную систему или сеть, использования специальных технических средств, а равно иным незаконным способом в целях разглашения либо незаконного использования этих сведений несет(-ут) уголовную, административную, гражданско-правовую или иную ответственность в соответствии с законодательством Республики Казахстан.

6. Права и обязанности

6.1. Учреждение имеет право:

1) требовать от работников подписания и выполнения Обязательства о неразглашении конфиденциальных данных;

2) предупреждать лиц, осуществляющих проверку его деятельности, об ответственности за разглашение коммерческой тайны в соответствии с законами Республики Казахстан;

3) не предоставлять государственным органам и должностным лицам при выполнении регистрационных, контрольных и надзорных функций и совершении других действий доступ к информации, составляющей коммерческую тайну, кроме той, которая необходима для реализации возложенных на них функций.

6.2. Учреждение обязано:

1) принимать и соблюдать необходимые меры, в том числе правовые, организационные и технические, для охраны конфиденциальных данных в соответствии с законодательством Республики Казахстан:

- определить места хранения (носители) конфиденциальных данных и лиц, ответственных за реализацию мер по созданию условий, обеспечивающих их сохранность и исключающих несанкционированный доступ к ним;
- устанавливать в договорах с третьими лицами условия конфиденциальности и ответственность за их нарушение;
- принимать меры по защите информационных систем, содержащих конфиденциальные данные;

2) обеспечить работников условиями для хранения конфиденциальных данных и принятия иных мер к их охране.

6.3. Работники Учреждения обязаны:

1) неукоснительно соблюдать требования законодательства Республики Казахстан, настоящего Положения,

2) подписать и соблюдать Обязательство о неразглашении конфиденциальных данных, являющееся неотъемлемой частью к трудовому договору;

3) со дня принятия на работу и после прекращения трудового договора соблюдать конфиденциальность информации ограниченного доступа, ставшей им известными по работе, пресекать действия других лиц, которые могут привести к разглашению таких сведений;

4) принимать все доступные меры к охране конфиденциальных данных, хранящихся на бумажных, электронных носителях, в памяти персональных компьютеров;

5) исключить доступ посторонних лиц, а также иных работников Учреждения, которым не предоставлено право доступа к конфиденциальным данным соответствующим приказом Учреждения, к конфиденциальным данным (электронным информационным ресурсам, содержащим конфиденциальные данные), хранящимся в Учреждении;

6) хранить, необходимые в повседневной работе, документы, содержащие конфиденциальные данные, в запираемых сейфах и шкафах (ящиках);

7) при утрате или недостаче документов, содержащих конфиденциальные данные, ключей от хранилищ (сейфов, металлических шкафов, архива) и о других фактах, которые могут привести к разглашению конфиденциальных сведений, незамедлительно информировать своего непосредственного руководителя или руководителя Учреждения;

8) при выходе в ежегодный оплачиваемый трудовой отпуск, социальный отпуск или расторжении трудового договора своевременно сдать непосредственному руководителю или иному лицу, определенному непосредственным руководителем или руководителем Учреждения все документы, содержащие конфиденциальные данные, и другие материалы, Принадлежащие Учреждению;

9) представлять по требованию непосредственного руководителя и/или HR-менеджера устные и письменные объяснения о нарушениях установленных требований обеспечения сохранности конфиденциальных данных;

10) не использовать знание коммерческой тайны и иных конфиденциальных данных для занятий деятельностью, которая в результате конкурентного действия может нанести ущерб Учреждению и/или его контрагентам/партнерам.

