АСТАНА ҚАЛАСЫ
ӘКІМДІГІНІҢ «№2 КӨПБЕЙІНДІ
ҚАЛАЛЫҚ БАЛАЛАР АУРУХАНАСЫ»
ШАРУАШЫЛЫҚ ЖҮРГІЗУ
ҚҰҚЫҒЫНДАҒЫ МЕМЛЕКЕТТІК
КОММУНАЛДЫҚ КӘСІПОРНЫ

ГОСУДАРСТВЕННОЕ
КОММУНАЛЬНОЕ ПРЕДПРИЯТИЕ
НА ПРАВЕ ХОЗЯЙСТВЕННОГО ВЕДЕНИЯ
«МНОГОПРОФИЛЬНАЯ ГОРОДСКАЯ
ДЕТСКАЯ БОЛЬНИЦА №2»
АКИМАТА ГОРОДА АСТАНА

БҰЙРЫҚ

26.08.2026 № 106-О
Астана қаласы

ПРИКАЗ

№_____
город Астана

Об утверждении Положения о кибербезопасности ГКП на ПХВ «Многопрофильная городская детская больница №2» акимата города Астаны и назначения ответственных за соблюдение правил кибербезопасности.

В соответствии с пунктом 2 статьи 22, подпунктом 25-1) пункта 2 статьи 23 Трудового кодекса Республики Казахстан, Законом Республики Казахстан от 24 ноября 2015 года № 418-V «О кибербезопасности», Положением о кибербезопасности ГКП на ПХВ «Многопрофильная городская детская больница №2» акимата города Астаны, а также в целях организации соблюдения требований кибербезопасности в ГКП на ПХВ «Многопрофильная городская детская больница №2» акимата города Астаны (далее — Предприятие), **ПРИКАЗЫВАЮ:**

1.Утвердить Положение о кибербезопасности ГКП на ПХВ «Многопрофильная городская детская больница №2» акимта города Астаны (далее — Положение).

2.Ввести в действие Положение о кибербезопасности с 26 августа 2026 года.

3. Назначить ответственным за организацию работы по обеспечению кибербезопасности в Предприятие начальника отдела информационного обеспечения.

4.Возложить на ответственного, указанного в пункте 3 настоящего приказа, следующие обязанности:

4.1.) организация разработки, актуализации и утверждения внутренних актов Предприятия по кибербезопасности;

000658

4.2.) координация взаимодействия структурных подразделений Предприятии по вопросам кибербезопасности;

4.3.) организация обучения работников и повышения их осведомленности по вопросам кибербезопасности не реже одного раза в год, а также дополнительно — после существенного обновления акта или выявленного инцидента;

4.4.) представление руководителю Предприятия отчета о состоянии кибербезопасности и результатах внутреннего контроля не реже одного раза в год.

5. Назначить ответственным за ознакомление работников с Положением о кибербезопасности под подпись, включая новых работников при приеме на работу, руководителя отдела управления человеческими ресурсами.

6.Назначить ответственным за техническое обеспечение кибербезопасности, мониторинг и реагирование на инциденты кибербезопасности начальника отдела информационного обеспечения в том числе за:

6.1.) технический мониторинг соблюдения требований кибербезопасности (сложность паролей, наличие антивирусной защиты, своевременность обновлений программного обеспечения и другое);

6.2) прием и первичную обработку сообщений работников о подозрительной активности и инцидентах кибербезопасности;

6.3.) уведомление уполномоченного органа в сфере защиты персональных данных в случаях и сроки, предусмотренные законодательством Республики Казахстан, при инцидентах, связанных с нарушением безопасности персональных данных.

7. Ответственным лицам, указанным в пунктах 3 и 5 настоящего приказа, ознакомиться с настоящим приказом под подпись.

