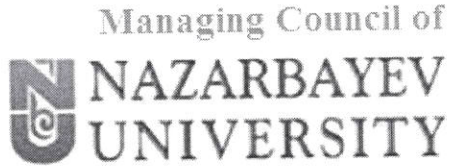
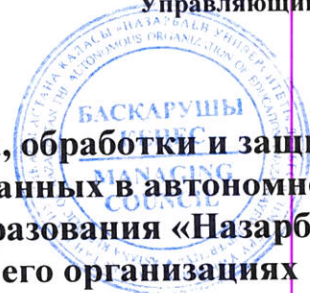


Применение № 1

Управляющий совет



Регламент сбора, обработки и защиты персональных данных в автономной организации образования «Назарбаев Университет» и его организациях



Версия*	Утверждено решением Управляющего совета*		Дата вступления документа в силу
	№ решения	Дата утверждения	
1.0	22.09.15	22.09.15	22.09.15
Статус	<input checked="" type="checkbox"/> Утвержден <input type="checkbox"/> Рассмотрен, отправлен на доработку (см. Приложение протокола) <input type="checkbox"/> Отклонен <input type="checkbox"/> Другое		
Ссылка на основные документы (вышестоящего уровня), послужившие основанием для разработки документа	Политика безопасности автономной организации образования «Назарбаев Университет» утвержденная решением Исполнительного совета от 25.04.14 за номером 4.4.1		
Ответственное должностное лицо	Lonsdale Anne, Провост		
Должностное лицо – инициатор документа	Упушева Гаухар Елемесовна, Генеральный директор, ЧУ "Nazarbayev University Library and IT Services"; +7(7172) 70 65 78; administration_nulits@nu.edu.kz		
Предыдущие/устаревшие документы	-		
Взаимосвязанные документы	-		
Язык документа	Каз - 22.09.15; Рус. - , англ. - 22.09.15		

1. Общие положения

1. Настоящий Регламент сбора, обработки и защиты персональных данных в автономной организации образования «Назарбаев Университет» и его организациях (далее — Регламент) разработан в соответствии с законодательством Республики Казахстан, включая:

- 1) Трудовой кодекс Республики Казахстан;
 - 2) Закон Республики Казахстан «О персональных данных и их защите» (далее - Закон);
 - 3) Закон Республики Казахстан «Об информатизации»;
 - 4) постановление Правительства Республики Казахстан «Об утверждении Правил определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач»;
 - 5) СТ РК ИСО/МЭК 27001-2008. «Информационные технологии. Методы защиты системы менеджмента информационной безопасности»;
 - 6) СТ РК ИСО/МЭК 17799-2006 «Информационная технология. Методы обеспечения защиты»;
- а также в соответствии с внутренними документами Университета и Организаций.

Handwritten signature

Handwritten signature

2. Требования настоящего Регламента распространяются на всех работников и обучающихся Университета и Организаций.

В Регламенте применяются следующие термины и сокращения:

- 1) **Университет** – автономная организация образования «Назарбаев Университет»;
- 2) **NULITS** – частное учреждение «Nazarbayev University Library and IT Services»;
- 3) **Оператор** – оператор базы, содержащей персональные данные в соответствии с Законом – работник структурного подразделения Университета или Организации, указанного в Приложении 6 к настоящему Регламенту, осуществляющий сбор, обработку и защиту персональных данных;
- 4) **Субъект** – работник, обучающийся Университета или Организации или иное физическое лицо, вступающее в отношение с Университетом или Организацией, к которому относятся персональные данные;
- 5) **Персональные данные** – сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе, в информационно-телекоммуникационных сетях и иных информационных системах;
- 6) **Helpdesk** – служба ИТ сопровождения NULITS, обеспечивающая сервис в части технической поддержки пользователей (автоматизированная служба единого окна для приема, регистрации и обработки обращений пользователей о сбоях в аппаратном и программном обеспечении, инфраструктуре информационной вычислительной сети Университета и Организаций, а также заявок на обеспечение техникой и предоставление ИТ-сервисов);
- 7) **Служба информационной безопасности** – подразделение NULITS, осуществляющее контроль информационной безопасности в области информационных систем и технологий;
- 8) **обучающийся** – физическое лицо, обучающееся по какой-либо образовательной программе Университета или Организации;
- 9) **абитуриент** – физическое лицо, претендующее на поступление на образовательную программу Университета или Организации;

- 10) Организации** – некоммерческие организации, учреждаемые Университетом, а также их дочерние организации.

2. Цели и задачи

3. Целью настоящего Регламента является обеспечение соблюдения законодательства Республики Казахстан при сборе, обработке и защите персональных данных в Университете и Организациях.

4. Задачами настоящего Регламента являются:

- 1) определение принципов для руководства при обработке персональных данных;
- 2) определение условий обработки персональных данных и способов их защиты;
- 3) определение прав, обязанностей и ответственности при сборе, обработке персональных данных.

