«УТВЕРЖДЕНО»
Решением Правления
НАО «Университет Нархоз»
Протокол №_5_ от
«15»_06_20_23_г.

Правила использования мобильных устройств и носителей информации в Некоммерческом акционерном обществе «Университет Нархоз»

Алматы, 2023

Оглавление

Паспорт документа ……...……...3
Лист согласования……...……....4
1. Назначение документа ……...……...……..……5
2. Глоссарий……...……...……...……5
3. Ссылки……...……...……...……5
4. Риски использования мобильных устройств и носителей за пределами организациями……...…… ……...……6
5. Порядок использования мобильных устройств и носителей информации ……...……...……6
6. Ответственность ……...……...……8
7. Заключительные положения 8

Паспорт документа

Наименование документа:	Правила использования мобильных устройств и носителей информации в Некоммерческом акционерном обществе «Университет Нархоз»
Краткое описание:	Правила использования мобильных устройств и носителей информации в Некоммерческом акционерном обществе «Университет Нархоз»
Тема:	Информационная безопасность
Статус:	Новый
Дата утверждения:	«___» _____2023г.
Дата завершения действия:	
Дата аудита:	Ежедневно
Ответственный за аудит:	Эксперт по информационной безопасности

Лист согласования

Должность	Ф.И.О.	Подпись
Директор Административного департамента	Бисенғали Л	
Советник по цифровизации	Тебаев Д.Б.	
и.о. Директора Департамента информационных технологий	Жумажанов Б.Ж.	

1 Назначение документа

1.1 Настоящие Правила использования мобильных устройств и носителей информации (далее – «Правила») предназначена для защиты от рисков при использовании средств связи и переносных устройств при работе с IT инфраструктурой НАО «Университет Нархоз» (далее – «ITA») Некоммерческого акционерного общества «Университет Нархоз» (далее – «Общество»).

1.2 Требования настоящих Правил являются неотъемлемой частью комплекса мер безопасности и защиты информации в Обществе.

1.3 Требования настоящих Правил распространяются на всех работников структурных подразделений, а также работников сторонних организации, использующих в работе средства вычислительной техники и должны применяться для всех средств вычислительной техники, эксплуатируемых в ITA.

2 Глоссарий

2.1 Термины, использованные в настоящем документе, имеют следующие определения:

- **Мобильное устройство** – переносное электронно-вычислительное устройство, способное принимать, отображать, хранить, обрабатывать и передавать информацию.
- **Носитель информации** – любой материальный объект, используемый для хранения и передачи электронной информации.
- **Паспорт ПК** – документ, содержащий полный перечень оборудования и программного обеспечения АРМ.
- **Перечень** – документ «Перечень разрешенного к использованию ПО». Содержит перечень коммерческого свободно распространяемого ПО, разрешенного к использованию в Обществе.
- **ПО вредоносное** – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.
- **ПО коммерческое** – ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.
- **Пользователь** – работник, использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.
- **Эксперт по ИБ** – должностное лицо, осуществляющее комплекс организационно- технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

3 Ссылки

3.1 Настоящие Правила разработаны в соответствии со следующими нормативно-правовыми актами и документами:

- Закон Республики Казахстан «Об информатизации» от 24.11.2015г.;
- Постановление Правительства Республики Казахстан от 20.12.2016г. №832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»;
- СТ РК ИСО/МЭК 27002 «Методы обеспечения защиты. Свод правил по управлению защитой информации»;
- СТ РК ИСО/МЭК 27001 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.

Требования»;

• СТ РК ГОСТ Р 50739 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».

4 Риски использования мобильных устройств и носителей за пределами организациями

4.1 Проблемы с безопасностью использования мобильных устройств и носителей являются несанкционированный доступ к данным и их утечка, а также проникновение злоумышленника через мобильные устройства во внутреннюю сеть Общества (использование внешней сети, кража и т.д.).

4.2 При использовании мобильных устройств и носителей за пределами организации имеется риск распространения служебной информации работниками.

4.3 При использовании мобильных средств в общедоступных местах важно проявлять осторожность, чтобы уменьшить риск «подсмотра» паролей доступа неавторизованными лицами. Следует проявлять осторожность при использовании мобильных средств вычислительной техники и других сервисных средств в общедоступных местах, переговорных комнатах и незащищенных помещениях вне организации.

5 Порядок использования мобильных устройств и носителей информации

5.1 Под использованием мобильных устройств и носителей информации понимается их подключение к инфраструктуре Общества с целью обработки, приема/передачи информации между информационными ресурсами и мобильными устройствами, а также носителями информации.

5.2 В Обществе допускается использование только учтенных мобильных устройств и носителей информации, которые являются собственностью Общества и подвергаются регулярной ревизии и контролю.

5.3 На предоставленных Обществом мобильных устройствах допускается использование коммерческого и свободно распространяемого ПО, входящего в Перечень разрешенного к использованию ПО и указанного в Паспорте ПК.

5.4 К предоставленным Обществом мобильным устройствам и носителям информации предъявляются те же требования по защите информации, что и для стационарных ПК.

5.5 Мобильные устройства и носители информации предоставляются пользователям ІТА Общества по инициативе руководителей структурных подразделений в случаях:

• необходимости выполнения сотрудником своих должностных обязанностей;

• возникновения у сотрудника производственной необходимости.

5.6 Мобильные устройства и носители информации хранятся на складе, предоставление работникам мобильных устройств и носителей информации записываются в журнал выдачи носителей информации (Приложение 1 к Правилам) и закреплены договором по передачи ОС.

