«УТВЕРЖДЕНО»
Решением Правления
НАО «Университет Нархоз»
Протокол № 8 от
«15» 06 .2023 г.

Правила использования сети интернета и электронной почты Некоммерческого акционерного общества «Университет Нархоз»

Алматы, 2023

Оглавление

Паспорт документа

Наименование документа:	Правила использования сети интернета и электронной почты Некоммерческого акционерного общества «Университет Нархоз»
Краткое описание:	Правила использования сети интернета и электронной почты Некоммерческого акционерного общества «Университет Нархоз»
Тема:	Информационная безопасность
Статус:	Новый
Дата утверждения:	«___» _____2023г.
Дата завершения действия:	
Дата аудита:	Каждые 45 дней
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. Общие положения

1.1. Настоящие Правила использования сети интернет и электронной почты (далее – « Правила») регламентируют порядок работы с электронной почтой и службой Интернет, а также процесс управления доступом, обеспечения безопасности и проверки работы корпоративной электронной почтой, Интернет и службами Интернет-сообщений (Whatsapp, Skype, Gmail.com Telegramm и т.п.) в Некоммерческом акционерном обществе «Университет Нархоз» (далее – «Общество»).

2. Порядок доступа работников к ресурсам Интернета и электронной почте

2.1 Доступ к интернет-ресурсам предоставляется всем работникам Общества, которые ознакомились с Политикой информационной безопасности Общества и настоящей Инструкцией.

2.2 Ознакомление с указанными документами осуществляет Ответственный за ИБ, о чем делается запись в листе ознакомления за подписью работника Общества.

2.3 Подключение пользователей к Интернету осуществляется только через локальную вычислительную сеть.

2.4 Запрещены к загрузке файлы, имеющие расширения из списка, указанного в Приложении 1 к настоящей Инструкции. Доступ на загрузку файлов с данными расширениями из сети интернет предоставляется только по согласованию со специалистом по ИБ.

2.5 После установки или настройки программного обеспечения для работы с сетью Интернет и(или) электронной почтой сотруднику запрещается изменение любых параметров, касающихся подключения к серверам сети.

2.6 Пользователям Интернета запрещается:

- использование ресурсов Интернета для хранения закрытой и конфиденциальной информации;
- использование ресурсов Интернета и электронной почты в неслужебных целях;
- копирование из Интернета любых программ, архивов и данных, не имеющих прямого отношения к служебным обязанностям работника;
- предоставление доступа к сети Интернет с использованием данных своей учетной записи другим лицам;
- подписка по электронной почте на различные рекламные материалы, листы рассылки, электронные журналы и т.п., не связанные с выполнением пользователем функциональных обязанностей;
- открытие (запуск на выполнение) файла, полученного из сети Интернет или по электронной почте, без предварительной проверки его антивирусным программным обеспечением;
- загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;
- использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, запрещенному к использованию политикой информационной безопасности.

2.7 При работе с корпоративной электронной почтой работникам Общества запрещается:

- создавать оскорбительные или провокационные сообщения, содержащие сексуальные домогательства, расовые оскорбления, дискриминацию по половому признаку или другие комментарии, затрагивающие в оскорбительной форме вопросы возраста или сексуальной ориентации, религиозные или политические пристрастия, национальность или состояние здоровья, а также другую информацию, запрещенную законодательством Республики Казахстан;

• использовать вложения графических, видео, исполняемых и т.п. файлов, не относящихся к служебной деятельности, а также файлов, размер которых превышает установленный в требованиях;

• запрашивать и отправлять в открытом виде или с использованием зарубежных почтовых серверов сведения, составляющие служебную и/или конфиденциальную информацию с ограниченным доступом (передача разрешена только с использованием шифровальных средств – средств криптографической защиты информации);

• пользоваться групповой рассылкой в личных целях;

• использовать ресурсы для рассылки писем-пирамид, писем счастья, сообщений рекламного характера и другой подобной информации, не имеющей отношения к служебной деятельности;

• распространять вредоносные файлы и программы, а также программное обеспечение и материалы, защищенные авторским правом;

• использовать учетные записи других почтовых систем и пользователей;

• получать доступ к электронным сообщениям других пользователей (за исключением случаев, санкционированных руководством).

2.8 При нарушении вышеназванных пунктов, пользователь без предупреждения отключается от работы в сети Интернет, при этом в известность ставится его непосредственный руководитель.

2.9 Мониторинг и контроль доступа в Интернет осуществляется ответственным за ИБ.

2.10 Доступ к ресурсам Интернет и серверу электронной почты может быть блокирован без предварительного уведомления, при возникновении внештатных ситуаций, либо в иных случаях, предусмотренных организационными документами.

2.11 Все сотрудники, подрядчики и потребители от третьей стороны должны следовать правилам приемлемого использования информации и активов, связанных со средствами обработки информации, включая правила применения электронной почты и Интернета.