8. Контроль за исполнением настоящего приказа оставляю за собой

Директор **Г.Кулушева**

КЕЛІСУ ПАРАҒЫ /ЛИСТ СОГЛАСОВАНИЯ

2026 жылғы «___» _____ №____ бұйрыққа
К приказу от «___» _____ 2026 г. №____

Атауы /Наименование	Құрылымдық бөлімшеніңатауы/ Наименованиеструктурногоподразделения	Т.А.Ж., жауаптытұлғаныңқолы, Визаныңқойылғанкүні /Ф.И.О., подписьответственноголица, датавизирования	НақтыорындаушынынҢ ауазымы, Т.А.Ж., қолы, визаныңқойылғанкүні /Должность, Ф.И.О., подписьконкретногоисполнителя, датавизирования
ӘЗІРЛЕУ/ РАЗРАБОТКА	Адам ресурстарын басқару бөлімі	Кадирова Е.А Бөлім басшысы	
КЕЛІСУ/ СОГЛАСОВАНИЕ	Ұйымдастыру-құқықтық бөлімі	Бакижанова Д.Д. Бөлім басшысы	
МЕМ/ОРЫС/ТІЛІНЕ АУДАРУ/ПЕРЕВОД НА ГОС./РУССКИЙ/ЯЗЫК			
ТІРКЕУ/ РЕГИСТРАЦИЯ			
ЖІБЕРУ/ РАССЫЛКА			

Утверждено
приказом директора больницы
от « 26 » августа 2026 года №106-ө

ПОЛОЖЕНИЕ

о кибербезопасности ГКП на ПХВ «Многопрофильная городская детская больница №2» акимата города Астаны

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящим Положением устанавливаются требования кибербезопасности при использовании цифровых объектов работниками ГКП на ПХВ «Многопрофильная городская детская больница №2» акимата города Астаны (далее Предприятие), порядок ознакомления работников с этими требованиями и порядок контроля за их соблюдением.

2. Положение разработано в соответствии с Трудовым кодексом Республики Казахстан (пп. 3) п. 2 ст. 22, пп. 25-1) п. 2 ст. 23), Кодексом Республики Казахстан от 9 января 2026 года № 255-VIII «Цифровой кодекс Республики Казахстан», Законом Республики Казахстан от 24.11.2015 № 418-V «О кибербезопасности» и Законом Республики Казахстан от 21.05.2013 № 94-V «О персональных данных и их защите».

3. Настоящее Положение обязательно для исполнения всеми работниками Предприятия независимо от занимаемой должности, включая работников, работающих на условиях дистанционной работы, а также лиц, привлеченных к работе по гражданско-правовым договорам, если это прямо предусмотрено таким договором.

4. В настоящем Положении используются следующие основные понятия:

1) кибербезопасность – состояние защищенности цифровых объектов (компьютеров, сетей, программ, данных в электронной форме) от нарушения их конфиденциальности, целостности или доступности;

2) цифровой объект – обособленный элемент цифровой среды, созданный, используемый или передаваемый посредством цифровых технологий (компьютеры, серверы, программное обеспечение, учетные записи, данные в электронной форме), обладающий уникальными цифровыми характеристиками и позволяющий субъектам цифровой среды осуществлять правомочия владения, пользования либо распоряжения в объёме, установленном законодательством Республики Казахстан;

3) инцидент кибербезопасности – событие или совокупность событий, негативно влияющих на кибербезопасность цифрового объекта (заражение

вредоносным ПО, утечка данных, несанкционированный доступ, потеря устройства и т. п.);

4) конфиденциальность – состояние, при котором доступ к информации имеют только лица, которым он разрешён;

5) целостность – состояние, при котором данные не могут быть изменены или уничтожены без соответствующего разрешения;

6) доступность – состояние, при котором лица, имеющие право доступа к данным и ресурсам, могут получить его в нужный момент.

5. Требования настоящего Положения не заменяют собой более строгие требования по обеспечению кибербезопасности, установленные для Предприятия законодательством Республики Казахстан, если Предприятие является собственником или владельцем информационных систем либо объектов критически важной информационно-коммуникационной инфраструктуры (см. п. 40 настоящего Положения).