5. В Университете и Организациях осуществляется сбор и обработка персональных данных следующих категорий Субъектов:

- 1) работники, состоящие в трудовых отношениях с Университетом или Организациями;
- 2) абитуриенты;
- 3) обучающиеся Университета или Организаций;
- 4) иные физические лица, данные о которых обрабатываются в процессе деятельности Университета и Организаций.

6. Персональные данные, обрабатываемые в Университете и Организациях содержатся на следующих носителях:

- 1) на бумажных носителях;
- 2) на электронных носителях;
- 3) в информационно-телекоммуникационных сетях и информационных системах.

7. Университет и Организации используют следующие способы обработки персональных данных:

- 1) без использования средств автоматизации;
- 2) смешанная обработка (с применением объектов вычислительной техники);
- 3) автоматизированная обработка персональных данных.

3. Сбор и обработка персональных данных

8. Сбор и обработка персональных данных в Университете и Организациях осуществляется только на материально-технических средствах Университета и Организаций, для следующих целей:

- 1) контроль за отпусками и пособиями по временной нетрудоспособности;

2) учет и управление обучением, профессиональным развитием и трудовыми показателями;

3) обеспечение воспитательного процесса, культурное развитие обучающихся и работников;

4) учет, идентификация и предоставление доступа в помещения/здания/офисы/ информационные системы, путем изготовления ID карт, учетной записи, в порядке и с учетом ограничений, предусмотренных внутренними документами Университета и Организаций;

5) проверка соответствия и пригодности для работы, обучения, в том числе проверку личности и истории;

6) качественный отбор работников, обучающихся, для участия в образовательной, общественной, культурной и спортивной деятельности Университета и Организации;

7) контроль за выплатами и функциями ведения ведомости заработной платы, стипендий, грантов;

8) контроль за отпусками по беременности и родам и схемам оплаты;

9) управление и поддержание безопасной рабочей и образовательной среды;

10) тестирование на предмет предложений для изменения внутренней документации Университета и Организаций;

11) контроль за соблюдением принципов равноправия, общепринятой этики, прав и свобод субъекта;

12) обмен информацией, в том числе, для рассмотрения и (или) предоставления ответов на обращения, предложения, рекомендации, поручения Субъекта (и/или третьих лиц), передачи (получения) корреспонденции (почты) в адрес Субъекта (в адрес лица, представителем которого является Субъект) для отправки (доставки)/получения посредством услуг, курьерской службы, экспресс почты и т.д.;

13) учет маркетинговых целей, предоставления Субъекту любых информационных материалов, в том числе услугах Университета и Организаций, а так же иных уведомлений посредством телефонной, факсимильной связи, иных видов связи, а так же по открытым каналам связи (в том числе SMS, E-mail, факс, и т.п.);

14) сбор статистических и служебных отчетов в соответствии с внутренней документацией Университета и Организаций;

15) для иных целей, которые могут быть установлены законодательством Республики Казахстан.

9. Перечень персональных данных, необходимых и достаточных для выполнения осуществляемых задач Университетом и Организациями (далее – Перечень персональных данных) установлен в Приложении 1 к настоящему Регламенту.

10. Сбор и обработка персональных данных работников осуществляется с согласия Субъекта, путем подписания согласия на обработку персональных данных работников, по форме согласно Приложению 2 к настоящему Регламенту.

11. Сбор и обработка персональных данных обучающихся осуществляется с согласия Субъекта путем заполнения аппликационных анкетных форм, принятых Университетом и Организациями и подписания согласия на обработку персональных данных обучающихся по форме согласно Приложению 3 к настоящему Регламенту.

12. При заключении с физическим лицом договора на оказание возмездного оказания услуг, такой договор должен содержать положение об использовании персональных данных такого физического лица и его согласие на такое использование.

13. В случае, если на момент предоставления согласия Субъект является несовершеннолетним лицом, подписание согласия, на обработку персональных данных обучающегося осуществляется его законным представителем (опекуном).

14. Согласие Субъекта на сбор и обработку персональных данных Субъекта не требуется в случаях, установленных Законом.

15. На основании полученной информации о Субъекте, Оператор заносит необходимую информацию (персональные данные) о Субъекте в информационную систему, базу данных.

16. Операторы, осуществляющие работу, напрямую связанную с образовательным процессом на текущий учебный год, получают доступ к персональным данным Субъекта только после подписания соответствующего приказа в Университете о зачислении студентов на текущий учебный год и только в том объеме, непосредственно с которым связана их работа.

17. Персональные данные хранятся в течение сроков в соответствии с внутренними документами и процедурами Университета и Организаций.

18. Персональные данные, содержащиеся на бумажных носителях, съемных маркированных носителях, сдаются в архив после истечения установленного срока их хранения в соответствии с внутренними документами Университета и Организаций.

19. Персональные данные, содержащиеся на носителях информации, встроенных в технические средства, информационно-телекоммуникационных сетях, базах данных информационных систем Операторов, после истечения установленного срока хранения, уничтожаются на основании решения экспертной комиссии Университета, созданной в соответствии с приказом Исполнительного вице-президента Университета.

20. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации, производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

21. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, производится способом,

исключающим дальнейшую обработку этих персональных данных, но с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

22. В случае отсутствия возможности уничтожения персональных данных, Оператор осуществляет блокирование либо принимает необходимые меры по обезличиванию персональных данных.

