МУНИЦИПАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«ГОРОДСКАЯ КОММУНАЛЬНАЯ СЛУЖБА»

ПРИКАЗ

16.01.2024 059-01-04-5

Об информационной безопасности

Во исполнение приказа департамента жилищно-коммунального хозяйства администрации города Перми от 15.01.2024 № 059-04-04-1 ,приказа МКУ «ГКС» от 18.08.2023 № 059-01-04-12 и в целях организации информационной безопасности, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты в муниципальном казенном учреждении «Городская коммунальная служба» (далее – Учреждение) ,

Приказываю:

1.Утвердить «Общие требования по информационной безопасности к работникам МКУ «Городская коммунальная служба» при осуществлении трудовой деятельности» (Приложение к настоящему приказу).

2.Кожевниковой Т.Г. – начальнику общего отдела, ознакомить сотрудников учреждения с настоящим приказом под роспись.

3.Контроль за исполнением приказа оставляю за собой.

Документ подписан электронной подписью
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 03051D2ECDDFA8FD9A1E485A561490CA
Владелец: Дернейко Константин Константинович
Действителен с 14-09-2023 до 07-12-2024

Директор К. К. Дернейко

С приказом ознакомлен:
(лист ознакомления)

Приложение к приказу

ОБЩИЕ ТРЕБОВАНИЯ
по информационной безопасности к работникам
МКУ «Городская коммунальная служба»
при осуществлении трудовой деятельности

I. Порядок доступа в Учреждение

1.1.Доступ сотрудников и посетителей на территорию учреждения по адресу ул. Ленина 34 в рабочие дни осуществляется через проходную систему департамента жилищно-коммунального хозяйства администрации города Перми.

1.2. Доступ сотрудников на рабочее место в нерабочие праздничные и выходные дни осуществляется по согласованию с начальником хозяйственного управления администрации города Перми (оформляется служебная записка).

II. Работа с документами и носителями информации

2.1. Запрещается выносить рабочие документы на бумажных или иных носителях информации (флеш-карты, внешние накопители и др.) за пределы территории Учреждения без служебной необходимости.

2.2. В случае утери рабочих документов и иных носителей информации (флеш-карты, внешние накопители и др.) необходимо незамедлительно сообщить об этом своему непосредственному руководителю.

2.3. Запрещается утилизировать рабочие документы, содержащие персональные данные работников Учреждения, в урны для мусора, корзины для макулатуры, предварительно не подвергнув их процедуре уничтожения.

2.4. Запрещается использование работниками Учреждения иностранных облачных ресурсов для совместного редактирования, таких как «Google Docs».

III. Работа с автоматизированными рабочими местами Учреждения

3.1. Работникам Учреждения (за исключением технических специалистов Учреждения, ответственных за администрирование информационно-коммуникационных систем) запрещается самостоятельно без согласования с техническим специалистом Учреждения, ответственным за администрирование информационно-коммуникационных систем, устанавливать, тиражировать или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств автоматизированного рабочего места (далее – АРМ).

3.2. Работникам Учреждения по окончании рабочего дня необходимо выйти из операционной системы (либо заблокировать АРМ).

3.3. Работникам Учреждения запрещается несанкционированно открывать общий доступ к каталогам на АРМ.

3.4. Работникам Учреждения запрещается подключать к АРМ съемные машинные носители информации и мобильные устройства, а также копировать

информацию, ставшую им известной в ходе выполнения должностных обязанностей на такие носители без служебной необходимости.

3.5. Работникам Учреждения запрещается отключать (удалять) установленные на АРМ средства защиты информации.

3.6. Работникам Учреждения запрещается привлекать лиц, не являющихся работниками Учреждения, для осуществления установки программного обеспечения, ремонта или настройки технических средств АРМ (за исключением случаев, когда данные услуги оказываются на договорной основе);

3.7. Работникам Учреждения запрещается осуществлять фото- и видеосъемку рабочих документов, а также публикацию таких документов в социальных сетях и других открытых ресурсах (за исключением случаев, когда это необходимо для выполнения должностных обязанностей).

3.8. Работникам Учреждения запрещается производить деструктивные действия в отношении АРМ Учреждения.

3.9. Работникам Учреждения необходимо соблюдать правила работы в сети Интернет (раздел IV настоящего документа).

3.10. Работникам Учреждения необходимо соблюдать правила антивирусной защиты (раздел V настоящего документа).

3.11. Работникам Учреждения необходимо не допускать случаев социальной инженерии и фишинга (раздел VI настоящего документа).