6.4. Работникам Учреждения запрещено:

1) вести разговоры, касающиеся содержания коммерческой тайны и иных конфиденциальных данных в присутствии посторонних лиц или работников Учреждения, к компетенции которых данные вопросы не относятся (отсутствует доступ);

2) использовать конфиденциальные сведения в документах, статьях, предназначенных для опубликования в открытой печати, выступлениях, интервью и т.д. без соответствующего поручения или разрешения Руководителя Учреждения;

3) письменно излагать сведения, содержащие коммерческую тайну, в заявлениях по личным вопросам, жалобах, просьбах;

4) делать записи, расчеты и т.п., раскрывающие коммерческую тайну, в личных блокнотах, записных книжках, личных компьютерах;

5) снимать копии с документов, содержащих коммерческую тайну и иные конфиденциальные данные, выносить документы (их копии) из помещений, офисов без разрешения руководителя соответствующего структурного подразделения, ответственного за хранение и обеспечения сохранности таких документов;

6) хранить в рабочих столах ненужные для работы документы, содержащие коммерческую тайну и/или иные конфиденциальные данные;

7) размещать сведения документов и изданий с грифом «Конфиденциально» и других документов, содержащих коммерческую тайну и иные конфиденциальные данные, в глобальных и локальных информационных сетях.

6.5. Работники Учреждения имеют право:

Требовать создания условий для хранения конфиденциальных данных и принятия мер к их охране.

7. Порядок сбора, обработки и охраны конфиденциальных данных

7.1. Перечень конфиденциальных данных

7.1.1. Перечень конфиденциальных данных определен в приложении к настоящему Положению. Отнесение сведений/информации к категории конфиденциальных данных осуществляется Учреждением.

7.1.2. Не являются конфиденциальными следующие сведения, содержащиеся в базах данных, формируемых уполномоченным органом в области государственной статистики и информация, относящаяся в соответствии с Гражданским кодексом Республики Казахстан, Предпринимательским кодексом Республики Казахстан к общедоступной:

1) фамилия, имя, отчество (при его наличии) и наименование индивидуального предпринимателя; идентификационный номер (ИИН); юридический адрес; вид деятельности;

2) наименование и дата регистрации юридического лица; идентификационный номер (БИН); место нахождения; вид экономической деятельности по общему классификатору видов экономической деятельности; код по классификатору административно-территориальных объектов;

3) код по классификатору размерности юридических лиц, филиалов и представительств, а также субъектов индивидуального предпринимательства по численности работников;

4) устав юридического лица.

7.1.3. Сведения, которые в соответствии с Законом Республики Казахстан «О некоммерческих организациях» не могут быть предметом коммерческой тайны определены таковыми в целях официального предоставления уполномоченными лицами Учреждения по запросу уполномоченных органов и организаций в соответствии с законодательством Республики Казахстан и являются конфиденциальными для работников Учреждения.

7.1.4. В процессе деятельности в Перечень могут быть внесены изменения и дополнения с обоснованием их необходимости. При этом изменения и дополнения, внесенные в Перечень, действуют с момента их введения в действие и не распространяются на отношения, возникшие до их введения в действие. Изменения и дополнения вносятся в Перечень в порядке, установленном для изменения документации системы менеджмента качества. Изменения и дополнения в Перечень могут быть инициированы структурными подразделениями Учреждения, аудиторами системы менеджмента качества Учреждения или Руководителем Учреждения.

7.2. Охрана конфиденциальных данных

7.2.1. Учреждение обязано принимать необходимые меры по охране конфиденциальных данных, обеспечивающие:

1) предотвращение несанкционированного доступа к конфиденциальным данным;

2) своевременное обнаружение фактов несанкционированного доступа к конфиденциальным данным, если такой несанкционированный доступ не удалось предотвратить;

3) минимизацию неблагоприятных последствий несанкционированного доступа к конфиденциальным данным.