2. ПРАВА И ОБЯЗАННОСТИ СТОРОН

6. Работодатель обязан:

1) утвердить настоящее Положение и обеспечить его актуальность;

2) назначить приказом лицо (лиц), ответственное за организацию обеспечения кибербезопасности в Предприятия (далее по тексту – Ответственное лицо);

3) ознакомить каждого работника с настоящим Положением под подпись до начала выполнения им трудовых обязанностей либо непосредственно после утверждения или изменения Положения (для уже работающих сотрудников);

4) обеспечить работников необходимыми техническими и программными средствами защиты (антивирусное программное обеспечение, средства резервного копирования и т. п.);

5) организовать обучение работников основам кибербезопасности не реже одного раза в год;

6) осуществлять внутренний контроль за соблюдением требований настоящего Положения.

7. Работник обязан:

1) соблюдать требования настоящего Положения и иных актов Предприятия по вопросам кибербезопасности;

2) незамедлительно сообщать Ответственному лицу о выявленных инцидентах кибербезопасности или признаках, указывающих на их возможное наступление;

3) не предпринимать самостоятельных действий по устранению инцидента кибербезопасности, кроме случаев, прямо согласованных с Ответственным лицом;

4) проходить обучение и инструктажи по вопросам кибербезопасности, организуемые Работодателем.

8. Работник имеет право обращаться к Ответственному лицу за разъяснениями по вопросам применения настоящего Положения.

9. Ответственное лицо:

1) осуществляет внутренний контроль за соблюдением работниками требований настоящего Положения;
2) организует ознакомление работников с настоящим Положением и последующими изменениями к нему;
3) принимает сообщения о выявленных инцидентах кибербезопасности и организует реагирование на них в порядке, установленном разделом 5 настоящего Положения;
4) готовит предложения по актуализации настоящего Положения.

3. ПРАВИЛА ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ

10. Пароли и учетные записи:
1) пароль должен содержать не менее 8 символов, включая буквы разного регистра, цифры и специальные символы;
2) пароль подлежит обязательной смене не реже одного раза в 90 календарных дней, а также незамедлительно, при подозрении на его компрометацию;
3) работникам запрещается передавать свои учётные данные (логин, пароль) от корпоративных систем, почты, программного обеспечения и устройств третьим лицам, включая коллег и руководителей;
4) запрещается записывать пароли на бумажных носителях или хранить их в незащищённых электронных файлах;
5) каждый работник несет персональную ответственность за сохранность своих учетных данных и за все действия, совершённые под его учётной записью;
6) для запоминания разных сложных паролей рекомендовано использовать «метод двойного пароля»: один короткий секретный элемент держать в памяти и никогда не записывать, а к нему добавлять свою заготовку под конкретный сервис;
7) не рекомендуется хранить рабочие пароли в браузере или в личных менеджерах паролей, установленных без согласования с Ответственным лицом. При компрометации устройства или очистке данных браузера такие пароли могут быть потеряны или похищены.
11. Работа с электронной почтой и подозрительными сообщениями:
1) работникам запрещается открывать вложения и переходить по ссылкам из писем от неизвестных или подозрительных отправителей;
2) при получении письма, вызывающего подозрение (в том числе с признаками фишинга (подробные признаки фишинга см. в Приложении 2 к настоящему Положению)), работник обязан не совершать с ним никаких действий и незамедлительно сообщить о нём Ответственному лицу;
3) корпоративная электронная почта предназначена исключительно для служебных целей;
4) если подозрительное письмо уже открыто, работник не должен переходить по ссылкам, скачивать вложения, вводить данные или пересылать письмо коллегам обычным способом;

1) осуществляет внутренний контроль за соблюдением работниками требований настоящего Положения;
2) организует ознакомление работников с настоящим Положением и последующими изменениями к нему;
3) принимает сообщения о выявленных инцидентах кибербезопасности и организует реагирование на них в порядке, установленном разделом 5 настоящего Положения;
4) готовит предложения по актуализации настоящего Положения.