2.12 Работники Общества:

• не разглашают присвоенное им имя пользователя и пароль;

• не предоставляют доступ в интернет с закрепленного за ними ПК другим сотрудникам Общества и третьим лицам;

• не открывают или не запускают любые файлы с расширениями, указанными в приложении 1 к настоящим Правилам, а также не заходят на интернет-ресурсы, указанные в приложении 2 к настоящим Правилам.

2.13 Пользователь несет персональную ответственность за сохранение в тайне основного пароля электронной почты. Запрещается сообщать пароль другим лицам, записывать его, а также пересылать открытым текстом в электронных сообщениях.

2.14 Восстановление забытого пароля электронной почты пользователя осуществляется администратором путем изменения (сброса) пароля пользователя на основании письменной либо электронной заявки пользователя.

2.15 Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

3 Требования к оформлению электронного сообщения

3.1 При оформлении электронного сообщения необходимо заполнять следующие поля:

• адрес получателя;

• тема электронного сообщения;

• текст электронного сообщения (при необходимости, могут быть вложены различные файлы);

• подпись отправителя.

Формат подписи отправителя:

С уважением,
<фамилия имя>
<должность>
<структурное подразделение
Общества>
<наименование Общества>
<адрес>
<номера телефонов,
мессенджеры,
адреса электронной почты>
<сайт>

3.2 Почтовый клиент должен предусматривать возможность создания подписи и автоматической вставки ее в электронное сообщение, а также возможность создания нескольких подписей для различных получателей.

3.3 При формировании ответов на полученные электронные сообщения можно использовать упрощенную подпись.

3.4 Перед отправкой электронного сообщения пользователю необходимо проверять правильность введенного адреса получателя.

4 **Ответственность за нарушение требований Правил**

4.1 Настоящие Правила обязательны для выполнения всеми работниками Общества. Руководитель подразделения обязан ознакомить каждого работника подразделения с настоящими Правилами под роспись.

4.2 Департамент информационных технологий под контролем эксперта по ИБ осуществляет плановые/внеплановые проверки правильности использования доступа в сеть Интернет и использования электронной почты.

4.3 Эксперт по ИБ проводит анализ инцидентов информационной безопасности по фактам нарушений требований защиты информации при работе с электронной почтой, интернет и службами интернет-сообщений.

4.4 За неисполнение или ненадлежащее исполнение настоящих Правил работники несут дисциплинарную ответственность в соответствии с действующим законодательством Республики Казахстан.

5 Заключительные положения

5.1 Настоящие Правила утверждаются решением Правления Университета.

5.2 Изменения и дополнения в настоящие Правила вносятся на основании решения Правления Университета.

Приложение 1
к правилам использования сети интернета
и электронной почты

Список расширений файлов, запрещенных к загрузке из сети Интернет

ace	bpl	it	miz	mtm	Tar	Wax
aif	cab	itz	mod	nsv	Tgz	Wm
aifc	cda	lh	mov	ogg	Tif	Wma
aiff	com	lha	mp1	pls	uc2	wmv
arj	dat	lzh	mp2	rar*	ult	wmx
asf	divx	m1v	mp3	rmi	umx	wvx
asx	dll	m2v	mp4	s3m	uue	
au	xmz	m3u	mpa	s3z	vob	
avi	exe	mdz	mpe	snd	voc	
b4s	gz	mid	mpeg	Stm	Wal	
bat	ifo	midi	mpg	Stz	Wav	

*доступ предоставляется если файл скачивается с официального интернет ресурса

Приложение 2
к правилам использования сети интернета
и электронной почты

Перечень запрещенных к использованию в Обществе Интернет-ресурсов

№ п.п.	Название категории (на английском языке)	Название категории (на русском языке)	Описание категории
1	**Games**	**Игры**	Интернет-ресурсы, посвященными электронным играм, видео играм, компьютерным игры, ролевым играм, и онлайн-играм.
2	**Meaningless Content**	**Бессмысленный контент**	URL-адреса, которые не могут быть окончательно классифицированы из-за отсутствия или неоднозначного содержания.
3	**Social Networking**	**Социальные сети**	Дружеское общение, онлайн-знакомства, личные объявления, службы знакомств, клубы и т.д.
4	**Web Chat**	**Веб-чат**	Веб-чаты
5	**Freeware and Software Downloads**	**Бесплатные сетевые загрузки**	Интернет-ресурсы, основная функция которых заключается в предоставлении бесплатных загрузок (загрузок программного обеспечения). Мелодии на сотовый телефон / фото / игры, обновления программного обеспечения для бесплатного скачивания, все включены в эту категорию.
6	**Adult Materials**	**Взрослые материалы**	Интернет-ресурсы, содержащие информацию для взрослых (18 лет и старше), которые показывают или продвигают сексуальность, стрип-клубы, секс-шопы и т.д., исключая половое воспитание, без намерения сексуально возбуждать.
7	**Alcohol**	**Алкоголь**	Интернет-ресурсы, которые законно продвигают или продают алкогольную продукцию и аксессуары.
8	**Alternative Beliefs**	**Альтернативные убеждения**	Интернет-ресурсы, которые предоставляют информацию о религиях или продвигают религии, не указанные в традиционных религиях или другие нетрадиционные, культовые или фольклорные верования и практики. Интернет-ресурсы, которые способствуют или предлагают методы, средства обучения или другие ресурсы, с целью повлиять на реальные события с помощью заклинаний, проклятий, магических сил, сатанинских или сверхъестественных существ.
9	**Dating**	**Знакомства**	Интернет-ресурсы, которые размещают или содействуют знакомству, межличностным отношениям и связанные с ними материалы.