23. При сборе и обработке персональных данных, должностные лица Университета и Организаций строго руководствуются положением настоящего Регламента и должностной инструкцией.

4. Защита персональных данных

24. При работе с персональными данными, Операторами должно быть обеспечено:

- 1) конфиденциальность персональных данных;
- 2) условия хранения персональных данных, исключающие их утрату или несанкционированный доступ к ним;
- 3) хранение материальных носителей в служебных помещениях, шкафах, сейфах (хранилищах) имеющих защищенный и контролируемый доступ;
- 4) использование только предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;
- 5) недопущение несанкционированного выноса из помещений оборудования, а также удаления, инсталляции или настройки программного обеспечения не уполномоченными на этот вид работ работниками.
- 6) недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- 7) постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

25. Компьютеры, в которых содержатся файлы с персональными данными, должны быть защищены индивидуальными паролями доступа, в соответствии с принятыми правилами парольной защиты в Университете и Организациях.

26. Работа на компьютерах с персональными данными без паролей доступа или под чужими, а равно общими (одинаковыми) паролями, не допускается.

27. При обнаружении сбоя в программном обеспечении, а так же в оборудовании, необходимо подать заявку в HelpDesk в соответствии с принятыми правилами в Университете и Организациях.

28. Информационные системы, где обрабатываются персональные данные, установлены в соответствии с Приложением 4 к настоящему Регламенту.

29. Возможные типы угроз и их последствия при обработке персональных данных в информационных системах, а так же принимаемые меры определяются Службой информационной безопасности и установлены в соответствии с Приложением 5 к настоящему Регламенту.

30. NULITS осуществляет необходимые меры по защите персональных данных, содержащихся в информационных системах, к ним относятся:

- 1) антивирусная защита;
- 2) техническая поддержка инфраструктуры;
- 3) управление телекоммуникациями;
- 4) серверное сопровождение;
- 5) наличие резервного оборудования;
- 6) программное и технологическое сопровождение и развитие информационных систем;
- 7) ежедневный мониторинг и анализ сервисов;
- 8) резервное копирование данных;
- 9) применение криптографических средств защиты;
- 10) средства обнаружения вторжений и атак;
- 11) средства защиты виртуальной инфраструктуры;
- 12) применение электронно-цифровой подписи;
- 13) ведение журналов, записей;
- 14) централизованное управление доступом к информационным системам.

31. При работе Операторов с персональными данными в информационных системах согласно Приложению 4, Службой информационной безопасности должно обеспечиваться:

- 1) обучение лиц, использующих средства защиты информации, правилам работы с ними;
- 2) учет лиц, допущенных к работе с персональными данными, прав и паролей доступа;
- 3) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- 4) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- 5) описание системы защиты персональных данных.

5. Ответственность и обязанность сторон

32. Университет и Организации при защите персональных данных Субъектов обеспечивают необходимые организационно-распорядительные меры.

33. Ответственность за организацию работы по сбору и обработке персональных данных в рамках каждого структурного подразделения Университета и Организаций согласно требованиям настоящего Регламента возлагается на руководителя соответствующего структурного подразделения.

34. При обращении Субъекта персональных данных или его законного представителя с запросом о предоставлении информации о персональных данных, относящихся к соответствующему Субъекту, Университет и Организации обязаны предоставить данному Субъекту соответствующую информацию, предоставить возможность ознакомления с ней.

35. Руководитель структурного подразделения, осуществляющего обработку персональных данных:

- 1) определяет места хранения персональных данных (материальных носителей);
- 2) осуществляет контроль наличия в структурном подразделении условий, обеспечивающих сохранность персональных данных и исключаящих несанкционированный к ним доступ;
- 3) информирует лиц, осуществляющих обработку персональных данных, о Перечне персональных данных, и принятых правилах их обработки в структурном подразделении.
- 4) обеспечивает хранение материальных носителей с персональными данными Субъекта, как и его согласие на обработку персональных данных, в служебных помещениях, шкафах, сейфах (хранилищах) имеющих защищенный и контролируемый доступ.

5) контролирует порядок сбора, обработки и хранения персональных данных Субъекта в информационных системах, серверных помещениях.

36. Ответственность за сбор и обработку персональных данных возлагается индивидуально на каждое должностное лицо подразделения, непосредственно осуществляющего работу с персональными данными в соответствии с должностной инструкцией.

37. Операторы обязаны:

- 1) соблюдать требования настоящего Регламента;
- 2) сопровождать соответствующие информационные системы в соответствии с Приложением 4;
- 3) обеспечить целостность, достоверность информации при сборе и обработке персональных данных, как на бумажных носителях, так и при наполнении баз данных;
- 4) обеспечить конфиденциальность при обработке персональных данных;
- 5) регулярно проверять и обновлять антивирусные средства, установленные на компьютере.