3. ПРАВИЛА ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ

10. Пароли и учетные записи:
1) пароль должен содержать не менее 8 символов, включая буквы разного регистра, цифры и специальные символы;
2) пароль подлежит обязательной смене не реже одного раза в 90 календарных дней, а также незамедлительно, при подозрении на его компрометацию;
3) работникам запрещается передавать свои учётные данные (логин, пароль) от корпоративных систем, почты, программного обеспечения и устройств третьим лицам, включая коллег и руководителей;
4) запрещается записывать пароли на бумажных носителях или хранить их в незащищённых электронных файлах;
5) каждый работник несет персональную ответственность за сохранность своих учетных данных и за все действия, совершённые под его учётной записью;
6) для запоминания разных сложных паролей рекомендовано использовать «метод двойного пароля»: один короткий секретный элемент держать в памяти и никогда не записывать, а к нему добавлять свою заготовку под конкретный сервис;
7) не рекомендуется хранить рабочие пароли в браузере или в личных менеджерах паролей, установленных без согласования с Ответственным лицом. При компрометации устройства или очистке данных браузера такие пароли могут быть потеряны или похищены.
11. Работа с электронной почтой и подозрительными сообщениями:
1) работникам запрещается открывать вложения и переходить по ссылкам из писем от неизвестных или подозрительных отправителей;
2) при получении письма, вызывающего подозрение (в том числе с признаками фишинга (подробные признаки фишинга см. в Приложении 2 к настоящему Положению)), работник обязан не совершать с ним никаких действий и незамедлительно сообщить о нём Ответственному лицу;
3) корпоративная электронная почта предназначена исключительно для служебных целей;
4) если подозрительное письмо уже открыто, работник не должен переходить по ссылкам, скачивать вложения, вводить данные или пересылать письмо коллегам обычным способом;

5) о письме следует сообщить Ответственному лицу, приложив его в качестве вложения, а не пересылкой исходного текста.

12. Программное обеспечение и устройства:

1) на рабочих устройствах допускается использование только лицензионного и предварительно согласованного с Ответственным лицом программного обеспечения;

2) самостоятельная установка, удаление или изменение настроек программного обеспечения без согласования с Ответственным лицом запрещается;

3) работник обязан блокировать экран рабочего устройства при каждом (даже кратковременном) отходе от рабочего места;

4) использование внешних съёмных носителей информации (флеш-накопителей, внешних дисков) для работы со служебной информацией допускается только с предварительного разрешения Ответственного лица;

5) для быстрой блокировки рабочего устройства используются стандартные сочетания клавиш (Windows – WIN + L, macOS – CTRL + CMD + Q);

6) запрещается подключать к рабочим устройствам неизвестные съёмные носители (в том числе найденные в офисе или полученные от посторонних лиц) без предварительной проверки антивирусом или согласования с Ответственным лицом;

7) перед скачиванием файлов или вводом данных на незнакомом сайте необходимо проверить правильность написания его адреса (домена) и наличие защищённого соединения (значок замка в адресной строке браузера).

13. При получении в мессенджерах или по телефону сообщений и звонков с просьбой сообщить пароли, коды, персональные или финансовые данные, а также совершить срочный платёж, работник обязан проявить повышенную осторожность, поскольку такие обращения могут являться попыткой мошенничества, в том числе от имени директора или коллег Предприятия. Признаками возможного мошенничества являются (см. также Приложение 2 к настоящему Положению):

1) обращение с незнакомого номера или аккаунта, в том числе оформленного под имя и фотографию знакомого работнику лица;

2) требование срочно и без промедления совершить действие, создание атмосферы спешки и давления;

3) несвойственный привычному собеседнику стиль общения (например, резкая смена обращения на «Вы» и по имени-отчеству);

4) просьба сохранить обращение в тайне от руководителя или коллег.