IV. Правила работы в сети Интернет

4.1. При работе в сети Интернет работник Учреждения обязан:

4.1.1. Противодействовать методам социальной инженерии: не открывать вложения в письмах от неизвестных источников, не переходить по подозрительным баннерам и ссылкам на веб-сайтах, проверять вводимый адрес веб-сайтов на предмет опечаток;

4.1.2. Не скачивать с сайтов сомнительной репутации (сайты, содержащие нелегально распространяемое программное обеспечение, торрент-сайты, и т.д.) какие-либо файлы и программное обеспечение.

4.1.3. Обращаться к начальнику общего отдела в случае выявления фактов нарушения информационной безопасности.

4.2. Использование электронной почты:

4.2.1. Каждому работнику Учреждения (за исключением профессий рабочих) при трудоустройстве должен создаваться служебный адрес электронной почты, размещенный на почтовом сервере Единого почтового домена Пермского края, в адресном пространстве permkrai.ru;

4.2.2. При увольнении работника Учреждения служебный адрес электронной почты в обязательном порядке подлежит удалению;

4.2.3. Ответственным за организацию создания (удаления) служебных адресов электронной почты работников Учреждения является начальник общего отдела.

4.2.4. Не допускается передача учетных данных (логин, пароль) электронной почты другим работникам Учреждения и третьим лицам;

4.2.4. Для направления ответов на обращения граждан рекомендуется использовать только служебный адрес электронной почты, размещенный на почтовом сервере Единого почтового домена Пермского края, в адресном пространстве permkrai.ru.

4.3. В случае, если должностны- ми обязанностями предусмотрено использование социальных сетей («Вконтакте», «Instagram», и др.) (далее – Приложение), работнику Учреждения необходимо:

4.3.1. Ознакомиться с политикой использования Приложения;

4.3.2. Не загружать конфиденциальную информацию в Приложение (в т.ч. персональные данные);

4.3.3. Исключить передачу учетных данных (логин, пароль) третьим лицам и другим работникам Учреждения;

4.3.2. В случае наличия технической возможности Приложения использовать двухфакторную аутентификацию.

V. Соблюдение антивирусной защиты информации

5.1. Работник Учреждения обязан:

5.1.1. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник обязан самостоятельно или совместно с техническим специалистом Учреждения, ответственным за администрирование информационно-коммуникационных систем, провести внеочередной антивирусный контроль АРМ;

5.1.2. Производить антивирусную проверку отчуждаемых машинных носителей (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

5.2. Работнику Учреждения запрещается:

5.2.1 Удалять средства антивирусной защиты, установленные на АРМ;

5.2.2. Вносить изменения в настройки средства антивирусной защиты, установленного на АРМ.

VI. Противодействие социальной инженерии и фишингу

6.1. Социальная инженерия – совокупность приемов и методов, применяемых злоумышленниками, направленных на получение от работника служебной (конфиденциальной) информации;

6.1.1. В целях противодействия социальной инженерии работникам Учреждения необходимо:

- не сообщать по электронной почте и по телефону служебной информации пока не будет установлена личность запрашивающего и его право на доступ к такой информации;

- не осуществлять работу за АРМ и с документами в присутствии посторонних лиц;

- блокировать АРМ (при отсутствии за рабочим местом, при окончании рабочего дня и т.д.);

- в случае попытки посторонних лиц получить от работника служебную (конфиденциальную) информацию, незамедлительно сообщить об этом непосредственному руководителю;

6.2. Фишинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (логинам, паролям и т.д.).

6.2.1. В целях противодействия фишингу работникам Учреждения необходимо:

- осуществлять проверку адреса любого сайта, который запрашивает идентификационную информацию;

- осуществлять проверку электронной почты отправителя писем;

- не проходить по подозрительным ссылкам и не скачивать подозрительные файлы;

- об утере или компрометации логинов и паролей сообщать начальнику общего отдела для организации их восстановления или замены.

VII. Удаленная (дистанционная) работа

7.1. При установлении удаленного (дистанционного) режима работы требования по информационной безопасности должны соблюдаться в полном объеме.

VIII. Порядок информирования о выявлении инцидентов информационной безопасности

8.1. Начальник общего отдела в кратчайший срок организует информирование Министерства информационного развития и связи Пермского края по электронной почте incident@it.permkrai.ru о выявлении инцидентов информационной безопасности, повлекших некорректную работу или временную недоступность информационной инфраструктуры Учреждения и (или) имеющихся рисков их возникновения.

8.2. При направлении информационного сообщения о выявлении инцидентов информационной безопасности в теме письма необходимо указать «Инцидент ИБ МКУ «ГКС». К письму приложить заполненную карточку инцидента, при необходимости приложить скриншоты или фотографии. В карточке или письме указать контактные данные заявителя.