10	**Extremist Groups**	**Экстремистские группы**	Интернет-ресурсы, которые показывают радикальные милитаристические группировки или движения с агрессивными антиправительственными убеждениями или верованиями.
11	**Gambling**	**Азартные игры**	Интернет-ресурсы, которые содержат азартные игры, такие как пари, лотереи, казино, включая игровую информацию, инструкции и статистику.
12	**Marijuana**	**Марихуана**	Интернет-ресурсы, которые предоставляют информацию о марихуане или способствуют ее выращиванию, приготовлению и использованию.
13	**Nudity and Risque**	**Нагота и непристойность**	Интернет-ресурсы, содержащие информацию для взрослых (18 лет и старше), которые изображают человеческое тело в полной или частичной наготе без намерения сексуально возбуждать.
14	**Pornography**	**Порнография**	Интернет-ресурсы, содержащие информацию для взрослых (18 лет и старше), которые представляют или отображают половые акты с намерением сексуально возбуждать.
15	**Tobacco**	**Табачные изделия**	Интернет-ресурсы, которые законно продвигают или продают табачные изделия и аксессуары
16	**Weapons (sales)**	**Оружие, вооружение (продажа)**	Интернет-ресурсы, которые имеют законные основания на продвижение или продажу оружия, такие как пистолеты, ножи, ружья, взрывчатые вещества и т.д.
17	**Child Abuse**	**Жестокое обращение с детьми/насилие над ребенком**	Интернет-ресурсы, которые были проверены фондом Internet Watch Foundation (IWF) и содержат или распространяют изображения несовершеннолетних детей, находящихся в состоянии жестокого обращения. Информация о фонде IWF доступна по адресу: http://www.iwf.org.uk/.
18	**Discrimination**	**Дискриминация**	Интернет-ресурсы, которые способствуют выявлению расовых групп, унижению или подчинению групп, или превосходства любой группы.
19	**Drug Abuse**	**Злоупотреблении наркотиками**	Интернет-ресурсы, которые показывают информацию о незаконной деятельности с наркотиками, включающую: рекламу наркотических средств, приготовление, выращивание, торговлю, распространение, подстрекательство и т.д.
20	**Hacking**	**Деятельность хакеров; несанкционированная попытка доступа**	Интернет-ресурсы, которые изображают незаконную деятельность, связанную с несанкционированной модификации или несанкционированным доступом к программам, компьютерам, оборудованию и веб-сайтам.

21	**Illegal or Unethical**	**Незаконные или неэтичные**	Интернет-ресурсы, которые показывают информацию, методы и инструкции мошеннических действий или противоправного поведения (ненасильственного), таких как мошенничество, альшивомонетничество, уклонение от уплаты налогов, мелкие кражи, шантаж и т.п.
22	**Proxy Avoidance**	**Анонимные прокси-сервера**	Интернет-ресурсы, которые предоставляют информацию или инструменты о том, как обойти контроль доступа в Интернет и просматривать веб- страницы анонимно, включают в себя анонимные прокси-сервера.
23	**Violence**	**Насилие**	К этой категории относятся сайты, которые изображают оскорбительные материалы о жестокости, смерти, актах насилия, увечьях и т.д.
24	**Malicious Websites**	**Вредоносные сайты**	Интернет-ресурсы, размещающие программное обеспечение, которое скрытно скачивается на компьютер пользователя для сбора информации и мониторинга активности пользователей и сайты, зараженные разрушительными или вредоносными программами, специально разработанными для повреждения, нарушения, атаки или управления компьютерными системами без согласия пользователя, такие как вирус или троян.
25	**Phishing**	**Фишинг**	Поддельные веб-страницы, которые дублируют законные веб-страницы компаний с целью выявления финансовой, личной или другой конфиденциальной информации от пользователей.
26	**Spam URLs**	**Спам адреса**	Интернет-ресурсы или веб-страницы, адреса которых находятся в спам-письмах. Эти веб-страницы часто рекламируют секс-сайты, мошеннические товары, а также другие потенциально оскорбительные материалы.

ЛИСТ ОЗНАКОМЛЕНИЯ

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