38. Работники, работающие с персональными данными, обязаны немедленно сообщать своему непосредственному руководителю и (или) Службе информационной безопасности обо всех ставших им известных фактах получения третьими лицами несанкционированного доступа, либо попытках получения доступа к персональным данным, об утере или недостатке носителей информации, содержащих персональные данные, удостоверений, пропусков, ключей от сейфов (хранилищ), электронных ключей и других фактах, которые могут привести к несанкционированному доступу к персональным данным, а также о причинах и условиях возможной утечки этих сведений.

39. При работе с персональными данными работниками должна соблюдаться политика «чистого стола» и личный контроль доступа к компьютеру.

40. Без согласования с непосредственным руководителем, формирование и хранение баз данных, содержащих персональные данные, запрещается.

41. Работникам, работающим с персональными данными, запрещается передавать их устно или письменно кому либо, если это не вызвано целями подразделения в соответствии с положением о подразделении и должностной инструкцией работника.

42. Администраторы, осуществляющие программное и технологическое сопровождение информационных систем, обязаны:

- 1) своевременно проводить профилактические работы;
- 2) устанавливать необходимые технические меры по защите сведений;
- 3) осуществлять своевременное резервное копирование;
- 4) проводить ежедневный мониторинг информационных систем;
- 5) проводить мониторинг сетевых ресурсов;
- 6) вести записи по регистрации неисправностей.

43. Служба информационной безопасности обязана:

- 1) осуществлять мониторинг в области защиты персональных данных;
- 2) ежегодно проводить проверку бизнес-процессов связанных со сбором, обработкой и защитой персональных данных;
- 3) вести записи инцидентов в области информационной безопасности;
- 4) предоставлять рекомендации и проводить служебные расследования в области защиты персональных данных;
- 5) осуществлять контроль доступа к информационным системам персональных данных.

44. Субъекты персональных данных обязаны:

- 1) передавать Операторам достоверные персональные данные;
- 2) своевременно в срок, не превышающий 30 дней, сообщать Оператору об изменениях в сведениях, о персональных данных.

45. Лица, виновные в нарушении настоящего Регламента, регулирующих сбор, обработку и защиту персональных данных, несут дисциплинарную ответственность в соответствии с внутренними документами Университета и Организаций, а так же ответственность в соответствии с законодательством Республики Казахстан.

46. Споры, возникающие при сборе, обработке и защите персональных данных, подлежат рассмотрению в порядке, установленном законодательством Республики Казахстан а так же внутренними документами Университета и Организаций.

6. Заключительные положения

47. Актуализация Регламента осуществляется в случаях изменений законодательства, регулирующих персональные данные, организационной

структуры, в связи с внедрением новых технологий или иных механизмов и процедур, требующих пересмотр положений Регламента.



Приложение 1
к Регламенту сбора, обработки и защиты
персональных данных в автономной организации
образования «Назарбаев Университет» и его
организациях

**Перечень персональных данных, необходимый и достаточный для выполнения
осуществляемых задач в автономной организации образования «Назарбаев Университет» и его
организациях.**

№ п/п	Наименование персональных данных.
1.	Фамилия
2.	Имя
3.	Отчество (при его наличии)
4.	Сведения о смене фамилии, имени, отчества
5.	Транскрипция фамилии и имени
6.	Данные о рождении: дата рождения; место рождения
7.	Национальность
8.	Пол
9.	Сведения о семейном положении: состояние в браке; данные свидетельства о заключении брака; данные свидетельства о расторжении брака; фамилия, имя, отчество супруги(а); данные документа, удостоверяющего личность супруги(а); степень родства; фамилии, имена, отчества и даты рождения, место работы, место учебы, домашний адрес, номера мобильного телефона и служебного телефона других членов семьи, иждивенцев; наличие детей и их возраст
10.	Данные о гражданстве (прежнее гражданство)
11.	Социальный статус.
12.	Сведения о номере, серии и дате выдачи трудовой книжки
13.	Данные о трудовой деятельности на текущее время: полное указание должности, структурного подразделения, организации ее наименование; общий и непрерывный стаж работы; адреса и телефоны, а также название других организаций с полным наименованием занимаемых ранее в них должностей и период работы в этих организациях
14.	Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки: дата поступления в учебное заведение (отчисления из учебного заведения); серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения; наименование и местоположение образовательного учреждения; факультет или отделение, квалификация и специальность по окончании образовательного учреждения; ученая степень;

	ученое звание; владение иностранными языками
15.	Сведения о повышении квалификации и переподготовке: серия, номер, дата выдачи документа о повышении квалификации или о переподготовке; наименование и местоположение образовательного учреждения; квалификация и специальность по окончании образовательного учреждения
16.	Адрес проживания, адрес прописки
17.	Номера контактных телефонов
18.	Адрес электронной почты
19.	Индивидуальный идентификационный номер (ИИН)
20.	Портретное изображение на бумажном носителе, так же оцифрованная фотография
21.	Данные документа, удостоверяющего личность: наименование документа; номер документа; дата выдачи документа; срок действия документа; орган, выдавший документ
22.	Сведения о прохождении медицинского осмотра
23.	Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу: серия, номер, дата выдачи (сдачи) военного билета; наименование органа, выдавшего военный билет; военно-учетная специальность; воинское звание; данные о принятии/снятии с учета; основания освобождения от воинской службы
24.	Сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях, сертификатах; наименование или название награды, звания или поощрения; дата и вид нормативного акта о награждении или дата поощрения
25.	Информация о лицах, имеющих право на получение алиментов
26.	Сфера деятельности родителей/попечителей.
27.	Сведения о вне учебном занятии и опыте работы
28.	Портретное изображение на бумажном носителе, а так же, оцифрованная фотография для выпуска ID карты