14. При возникновении сомнений в подлинности обращения работник обязан:

1) связаться с предполагаемым отправителем по заведомо известному контакту (например, позвонить самому, а не по номеру из подозрительного сообщения), чтобы уточнить, действительно ли запрос направлен им;

2) ни при каких обстоятельствах не сообщать код из смс или пуш-уведомления кому-либо, включая лиц, представляющихся сотрудниками банка, государственных органов или руководством Предприятия;

3) сообщить о подозрительном сообщении или звонке Ответственному лицу в порядке, установленном разделом 5 настоящего Положения.

15. Работникам запрещается хранить, обрабатывать или передавать служебную и конфиденциальную информацию, а также данные, составляющие охраняемую законом тайну, на личных облачных сервисах (Google Drive, Яндекс.Диск, Dropbox, iCloud и другие), не одобренных Работодателем. Все служебные данные должны храниться исключительно на согласованных Работодателем информационных ресурсах.

16. Использование личных мобильных устройств и учётных записей в личных социальных сетях для решения служебных задач допускается только с согласия Работодателя и при условии соблюдения требований настоящего Положения.

17. Использование внешних сервисов на основе искусственного интеллекта в служебных целях допускается только из перечня, согласованного Ответственным лицом. Запрещается вводить в такие сервисы персональные данные, коммерческую тайну, тексты договоров, финансовую и иную конфиденциальную информацию Предприятия и её контрагентов, а также фрагменты внутренних систем и исходного кода. Результат, полученный с использованием таких сервисов, подлежит проверке работником; ответственность за достоверность и правомерность его использования несёт работник.

4. РАБОТА С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

18. Доступ к конфиденциальной информации, включая персональные данные работников и клиентов Предприятия, предоставляется работнику только при наличии служебной необходимости и в объёме, требуемом для выполнения его трудовых обязанностей.

19. Меры защиты применяются с учётом вида обрабатываемых данных:

Вид данных	Примеры	Меры защиты
Общие персональные данные	Ф. И. О., ИИН, дата рождения, адрес, контакты	Ограничение доступа, хранение в защищённых системах
Данные о трудовой деятельности	Должность, зарплата, взыскания	Доступ по принципу необходимости, контроль логирования
Биометрические данные	Отпечатки пальцев, скан лица (системы доступа)	Шифрование, специализированные базы данных

20. Передача конфиденциальной информации третьим лицам допускается только в случаях, прямо предусмотренных законодательством Республики Казахстан, либо с письменного согласия лица, которому принадлежит данная информация.

21. При направлении писем нескольким внешним адресатам их адреса указываются в поле скрытой копии. Указание адресов внешних получателей в общедоступных полях «Кому» или «Копия» является распространением персональных данных без согласия субъектов.

5. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ КИБЕРБЕЗОПАСНОСТИ

22. При обнаружении инцидента кибербезопасности либо признаков, указывающих на его возможное наступление (подозрительная активность на устройстве, потеря устройства с доступом к корпоративным ресурсам, случайный переход по фишинговой ссылке и т. п.), работник обязан незамедлительно, но не позднее 1 (одного) часа с момента обнаружения, сообщить об этом Ответственному лицу по контактам, указанным в Приложении 1 к настоящему Положению.

23. Сообщение об инциденте направляется независимо от того, по чьей вине он произошел. Добровольное и своевременное сообщение работника о собственной ошибке учитывается как смягчающее обстоятельство при оценке его действий.

24. Ответственное лицо при получении сообщения об инциденте:

1) принимает меры по блокировке скомпрометированных учётных данных и (или) устройств;

2) проводит первичное расследование обстоятельств инцидента;

3) фиксирует факт инцидента, включая дату, время, обстоятельства и предпринятые меры;

4) при необходимости привлекает работника для дачи письменных пояснений.

25. Если инцидент связан с нарушением безопасности персональных данных, Ответственное лицо обеспечивает уведомление уполномоченного органа в сфере защиты персональных данных в течение одного рабочего дня с момента обнаружения нарушения, с указанием контактных данных лица, ответственного за организацию обработки персональных данных, в соответствии с пп. 8) п. 2 ст. 25 Закона Республики Казахстан от 21.05.2013 № 94-V «О персональных данных и их защите».