7.2.2. Охрана конфиденциальных данных в Учреждении осуществляется путем реализации мер правового, организационного и технического характера:

1) установление условий доступа к документации и электронным информационным ресурсам и ответственности за нарушение условий доступа и использования электронных информационных ресурсов;

2) обеспечение режима допуска на территорию (в помещения), где может быть осуществлен доступ к информации (к материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации;

3) хранение информации (документов, носителей информации, информационных массивов) в условиях, исключающих несанкционированное уничтожение, блокирование, модификацию, копирование, использование;

4) контроль действий работников с конфиденциальными документами, а также действий пользователей в автоматизированных системах;

5) физическая защита информационных систем, использование средств защиты информации, а также систем контроля доступа и регистрации фактов доступа к информации.

7.2.3. Охрана конфиденциальных данных заключается в запрете разглашения вышеуказанных сведений среди определенного либо неопределенного круга лиц, не имеющих к ним доступ в любой доступной для восприятия форме. С документами, решениями и источниками информации, затрагивающими права и интересы граждан, могут знакомиться только граждане, чьи права и интересы затрагиваются, а также лица, имеющие право доступа к такой информации.

7.2.4. При совершении сделок, в том числе с иностранными партнерами, в заключаемых договорах предусматриваются условия о конфиденциальности либо подписывается отдельный договор, в котором оговариваются характер, состав конфиденциальных сведений, а также взаимные обязательства по обеспечению ее сохранности, не противоречащие применимому законодательству.

7.2.5. Использование для открытого опубликования сведений, полученных на договорной или доверительной основе, или являющихся результатом совместной деятельности, допускается только с общего согласия партнеров.

7.3. Доступ к конфиденциальным сведениям. Специальное делопроизводство.

7.3.1. Доступ работника Учреждения к конфиденциальным данным осуществляется после подписания им Обязательства о неразглашении конфиденциальных данных, который является неотъемлемой частью трудового договора.

7.3.2. К конфиденциальным сведениям Учреждения и/или его контрагентов (партнеров, Участников) имеют доступ:

- ответственные лица Участников Учреждения, осуществляющие рассмотрение, согласование, визирование, вынесение на утверждение

соответствующего органа управления Участников Учреждения, материалов и документов по вопросам, входящим в компетенцию Общего Собрания Участников Учреждения;

- члены Ревизионной комиссии Учреждения;
- Директор Учреждения и руководители уровня CEO-1;
- руководители структурных подразделений в рамках компетенции, определенной Положением о соответствующем структурном подразделении и должностной инструкцией;
- делопроизводитель и иной работник Учреждения, ответственный за делопроизводство, обеспечивающие организацию работы конфиденциальными документами.

7.3.3. Остальные работники Учреждения обладают доступом к конфиденциальным сведениям и их содержащим документам только в объеме, необходимом им для выполнения своих функциональных обязанностей.

Копирование, фотографирование, размножение конфиденциальных документов любым способом запрещено!

7.3.4. Работник(-и) сторонней организации может(-гут) быть допущен(-ы) к ознакомлению и работе с документами, содержащими конфиденциальные данные Учреждения, при наличии соглашения о конфиденциальности между этой организацией и Учреждением, мотивированного письменного запроса такой организации с указанием темы выполняемого задания и ФИО работника(-ов) или в силу требований тендерной документации в целях подачи Учреждением тендерной заявки для участия в соответствующем тендере.

7.3.5. Документы, содержащие конфиденциальные данные, хранятся в структурных подразделениях Учреждения, к компетенции которых отнесена информация, отраженная в данных документах.

7.3.6. Предоставление доступа работнику одного структурного подразделения к конфиденциальной информации, хранящейся в другом структурном подразделении, осуществляется с разрешения руководителя последнего.

7.3.7. На документах, делах и изданиях, содержащих конфиденциальные данные, в целях предотвращения доступа к ним посторонних лиц, проставляется гриф «Конфиденциально».

7.3.8. Документы, содержащие конфиденциальные данные, должны храниться в служебных помещениях в надежно запираемых и несгораемых сейфах, металлических шкафах (ящиках), обеспечивающих их физическую сохранность.

7.3.9. Проверка наличия документов, имеющих гриф «Конфиденциально», производится не реже одного раза в год работником, ответственным за делопроизводство в соответствующем подразделении.