ФИО (полностью) _____

Подпись _____ Дата _____




Приложение 2
к Регламенту сбора, обработки и защиты
персональных данных в автономной организации
образования «Назарбаев Университет» и его
организациях

Кому _____
от ФИО _____
уд. личности, паспорт
№ _____ дата _____
гос. орган выдачи _____

**Согласие
на обработку персональных данных работника**

В целях соблюдения Трудового кодекса, Закона Республики Казахстан «О персональных данных и их защите», Работник дает Работодателю: _____, расположенному по адресу г. Астана район Есиль, пр. Кабанбай - батыра, д. 53 (далее – Работодатель) согласие на сбор (в том числе у третьих лиц), обработку, использование, хранение персональных данных, фиксируемых на электронном и бумажном носителе, и (или) ином материальном носителе, которые могут содержать (включая, но не ограничиваясь):

1. Сведения, необходимые для надлежащей идентификации

- Фамилия, имя, отчество, транскрипция фамилии и имени.
- Сведения о смене фамилии, имени, отчества.
- Данные о рождении: место рождения, дата рождения, национальность, пол.
- Сведения о семейном положении: состояние в браке; данные свидетельства о заключении брака; данные свидетельства о расторжении брака; фамилия, имя, отчество супруги(а); данные документа, удостоверяющего личность супруги(а); степень родства; фамилии, имена, отчества и даты рождения других членов семьи, иждивенцев; наличие детей и их возраст.
- Данные о гражданстве (прежнее гражданство).
- Данные документа, удостоверяющего личность: наименование документа; номер документа; дата выдачи документа; срок действия документа; орган, выдавший документ.
- Индивидуальный идентификационный номер
- Портретное изображение на бумажном носителе, а так же, оцифрованная фотография для выпуска ID карты

2. Сведения об образовании, профессиональной деятельности, служебном положении

- Сведения о номере, серии и дате выдачи трудовой книжки.
- Данные о трудовой деятельности на текущее время: полное указание должности, структурного подразделения, организации ее наименование; общий и непрерывный стаж работы; адреса и телефоны, а также название других организаций с полным наименованием занимаемых ранее в них должностей и период работы в этих организациях.
- Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки: дата поступления в учебное заведение (отчисления из учебного заведения); серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения; наименование и местоположение образовательного учреждения; факультет или отделение, квалификация и специальность по окончании образовательного учреждения; ученая степень; ученое звание; владение иностранными языками.
- Сведения о повышении квалификации и переподготовке: серия, номер, дата выдачи документа о повышении квалификации или о переподготовке; наименование и местоположение образовательного учреждения; квалификация и специальность по окончании образовательного учреждения.
- Сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях, сертификатах; наименование или название награды, звания или поощрения; дата и вид нормативного акта о награждении или дата поощрения.

3. Сведения необходимые для поддержания связи

- Номера контактных телефонов.
- Адрес электронной почты.

– Адрес места жительства, адресная справка.

4. Иные сведения необходимые Работодателю

– Сведения о прохождении медицинского осмотра.

– Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу: серия, номер, дата выдачи (сдачи) военного билета; наименование органа, выдавшего военный билет; военно-учетная специальность; воинское звание; данные о принятии/снятии с учета; основания освобождения от воинской службы.

– Информация о лицах, имеющих право на получение алиментов.

Указанная информация будет использована в соответствии с деятельностью Работодателя, включая, но, не ограничиваясь, исполнением следующих целей:

- 1) контроль за отпусками и пособиями по временной нетрудоспособности;
- 2) учет и управление обучением, персональным развитием и трудовыми показателями;
- 3) учет, идентификация и предоставление доступа в помещения/здания/офисы/ информационные системы, изготовление ID карты, создание учетной записи, в порядке и с учетом ограничений, предусмотренных внутренними документами Работодателя;
- 4) обмен информацией, в том числе, для рассмотрения и (или) предоставления ответов на обращения, предложения, рекомендации, поручения и т.д. субъекта (и/или третьих лиц), передачи (получения) корреспонденции (почты) в адрес субъекта (адрес лица представителем которого является субъект) для отправки (доставки)/получения посредством услуг, курьерской службы, экспресс почты и т.д.;
- 5) предоставления субъекту любых информационных материалов, в том числе услугах Работодателя, а так же иных уведомлений посредством телефонной, факсимильной связи, иных видов связи, а так же по открытым каналам связи (в том числе SMS, E-mail, факс, и т.п.);
- 6) учет дней отпуска;
- 7) проверка соответствия и пригодности для работы, в том числе проверку личности и истории;
- 8) контроль за выплатами и функциями ведения ведомости заработной платы;
- 9) контроль за отпусками по беременности и родам и схемам оплаты;
- 10) управление и поддержание безопасной рабочей обстановки;
- 11) для иных целей, которые могут быть установлены законодательством Республики Казахстан.