26. Персональные данные подлежат блокированию в течение одного рабочего дня при поступлении информации о нарушении условий их сбора или обработки и разблокированию – при неподтверждении факта нарушения.

27. По результатам рассмотрения инцидента Ответственное лицо готовит отчёт с указанием причин инцидента и предложениями по недопущению подобных случаев в будущем.

6. ВНУТРЕННИЙ КОНТРОЛЬ

28. Внутренний контроль за соблюдением требований настоящего Положения осуществляет Ответственное лицо на постоянной основе, а также в ходе плановых проверок не реже одного раза в квартал.

29. В ходе проверки оценивается, в частности:
1) соответствие используемых паролей установленным требованиям;
2) наличие и актуальность антивирусного программного обеспечения на рабочих устройствах;
3) отсутствие несанкционированно установленного программного обеспечения;
4) соблюдение правил работы со съёмными носителями и облачными сервисами;
5) факт блокировки рабочих устройств в отсутствие работника.
30. Результаты проверок фиксируются в акте и доводятся до сведения директору Предприятия. При выявлении нарушений Ответственное лицо информирует непосредственного руководителя работника, допустившего нарушение.

7. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ

31. За неисполнение или ненадлежащее исполнение требований настоящего Положения работник несёт дисциплинарную ответственность в порядке, установленном Трудовым кодексом Республики Казахстан.
32. Привлечение работника к дисциплинарной ответственности допускается при одновременном соблюдении следующих условий:
1) соответствующее правило прямо предусмотрено настоящим Положением;
2) работник ознакомлен с настоящим Положением под подпись;
3) факт нарушения зафиксирован документально.
33. К нарушениям требований настоящего Положения, в частности, относятся:
1) разглашение конфиденциальной информации;
2) использование нелицензионного программного обеспечения;
3) переход по фишинговым ссылкам, повлекший заражение системы;
4) использование несанкционированных съёмных носителей;
5) передача учётных данных третьим лицам;
6) несообщение об инциденте кибербезопасности в установленный срок.
34. Работник, чьи неправомерные действия привели к причинению Предприятия материального ущерба, может быть привлечён к материальной ответственности в порядке, установленном Трудовым кодексом Республики Казахстан.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

35. Настоящее Положение вступает в силу с даты его утверждения приказом директора Предприятия и действует до его отмены или замены новым положением.
36. Изменения и дополнения в настоящее Положение вносятся приказом директором Предприятия. О внесённых изменениях работники должны быть ознакомлены под подпись в срок не позднее 10 (десяти) рабочих дней с даты утверждения изменений.
37. Ознакомление работников с настоящим Положением производится путём проставления личной подписи в листе ознакомления (Приложение 3) либо

иным способом, позволяющим достоверно зафиксировать факт и дату ознакомления, в том числе с использованием электронной подписи.

38. Настоящее Положение подлежит пересмотру не реже одного раза в год, а также при существенном изменении законодательства Республики Казахстан в сфере кибербезопасности.

39. Вопросы, не урегулированные настоящим Положением, разрешаются в соответствии с законодательством Республики Казахстан.

40. Если Предприятия является собственником или владельцем информационных систем либо объектов критически важной информационно-коммуникационной инфраструктуры, на неё дополнительно распространяются требования Закона Республики Казахстан «О кибербезопасности», в том числе по:

1) оценке рисков и формированию каталога угроз по национальным стандартам;

2) разработке профилей защиты для значимых информационных систем;

3) применению средств криптографической защиты информации;

4) учёту обучения сотрудников кибербезопасности с выдачей электронных сертификатов;

5) созданию собственного оперативного центра информационной безопасности либо приобретению такой услуги у третьих лиц и взаимодействию с Национальным координационным центром информационной безопасности.