5.7 Внос на территорию предоставленных мобильных устройств и носителей информации работниками, а также вынос их за его пределы производится только с письменного разрешения руководства согласно следующим правилам:

• работники и подрядчики, имеющие разрешение на внос/вынос мобильных устройств и носителей информации, должны быть чётко идентифицированы;

• устанавливаются предельные сроки вноса/выноса мобильных устройств и носителей информации;

5.8 При использовании предоставленных работникам мобильных устройств и носителей информации необходимо:

• соблюдать требования настоящих Правил;

• использовать мобильные устройства и носители информации исключительно для выполнения своих служебных обязанностей;

• ставить в известность менеджера по ИБ о любых фактах нарушения требований настоящих Правил;

• эксплуатировать и транспортировать мобильные устройства и носители информации в соответствии с требованиями производителей;

• обеспечивать физическую безопасность мобильных устройств и носителей информации всеми разумными способами;

• извещать специалиста по ИБ и ДИТ о фактах утраты (кражи) мобильных устройств и носителей информации.

5.9 При использовании предоставленных работникам мобильных устройств и носителей информации запрещено:

• использовать мобильные устройства и носители информации в личных целях;

• передавать мобильные устройства и носители информации другим лицам;

• оставлять мобильные устройства и носители информации без присмотра, если не предприняты действия по обеспечению их физической безопасности.

5.10 Любое взаимодействие (обработка, прием/передача информации) инициированное работником Общества неучтенными (личными) мобильными устройствами, а также носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с ответственным за ИБ заранее). Общество оставляет за собой право блокировать или ограничивать использование таких устройств и носителей информации.

5.11 При подозрении работника в несанкционированном или нецелевом использовании мобильных устройств и носителей информации инициируется расследование допущенных нарушений.

5.12 Информация, хранящаяся на мобильных устройствах и носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

5.13 Составление перечня мобильных устройств, носителей информации и их маркировка осуществляется в соответствии с Правилами идентификации, классификации и маркировки активов, связанных со средствами обработки информации.

5.14 В случае увольнения или перевода работника в другое структурное подразделение, предоставленные ему мобильные устройства и носители информации изымаются.

5.15 Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению.

5.16 Уничтожение съемных носителей с конфиденциальной информацией осуществляется при участии работников Общества.

5.17 Вышедшие из употребления носители информации должны утилизироваться способами, не допускающими получения с них информации в каком-либо виде.

5.18 Процедуры безопасной утилизации носителей информации должны сводить к минимуму риск утечки конфиденциальной информации к лицам, которые не должны иметь к ней доступа.

5.19 Процедуры безопасной утилизации носителей информации, содержащих такую информацию, должны быть адекватны степени критичности этой информации.

5.20 Должны быть рассмотрены следующие рекомендации:

• носители информации, содержащие критичную информацию, должны храниться и утилизироваться надежными и безопасными способами, например, сжиганием или измельчением, либо стиранием данных, если они будут затем использоваться в пределах организации для работы с другими приложениями;

• должны быть разработаны и реализованы процедуры по идентификации объектов, которые могут потребовать безопасной утилизации;

• допускается применять групповое уничтожение носителей путем физического уничтожения (измельчение, сжигание, и т.д.);

• услуги по сбору и утилизации бумаги, оборудования и носителей информации предлагаются многими организациями; необходимо соблюдать осторожность при выборе подходящего контрагента с адекватными средствами управления и опытом или воспользоваться рекомендациями компетентных органов;

• при утилизации носителей, содержащих конфиденциальную (критичную) информацию, должны составляться отчеты. Эти отчеты затем следует использовать при аудиторских проверках.

5.21 Утилизацию носителей необходимо производить периодически. Не следует накапливать большие объемы предназначенных для утилизации носителей. При этом возможно проявление эффекта агрегирования, заключающегося в том, что большое количество открытой, несекретной информации, собранное воедино, может быть успешно использовано для поиска конфиденциальной информации методом сопоставимости.

5.22 Утилизацию носителей не следует считать «третьесортным» процессом и выполнять ее надо со всей тщательностью.

5.23 По результатам уничтожения носителей составляется акт по прилагаемой форме (Приложение 2 к настоящим Правилам).

6 **Ответственность**

6.1 В случае нарушения требований настоящих Правил работники привлекаются к административной или иной ответственности в соответствии с действующим законодательством Республики Казахстан.

7. Заключительные положения

7.1. Настоящие Правила утверждаются решением Правления.

7.2. Изменения и дополнения в Правила вносятся решением Правления

Приложение 1

Журнал выдачи носителей информации

№. п/ п	Вид носителя информации	Учетный номер носителя	Дата выдачи	Кому выдано (ФИО, должность, подразделение, подпись)	ФИО, подпись материального ответственного лица	Примечание

Приложение 2

АКТ УНИЧТОЖЕНИЯ
ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

Мы, нижеподписавшиеся:

1._____;
(должность, фамилия и инициалы)

2._____;
(должность, фамилия и инициалы)

составили настоящий акт в том, что перечисленные в нем электронные носители информации подлежат уничтожению как утратившие практическое значение и непригодные для перезаписи:

№. п/п	Вид носителя информации	Учетный номер носителя	Дата поступления	Краткое содержание

Всего подлежит списанию и уничтожению _____информации.
_____ наименований электронных носителей

«___»___20г. Подписи:

1._____

2._____

Правильность произведенных записей в акте проверил:

_____
(подпись)

Электронные носители информации перед уничтожением сверили с записями в акте и полностью уничтожили путем

_____

_____

«___» _____20г.

Подписи:

1. _____

Акт составлен в ___ экземплярах

ЛИСТ ОЗНАКОМЛЕНИЯ

№	Фамилия, имя, отчество	Должность	Подпись	Дата
1	2	3	4	5