Подтверждение работника:

Я даю свое согласие Работодателю на анализ и использование персональных данных, для исполнения целей указанных Работодателем.

Я даю свое согласие на использование данных (ФИО; должность; номер служебного телефона; номер мобильного телефона; адрес электронной почты) в телефонной книге в рамках функциональной работы информационного портала my.nu.edu.kz.

Я уведомлен о ведущемся видеонаблюдении, предусмотренном для выполнения функций безопасности.

Настоящее Соглашение дано Работодателю на срок действия трудового договора и может быть отозвано путем подачи письменного заявления.

ФИО (полностью) _____

Подпись _____ Дата _____

Приложение 3
к Регламенту сбора, обработки и защиты
персональных данных в автономной организации
образования «Назарбаев Университет» и его
организациях

Кому _____
от ФИО _____
документ, удостоверяющий личность
№ _____ дата _____
гос. орган выдачи _____

Согласие на обработку персональных данных обучающегося

В целях соблюдения закона Республики Казахстан «О персональных данных и их защите», обучающийся дает согласие _____ адрес г. Астана район Есиль, пр. Кабанбай - батыра, д. 53 (далее - Университет) на сбор (в том числе у третьих лиц), обработку, использование, хранение, персональных данных, фиксируемых на электронном и бумажном носителе, и (или) ином материальном носителе, которые могут содержать (включая, но не ограничиваясь):

1. Сведения, необходимые для надлежащей идентификации

- Фамилия, имя, отчество, транскрипция фамилии и имени.
- Сведения о смене фамилии, имени, отчества.
- Данные о рождении: место рождения, дата рождения, национальность, пол.
- Данные о гражданстве.
- Сведения о ближайших родственниках (о родителях, братьях, сестрах, попечителях)

фамилия, имя, отчество родственника; место работы; место учебы; домашний адрес; номера мобильного телефона и служебного телефона;

- Данные документа, удостоверяющего личность: наименование документа; номер документа; дата выдачи документа; срок действия документа; орган, выдавший документ.
- Индивидуальный идентификационный номер
- Портретное изображение на бумажном носителе, а так же, оцифрованная фотография для выпуска ID карты

2. Сведения об образовании

- Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки: дата поступления в учебное заведение (отчисления из учебного заведения); серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения; наименование и местоположение образовательного учреждения; факультет или отделение, квалификация и специальность по окончании образовательного учреждения; ученая степень; ученое звание; владение иностранными языками.

3. Сведения необходимые для поддержания связи

- Номера телефонов, мобильный, домашний, дополнительный контактный телефон при экстренных случаях.
- Адрес электронной почты.
- Адрес проживания. Адрес прописки.

4. Иные сведения, необходимые Университету

- Социальный статус.
- Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу: серия, номер, дата выдачи (сдачи) военного билета; наименование органа, выдавшего военный билет; военно-учетная специальность; воинское звание; данные о принятии/снятии с учета; основания освобождения от воинской службы.
- Сфера деятельности родителей/попечителей.
- Сведения о вне учебном занятии и опыте работы

Указанная информация будет использована в соответствии с деятельностью Университета, включая, но, не ограничиваясь, исполнением следующих целей:

- 1) учет и управление обучением, персональным развитием и показателями успеваемости;
- 2) обеспечение воспитательного процесса, культурное развитие обучающегося;
- 3) учет, идентификация и предоставление доступа в помещения/здания/офисы/ информационные системы, изготовление ID карты, создание учетной записи, в порядке и с учетом ограничений, предусмотренных внутренними документами Университета и его организаций;
- 4) обмен информацией, в том числе, для рассмотрения и (или) предоставления ответов на обращения, предложения, рекомендации, поручения и т.д. обучающегося (и/или третьих лиц), передачи (получения) корреспонденции (почты) в адрес обучающегося (адрес лица представителем которого является обучающийся) для отправки (доставки)/получения посредством услуг, курьерской службы, экспресс почты и т.д.;
- 5) предоставления обучающемуся любых информационных материалов, в том числе об услугах Университета и его организаций, а так же иных уведомлений посредством телефонной, факсимильной связи, иных видов связи, а так же по открытым каналам связи (в том числе SMS, E-mail, факс, и т.п.);
- 6) проверка соответствия и пригодности для прохождения обучения, в том числе проверку личности и истории;
- 7) контроль за выплатами (стипендии, гранты) и функциями ведения ведомости;
- 8) управление и поддержание безопасной учебной обстановки;
- 9) для иных целей, которые могут быть установлены законодательством Республики Казахстан.

Подтверждение обучающегося:

Я даю свое согласие Университету и его организациям на анализ и использование моих персональных данных, для исполнения выше указанных целей.

Я даю свое согласие на использование данных (ФИО; номер мобильного телефона; адрес электронной почты) в телефонной книге в рамках функциональной работы информационного портала tu.nu.edu.kz.