7.3.10. Оригиналы или копии документов, содержащих конфиденциальные данные, могут находиться у исполнителя в течение срока, необходимого для выполнения задания, при условии полного обеспечения их сохранности, под его личную ответственность.

7.3.11. Не допускается оставление работниками на рабочих столах, сетевых принтерах и ксероксах оригиналов и копий документов, содержащих конфиденциальные данные.

7.3.12. Компьютеры, содержащие сведения, составляющие конфиденциальные данные, в обязательном порядке должны быть защищены паролем в соответствии с Правилами информационной безопасности.

7.3.13. О фактах утраты документов, содержащих конфиденциальные данные, либо разглашения сведений, содержащихся в них, немедленно ставится в известность руководитель соответствующего структурного подразделения, делопроизводитель и руководитель структурного подразделения, ответственного за делопроизводство в Учреждении. При этом указанные лица должны быть проинформированы об обстоятельствах утраты документов.

7.3.14. По факту утраты документов, содержащих конфиденциальные данные, проводится служебное расследование.

Для служебного расследования факта утраты документов, содержащих конфиденциальные данные, или факта разглашения сведений, содержащихся в этих материалах, приказом Директора может быть создана комиссия. Собранные комиссией материалы в ходе расследования таких фактов и заключение комиссии (акт) о результатах расследования являются основанием для привлечения виновных лиц к установленной законодательством ответственности.

8. Необходимые основные ресурсы

8.1. Запираемые места хранения, обеспечивающие целостность и сохранность носителей конфиденциальных данных;

8.2. Управляемое сетевое оборудование, информационные системы с разграничением уровней доступа с авторизацией, физическая безопасность серверного и сетевого оборудования.

Разработал:

должность	Фамилия И.О.	Дата	Подпись
начальник юрид. отдела	Шарипова Я	08.02.2024	

Согласовал:

должность	Фамилия И.О.	Дата	Подпись
Директор ДЯПР	Дильдяклеева Я	09.02.2024	

Приложение к
Положению о конфиденциальных данных

Перечень конфиденциальных данных

Управление

• сведения о перспективных и оригинальных методах управления;

• сведения о подготовке, принятии и исполнении отдельных решений руководства по коммерческим, организационным и иным вопросам;

• отчеты/результаты ревизионных проверок;

• документы, регулирующие внутреннюю деятельность Учреждения, в том числе их проекты и типовые формы.

Планы

• планы развития;

• количественные показатели, приведенные в Стратегиях и планах развития, отчетных материалах о выполнении планов развития

• сведения о планах по расширению линейки услуг;

• план производства и перспективный план;

• планы закупок и продаж;

• планово-аналитические материалы за текущий период;

•сведения о свертывании различных видов услуг и их обоснование.

Финансы

• сведения, содержащиеся в бухгалтерских книгах;

• сведения, раскрывающие плановые и фактические показатели финансового плана;

• сведения о балансах;

• имущественное положение;

• стоимость товарных запасов;

• бюджет;

• обороты;

• банковские операции;

• сведения о финансовых операциях;

• банковские связи;

• специфика международных расчетов с нерезидентами;

• плановые и отчетные данные по валютным операциям;

• состояние банковских счетов и производимых операций;

• уровень выручки;

• уровень доходов;

• долговые обязательства предприятия;

• состояние кредита (пассивы и активы);

• размеры предоставленного кредита, вклада Участника(-ов);

• источники финансирования и условия по ним;

Рынок

• оригинальные методы изучения рынка сбыта;

• состояние рынка сбыта и перспектив рыночной конъюнктуры;

• обзоры рынка;

• результаты маркетинговых исследований;

• сведения, содержащие выводы и рекомендации специалистов по стратегии и тактике деятельности;

• сведения об эффективности предпринимательской деятельности;

• оригинальные методы осуществления продаж.

