«УТВЕРЖДЕНО»
Решением Правления
НАО «Университет Нархоз»
Протокол № 6 от
«15». 06 .2023 г.

Правила парольной политики IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»

Алматы, 2023

Оглавление

Паспорт документа

Наименование документа:	Правила парольной политики IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»
Краткое описание:	Правила парольной политики IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»
Тема:	Информационная безопасность
Статус:	Новый
Дата утверждения:	«___» _____2023г.
Дата завершения действия:	
Дата аудита:	Ежемесячно
Ответственный за аудит:	Эксперт по информационной безопасности

Лист согласования

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

1 Общие положения

1.1 Настоящие Правила парольной политики Некоммерческого акционерного общества «Университет Нархоз» (далее – «Правила») разработана в соответствии с законодательством Республики Казахстан, требованиями международных стандартов управления информационной безопасностью, стандартом по информационной безопасности ТОО «Verny Capital», Положением информационной безопасностью НАО «Университет Нархоз», Уставом и иными внутренними документами Некоммерческого акционерного общества «Университет Нархоз» (далее – «Общество»).

1.2 Правила определяет основные принципы, направления и требования по защите информации, является основой для обеспечения режима информационной безопасности.

1.3 Цель Правил – обеспечение и защиты объектов IT инфраструктуры, автоматизированных информационных систем, Общества, минимизация рисков внешнего проникновения, обеспечение бесперебойной работы информационных систем.

2 Ссылки

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

- Закон Республики Казахстан «Об информатизации» от 24.11.2015г.;
- Постановление Правительство Республики Казахстан от 20 декабря 2016 года №832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечение 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»;
- Стандарт по информационной безопасности ТОО «Verny Capital» VC 04.04.2022.

3 Термины и определения

2.2 В настоящих Правилах используются следующие термины:

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Безопасность информации – защищенность информации от ее нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного ее тиражирования.

Доступность – возможность для авторизованного пользователя автоматизированной информационной системы за приемлемое время получить информационную услугу, предусмотренную функциональностью.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная безопасность – комплекс административно-правовых, организационно-распорядительных и технических мер, направленные на обеспечение конфиденциальности, целостности и санкционированной доступности информации в процессе ее сбора, обработки, передачи и хранения.

Конфиденциальность – защита от несанкционированного ознакомления.

Лог-файлы сервера – специальные файлы, в которых протоколируются определенные действия пользователя или программы на сервере.

Несанкционированное действие – действие субъекта в нарушение установленных в системе правил обработки информации.

Пользователь – работник, обучающийся, субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации.

Сеть (локальная сеть, ЛВС, LAN) – группа точек, узлов или других устройств, соединенных коммуникационным набором оборудования, обеспечивающих соединение станций и передачу между ними информации.

Риски информационной безопасности – реально или потенциально возможные действия по реализации опасных воздействующих факторов с целью преднамеренного или случайного нарушения режима функционирования объекта.

Уязвимость – любая характеристика автоматизированной системы, использование которой может привести к реализации угроз.

Целостность информации – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому ее состоянию).

Шифрование – преобразование данных в нечитабельную форму, используя ключи шифрования-расшифровки.

4 Область применения Политики

4.1. Настоящая Политика относится ко всему административно-управленческому персоналу, преподавателям и студентам Общества при использовании почтовых адресов, учетных записей с целью недопущения утечки и сохранения служебной, в том числе и конфиденциальной информации

5 Инструкции по созданию паролей

5.1. При создании новой учетной записи в информационной системе группы А.В.С. а также регистрации на почтовом сервере gmail@narxoz.kz пользователь должен руководствоваться следующими основными критериями:

5.1.1. Создаваемый пароль должен быть уникальным по своему содержанию и защите;

5.1.2. Пароль не должен быть коротким по количеству символов и содержать не менее 12 символов разных значений;

5.1.3. Пароль должен содержать в себе заглавные и строчные буквы, на латинице, обязательное использование цифр и специальных символов (*@#&* к примеру Nnaderoom15689@*);

5.1.4. При создании паролей необходимо избегать сведений содержащие паспортные данные, клички животных, имена друзей, работников, названия сайтов, место работы;

5.1.5. Пароль необходимо использовать только в течение последовательных 90 (девяносто) дней, по его истечению его необходимо поменять, при не смене пароля доступ к информационным ресурсам будет недоступен;

5.1.6. При отсутствии работника на рабочем месте более 15 (пятнадцать) последовательных минут доступ к его компьютеру автоматически ограничивается;

5.1.7. Количество неудачных попыток входа в информационные системы ограничивается 5 (пятью) последовательными попытками. В случае неудачных попыток входа учетная запись автоматически блокируется. С целью разблокировки учетной записи

пользователь обращается к менеджеру по ИБ для фиксации инцидента в журнале и к работникам Департамента информационных технологий для восстановления доступа к учетной записи.

6 Основные принципы Политики

6.1. Каждый пользователь должен помнить, что пароли являются персональной информацией конфиденциальны по своему содержанию и действиям. В частности запрещается:

6.1.1. Передавать свой пароль посредством мобильного телефона и иных электронных дивайсов;

6.1.2. Сохранять свой пароль на рабочем столе компьютера;

6.1.3. Не сообщать свой пароль своим родственникам, коллегам, друзьям, непосредственному руководству, иным лицам;

6.1.4. Не указывать свой пароль в опросниках и иных формах коммуникациях;

6.1.5. Не использовать функцию «Запомнить пароль» при входе в свою учетную запись;

6.1.6. При завершении работы со своей учетной записью обязательно осуществить выход.

7 HR контроль

7.1. При расторжении трудового договора с работником Отдел кадрового администрирования должен незамедлительно оповестить администратора информационных ресурсов о данном факте для блокировки доступа к учетной записи.

7.2. В случае выхода работника в отпуск доступ к учетной записи приостанавливается на период нахождения работника в отпуске.

7.3. При выходе на больничный или во внеочередной отпуск учетная запись к информационным ресурсам приостанавливается до получения официального запроса от Отдела кадрового администрирования.

7.4. При расторжении трудового договора с работником в обходном листе должна стоят роспись администратора с передачей паролей от учетной записи пользователя, в том числе, от почтового сервера.

8 Ответственность

8.1. Пользователи, соглашаясь и принимая положения настоящей Политики, несут персональную ответственность в соответствии с действующим законодательством Республики Казахстан.

8.2. Эксперт по информационной безопасности и руководитель Департамента информационных технологий несут ответственность за обеспечение условий, необходимых для реализации настоящей Политики.

9 Заключительные положения

9.1. Настоящая Политика утверждается решением Правления Университета.

9.2. Изменения и дополнения в настоящую Политику вносятся на основании решения Правления Университета.