Я уведомлен о ведущемся видеонаблюдении, предусмотренном для выполнения функций безопасности.

Настоящее Согласие дано Работодателю на срок действия договора об оказании образовательных услуг и может быть отозвано путем подачи письменного заявления.

ФИО (полностью) _____

Подпись _____ Дата _____

Приложение 4
к Регламенту сбора, обработки и защиты
персональных данных в автономной организации
образования «Назарбаев Университет» и его
организациях

Список информационных систем, обрабатывающих персональные данные

№	Наименование системы	Краткое описание системы	Оператор системы	Оператор по технической сопроводению	Количество пользователей	Резервное копирование и восстановление различных компонент системы	
						Наименование компонента Методы резервирования Методы восстановления	Затраченное время при восстановлении
1	Система Admissions	Регистрация абитуриентов на портале, предоставления аппликационных анкет, обработки сведений абитуриентов сотрудниками приемной комиссии	Департамент по приему	NULITS	18 тыс. и более абитуриентов включая сотрудников приемной комиссии	База данных Oracle, База данных DB2, LDAP, сервер приложений. Oracle - Rman, ежедневно. DB2 - встроенные функции резервирования, ежедневно. LDAP - встроенные функции резервирования, ежедневно. Сервер приложений - клонирование, еженедельно.	20-60 минут на восстановление базы данных, 15-45 минут на восстановление LDAP. Восстановление из клона 4-8 часов.
2	Система IC УПП	Система для ведения бухгалтерского, налогового, кадрового учета, расчета заработной платы, учета студентов, расчета стипендии, управления денежными средствами, получения финансовой, регламентированной и управленческой отчетности.	ФЭО, Кадровые службы	NULITS	170 и более пользователей	База данных Microsoft SQL Server 2008 R2. Архивирование БД средствами IC – ежедневно. Сервер приложений, сервер БД - клонирование, еженедельно.	20-60 минут на восстановление базы данных. Восстановление из клона 4-8 часов.
3	Система Офис-регистратора	Просмотр индивидуального расписания занятий и экзаменов, просмотр текущей успеваемости за семестр за весь период обучения. Выставления оценок ППС	Офис регистратора	NULITS	5000 студентов и более 200 ППС и более	База данных MySQL, сервер приложений MySQL Dump, архивирование в TAR файл, ежедневно, использование MySQL Dump,	15-30 минут на восстановление базы данных, 5-10 минут на распаковку

							резервного архива
4	Система Moodle	Создания образовательных ресурсов и организации учебной деятельности	Школы Университета	NULITS	3500 и более включая студентов, ППС и международны х партнеров	База данных Oracle, сервер приложений. Oracle Rman, ежедневно. Сервер приложений снятие копии файлов, перед изменением.	20-60 минут для восстановления баз данных, 10-20 мин для восстановления из копии.
5	Система CRM	Ведения базы данных кандидатов, планирующих поступить на программу магистратуры Университета, стать сотрудником, пройти стажировку и т.д.	Департамент по приему в высшие школы Университета	NULITS	20 и более	База данных Oracle, База данных DB2, LDAP, сервер приложений. Oracle - Rman, ежедневно. DB2 - встроенные функции резервирования, ежедневно. LDAP - встроенные функции резервирования, ежедневно. Сервер приложений - клонирование, еженедельно.	20-60 минут на восстановление базы данных, 15-45 минут на восстановление LDAP. Восстановление из клона 4-8 часов.
6	Система управления ID картами	Система управления контроля доступом на территорию и помещения Университета. Изготовление ID карт.	ЧУ «USM»	«USM»	3 администратор а Более 7000 пользователей id карт.	База данных SQL 2008 копия БД 1 раз в две недели	2 часа и более
7	ЕСУП	Управление регистрационными данными, учетными записями и доступом пользователей к информационным ресурсам Университета путем обеспечения передачи единых сведений о пользователях в целевые системы	NULITS	NULITS	3 администратор а более 7000 пользователей	БД – MS SQL Server 2008 R2 (дифференциальный бекап – ежедневно, полный - еженедельно); Серверы приложений бекапируются встроенным в Windows Server 2008 R2 средством Windows Server Backup ежедневно (полностью ОС), а также снапшотами VMware VSphege	сутки и более

Приложение 5
к Регламенту сбора, обработки и защиты
персональных данных в автономной организации
образования «Назарбаев Университет» и его
организациях