Партнеры

• сведения о заказчиках, поставщиках, партнерах, посредниках, спонсорах, представителях, а также об их конкурентах;

• сведения о финансовом состоянии, репутации или другие данные, характеризующие степень надежности поставщиков, партнеров, посредников, спонсоров, представителей, их дочерних организаций и партнеров;

• сведения, составляющие коммерческую тайну заказчиков, поставщиков, партнеров, посредников, спонсоров, представителей, их дочерних организаций и партнёров;

• документы, регулирующие внутреннюю деятельность заказчиков (поставщиков, партнеров, посредников, спонсоров, представителей, их дочерних организаций и партнёров), в том числе их проекты и типовые формы.

Переговоры

• сведения о подготовке и результатах проведения переговоров;

• сведения о получаемых и прорабатываемых заказах и предложениях;

• сведения о фактах подготовки и ведения переговоров;

•сроки, выделенные для проработки и заключения сделки;

сведения о лицах, ведущих переговоры, руководстве компаний, их характеристиках;

директивы по проведению переговоров, включая тактику, границы полномочий должностных лиц по ценам, скидкам и другим условиям;

сведения и документы, относящиеся к деловой политике и позиции по конкретным сделкам (структура продажной калькуляции, уровень выручки, уровень предложенных цен до определенного момента);

• материалы и приложения к предложениям при прямых переговорах;

• уровень предложенных цен, размера вознаграждения;

• сведения, раскрывающие тактику ведения переговоров при заключении контрактов или соглашений на закупку (продажу товаров), уровень максимально достижимых (уговорных) цен, объемы имеющихся средств (фондов) и другие конкурентные материалы, используемые для повышения эффективности сделки;

• сведения о мероприятиях, проводимых перед переговорами;

• информация о деловых приемах.

Контракты

• сведения, условия конфиденциальности, которые установлены в договорах, контрактах и т. п.;

• условия сделок (договоров, контрактов, соглашений), включая цены, условия платежа;

• особые условия сделок (ставки вознаграждения, скидки, предоплаты, рассрочки платежей и т.п.);

• сведения об исполнении контрактов (порядок, сроки исполнения, сведения о нарушениях исполнения обязательств, претензионной работе и ее результатах, фактах применения и размера штрафных санкций и др.);

• сведения о детальной расшифровке предмета лицензий при их купле-продаже, условия лицензионных и сублицензионных соглашений.

Цены

• сведения о методике и элементах расчета цен при оценке стоимости услуг;

• калькуляция издержек производства;

• затраты;

• внутренние прейскуранты и тарифы, размер скидок с прейскурантных цен;

•сведения о расчетах цен и обоснований сделок;

• сведения о контрактной цене услуг;

• сведения о размерах предоставленных скидках до и после заключения контракта.

Проекты, техника

• сведения о целях и задачах, программах перспективных исследований;

• результаты исследований и проектных разработок;

• проекты, модели и остальная документация по новым проектам;

• сведения о состоянии программного и компьютерного обеспечения, информационных систем.

Совещания

• сведения о фактах проведения и целях совещаний и заседаний;

• предмет и результаты совещаний и заседаний органов управления.

Безопасность

• сведения о наличии/отсутствии, структуре, составе, материально-техническом оснащении службы безопасности;

• сведения о порядке и состоянии организации защиты коммерческой тайны и иной конфиденциальной информации;

• сведения о порядке и состоянии организации охраны, пропускном режиме, системе сигнализации;

• логины и пароли доступа к информационным системам и системам безопасности, в том числе ключи электронных цифровых подписей аутентификации;

• системные журналы событий (логи) информационных систем и систем безопасности;

• информация о выявленных уязвимостях в информационных системах и статусах их устранения;

• материалы служебных расследований, связанных с инцидентами информационной безопасности.

Трудовые отношения

• схема должностных окладов;

• особые условия труда;

• персональные данные работников.