41. При наличии указанных обстоятельств рекомендуется дополнить настоящее Положение отдельным разделом, отражающим перечисленные требования, либо утвердить отдельный документ.

Приложение 1
к Положению о кибербезопасности

ПАМЯТКА СОТРУДНИКУ: КИБЕРГИГИЕНА НА РАБОЧЕМ МЕСТЕ

Надежные пароли. Уникальный сложный пароль для каждого сервиса. Не записывайте на бумаге и не храните в незащищённых файлах. Меняйте регулярно.

Осторожность с письмами. Не открывайте подозрительные письма, не переходите по ссылкам и не скачивайте вложения от неизвестных отправителей.

Защита устройств. Блокируйте экран компьютера или телефона, когда отходите от рабочего места даже на пару минут.

Сообщайте об инцидентах. Если заметили что-то подозрительное, например странное окно, потерю данных или необычную активность, сразу пишите Ответственному лицу.

Осторожность в мессенджерах. Не сообщайте пароли и коды из смс никому, даже если обращение выглядит как от руководителя, банка или коллеги. Если сомневаетесь – перезвоните человеку сами по уже известному номеру.

Контакты Ответственного лица: _____

Телефон/способ связи: _____

Приложение 2

к Положению о кибербезопасности

ПАМЯТКА: КАК РАСПОЗНАТЬ ФИШИНГ И МОШЕННИЧЕСКОЕ ОБРАЩЕНИЕ

Признаки подозрительного письма или сообщения:

1. Адрес отправителя не совпадает с корпоративным доменом Предприятия или содержит опечатки и подмену букв (например, «cornpany.kz» вместо «company.kz»);
2. В тексте создаётся ощущение срочности и давления: «срочно», «немедленно», «иначе заблокируем», «последний день»;
3. Содержится просьба сообщить пароль, код из смс, банковские реквизиты или перейти по ссылке для ввода данных;
4. Письмо просит сохранить обращение в тайне от руководителя или коллег;
5. Есть орфографические ошибки, нетипичное оформление, подозрительные или сокращённые ссылки;
6. Вложение имеет подозрительное расширение файла или неожиданно приходит от малознакомого отправителя.

Если письмо уже открыто, но действия не совершены:

1. Не переходите по ссылкам, не скачивайте вложения, не вводите данные;
2. Не пересылайте письмо коллегам обычным способом – возможно, вирус в его тексте или вложении;
3. Сообщите Ответственному лицу, приложив письмо как вложение, с пометкой о подозрении на фишинг.

Если ссылка уже открыта или данные уже введены:

1. Немедленно закройте вкладку и не вводите никаких данных на открывшемся сайте;
2. Если данные уже были введены – срочно смените пароль от скомпрометированного сервиса;
3. Сообщите об инциденте Ответственному лицу в порядке, установленном разделом 5 настоящего Положения;
4. Проверьте устройство на предмет необычной активности (всплывающие окна, неизвестные отправленные письма).

Признаки мошеннического сообщения или звонка в мессенджере:

1. Обращение с незнакомого номера или аккаунта, в том числе внешне похожего на коллегу или руководителя;
2. Требование срочно совершить платёж, передать данные или код из смс;
3. Стиль общения не соответствует привычной манере собеседника;
4. Просьба ничего не уточнять и не сообщать никому о разговоре.

Ни один банк, государственный орган или директор Предприятия не запрашивает пароли и коды из смс-сообщений по телефону, в мессенджерах или по электронной почте.

Приложение 3
к Положению о кибербезопасности

ЛИСТ ОЗНАКОМЛЕНИЯ
с Положением о кибербезопасности

№	Ф. И. О. работника	Должность	Дата ознакомления	Подпись
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Разработано:
Руководитель отдела
управления человеческими ресурсами _____ Е. Кадирова

Начальник отдела
информационного обеспечения _____ Ж. Кыстаубаев

Согласовано:
Руководитель
организационно-правового отдела _____ Д. Бакижанова