Типы угроз и принимаемые меры

№, № п/п	Тип угрозы	Возможные последствия	Принимаемые меры
1.	Анализ сетевого трафика	Перехват передаваемых данных, в том числе идентификаторов и паролей пользователей. Последствия: выявление злоумышленником сетевых сервисов, используемых в ИС, а так же некоторых их характеристик, с последующим нарушением их доступности и конфиденциальности.	<ul style="list-style-type: none"> - Шифрование трафика; - Использование Системы предотвращения атак (IPS); - Использование криптографических средств защиты; - Отслеживание и пресечение использования программ затрудняющих или нарушающих работу сети; - Контроль оборудования состава и структуры сети.
2.	Сканирование сети	Определение протоколов, доступных портов сетевых служб, определение процедур формирования идентификаторов соединений, активных сетевых сервисов, идентификаторов и паролей пользователей. Последствия: выявление злоумышленником структуры сети и направления информационных потоков.	<ul style="list-style-type: none"> - Использование фаирвола и его ресурсов для блокировки нежелательных адресов, блокировки неиспользуемых портов; - Контроль сетевых пакетов; - Использование нестандартных портов; - Использование сканеров узких мест с адвайзером. - Использование Системы предотвращения атак (IPS); - Средства антивирусной защиты.
3.	Угроза выявления пароля	Выполнение действия, связанного с получением несанкционированного доступа. Последствия: Несанкционированный доступ	<ul style="list-style-type: none"> - смена паролей раз в 6 месяцев; - контроль активности учетных записей в лог журналах; - актуальность учетных записей по кадровому передвижению 1 раз в месяц; - хранение паролей в зашифрованном виде; - использование сложных паролей в соответствии с Правилами парольной защиты; - применение политик безопасности для разграничения прав доступа к разделяемым

		ресурсам сети. - ежедневный мониторинг систем администраторами; - маршрутизация потоков информации внутри сетевого окружения, с помощью распределённой системы на базе сетевого оборудования Cisco; - использование сетевых протоколов с аутентификацией субъектов; - использование виртуального канала.
4.	Подмена доверенного объекта сети	Изменение трассы прохождения сообщений, несанкционированное изменение маршрутно-адресных данных. Последствия: Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации. Нарушение целостности, конфиденциальности и доступности передаваемых данных. Несанкционированное изменение маршрутно-адресных данных, анализ и модификация передаваемых данных, навязывание ложных сообщений
5.	Навязывание ложного маршрута сети	использование сетевых протоколов с аутентификацией субъектов, использование виртуального канала; - использование средств защиты виртуальной инфраструктуры.
6.	Внедрение ложного объекта сети	- маршрутизация потоков информации внутри сетевого окружения, с помощью распределённой системы на базе сетевого оборудования Cisco; - использование двухсторонней многоступенчатой аутентификации; - автоматизированное обновление программных комплексов; - полное резервное копирование проводится 1 раз в две недели, проверка резервных копий; - распределение нагрузки на серверах; - распределение нагрузки на сеть аппаратными средствами Cisco; контроль, обновление, увеличение объема ресурсов.
7.	Отказ в обслуживании	- профилактические мероприятия на рабочих станциях по заявкам; - профилактические мероприятия на сервере 1 раз в месяц; - использование системы бесперебойного питания; - распределение нагрузки на сеть аппаратными средствами Cisco.
	Частичное исчерпание ресурсов	Снижение пропускной способности каналов связи, производительности сетевых устройств. Последствия: Снижение производительности серверных приложений. Увеличение времени обработки данных и снижение эффективности вычислительных операций.
	Полное исчерпание ресурсов	Невозможность передачи сообщений из-за отсутствия доступа к среде передачи, отказ в установлении соединения. Последствия: остановка обработки и работы ИС.
	Нарушение логической связанности между	Невозможность передачи сообщений из-за отсутствия корректных маршрутно-адресных данных. Невозможность

		атрибутами, данными, объектами	получения услуг ввиду несанкционированной модификации идентификаторов, паролей и т.п.	
		Использование ошибок в программах	Нарушение работоспособности сетевых устройств	- мониторинг и включения функции debug в ППО.
		Путем рассылки файлов, содержащих деструктивный исполняемый код, вирусное заражение	Нарушение конфиденциальности, целостности, доступности информации	- сканирование рабочих станций на предмет наличия вирусов и закладок; - антивирусная защита, обновление антивирусных баз; - средства обнаружения и вторжения атак. - защита от несанкционированной массовой рассылки по электронной почте.
8.	Удаленный запуск приложений	Путем переполнения буфера серверного приложения		- отслеживание состояния серверов администраторам.
		Путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами	Скрытое управление системой	- сканирование рабочих станций на предмет наличия вирусов и закладок; - мониторинг и анализ серверов. - контроль и ограничение трафика в каналах связи с другими сетями и Интернет с целью предотвращения нецелевого использования ресурсов внешних каналов связи.

Приложение 6
к Регламенту сбора, обработки и защиты
персональных данных в автономной организации
образования «Назарбаев Университет» и его
организациях

Операторы

Работники следующих Департаментов/Служб Университета и Организаций являются Операторами для целей Регламента:

- 1) Департамент по приему;
- 2) Департамент по приему в Высшие школы
- 3) Департамент по студенческим делам;
- 4) Офис регистратора;
- 5) Департамент управления человеческими ресурсами;
- 6) Кадровые службы Учреждений;
- 7) IT Дирекция NULITS;
- 8) Финансово-экономические службы Университета и Организаций;
- 9) Школы Университета;
- 10) Библиотека NULITS;
- 11) ЧУ «USM»;
- 12) Служба слаботочных систем безопасности USM Астана.