УТВЕРЖДАЮ
Директор
_____ К.В.Багмет
Приложение №9 к приказу №26
от «29» апреля 2019 года

ПОЛИТИКА
допустимого использования информационных технологий
ГАУ ДПО «Центр повышения квалификации и профессиональной переподготовки работников социальной сферы»

1. Общие положения

Данный документ (далее – Политика) устанавливает требования и процедуры обеспечения информационной безопасности при использовании ИС и ИТ-сервисов ГАУ ДПО «Центр повышения квалификации и профессиональной переподготовки работников социальной сферы» (далее – Центр ДПО).

Целью документа является повышение общего уровня информационной безопасности (снижение количества ошибок и инцидентов информационной безопасности) Центра ДПО за счет следования базовым правилам и рекомендациям по информационной безопасности, а также контролю их выполнения.

Политика устанавливает правила по работе со следующими ИТ-сервисами:

1) Корпоративная электронная почта;
2) Доступ в сеть Интернет;
3) Доступ к сетевым дискам и файловым хранилищам;
4) Сетевая печать и копировально-множительная техника.

Политика устанавливает правила по работе со следующими средствами обработки информации:

1) Корпоративные рабочие станции;
2) Мобильные устройства и съемные носители информации.

Настоящая Политика не затрагивает вопросы использования систем «клиент-банк».

Обязанности по выполнению Политики возлагаются на каждого работника Центра ДПО, имеющего доступ к автоматизированному рабочему месту.

2. Общие требования

Доступ к ИТ-сервисам и средствам обработки информации Центра ДПО предоставляется для выполнения должностных обязанностей и

делового общения работников и решения других задач, выполняемых по указанию руководства Центра ДПО.

Программно-аппаратное обеспечение ИТ-сервисов и средства обработки информации принадлежат Центру ДПО.

К работе с ИТ-сервисами и средствами обработки информации допускаются работники Центра ДПО, подписавшие Соглашение о неразглашении информации ограниченного доступа, ознакомленные с документами, регламентирующими обеспечение информационной безопасности Центра ДПО, и прошедшие вводный инструктаж по информационной безопасности.

3. Корпоративная электронная почта

Сервис корпоративной электронной почты предоставляется Центру ДПО в соответствии с политикой управления доступом.

В Центре ДПО запрещено использование внешних почтовых систем (например, mail.ru, gmail, hotmail) для выполнения должностных обязанностей без согласования с директором.

Вся информация и сообщения, которые были созданы, отправлены, приняты или сохранены посредством корпоративной электронной почты, принадлежат Центру ДПО, за исключением случаев, предусмотренных законодательством Российской Федерации.

Корпоративная электронная почта организована на основе программного обеспечения Сервис корпоративной электронной почты.

Официальной программой для доступа к корпоративной электронной почте является MS Outlook.

Доступ к корпоративной электронной почте без настройки MS Outlook возможен с помощью веб-интерфейса, для чего необходимо указать в интернет-браузере адрес: Адрес web интерфейса корпоративной электронной почты.

Размер пользовательских почтовых ящиков ограничен квотой: Максимальный размер почтового ящика.

Решение о изменении категории квоты почтового ящика принимается директором.

Каждый пользователь несет персональную ответственность за соблюдение установленного размера личного почтового ящика и удаление информации из него.

Максимальный размер электронного сообщения в корпоративной электронной почте ограничен размером Максимальный размер письма.

Использование корпоративной электронной почты работниками Центра ДПО допустимо при соблюдении следующих требований:

1) приверженность корпоративному стилю и правилам почтового и профессионального этикета;

2) применение средств защиты информации, принятых в Центре ДПО.

Пользователям сервиса корпоративной электронной почты

запрещается:

1) использовать корпоративную электронную почту в личных и/или развлекательных целях;

2) пересылать информацию ограниченного доступа несанкционированным получателям (лицам, которым она не предназначена и/или не имеющим прав доступа к данной информации);

3) передавать информацию, способную скомпрометировать Центр ДПО, а также ее руководство;

4) рассылать материалы, содержащие вредоносное программное обеспечение, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности компьютерного или телекоммуникационного оборудования, программы для осуществления несанкционированного доступа к информации;

5) рассылать серийные номера к коммерческим программным продуктам и программы для их генерации, пароли и прочие средства для доступа к ресурсам ИС Центра ДПО;

6) осуществлять несанкционированные массовый рассылки любой информации (в том числе «письма счастья», предложения товаров и услуг и прочее);

7) публиковать свой адрес корпоративной электронной почты либо адреса корпоративной электронной почты других работников Центра ДПО на общедоступных Интернет ресурсах (форумы, блоги, социальные сети и прочие), если это не связано с профессиональной деятельностью;

8) предоставлять доступ (в том числе передавать пароль доступа) к своему электронному почтовому ящику другим работникам Центра ДПО и третьим лицам, за исключением своего непосредственного руководителя.

Пользователям необходимо соблюдать правила корпоративного стиля и этикета:

1) обмен информацией должен происходить с соблюдением правил делового этикета и максимально экономить время коллег;

2) при переписке рекомендуется использовать следующие формулировку обращения: «Добрый день, уважаемый (уважаемая) + имя отчество адресата». И только после этого переходить к цели обращения;

3) при составлении электронных писем следует соблюдать принципы грамотности написания текста в соответствии с нормами русского языка и логичности изложения содержания обращения. Следует разбивать письмо на логические абзацы и избегать чрезмерно длинных предложений;

4) общая структура делового электронного письма может быть следующей:

– приветствие;
– содержание, цель обращения;
– прощание;
– личная подпись с указание контактов;
– логотип Центра ДПО.

5) длина электронного письма должна отвечать переписке: если вы просто отвечаете на вопрос, делайте это кратко и по существу;

6) придерживайтесь темы переписки. Ели вы хотите обсудить, что-то новое, лучше направить отдельное письмо, делайте это кратко и по существу;

7) избегайте направлять публичные письма, составленные под влиянием эмоций. Всегда соблюдайте вежливость и тактичность при переписке;

8) при направлении письма должны быть заполнены поля: «Тема», «Кому», «Важность письма» (при необходимости).

9) в поле «Копия» вводится электронный адрес, которым письмо направляется в целях информирования;

10) в поле «Тема» следует вписать несколько слов, характеризующих тему сообщения:

– при согласовании проектов организационных или распорядительных документов, тема письма должна быть следующая: «Согласование: Наименование документа»;

– при направлении электронной версии визовой копии проекта ОРД и НМД тема письма должна быть следующая: «Визирование: Наименование документа»;

– если сообщение отправляется для сведения, тема письма должна быть следующая: «Несколько слов, характеризующих тему сообщения»;

– если сообщение содержит задачу, которую необходимо исполнить, тема письма должна быть следующая: «Несколько слов, характеризующую задачу»;

– если сообщение содержит зарегистрированные документы, с которыми необходимо ознакомится, то тема письма должна быть следующая: «Ознакомление: Наименование документа».

11) если сообщение носит срочный характер, то следует указать степень важности сообщения. Важность сообщения определяется непосредственный руководитель работника Центра ДПО. Письма с пометкой «Важное» получают приоритет при проверке почты;

12) работник не обязан отвечать на любое письмо. Особенно, если оно напрямую не адресовано работнику, а он указан только в «Копии». Не следует писать «Спасибо за совет», «Спасибо за помощь»;

13) старайтесь не смешивать в своем послании информацию общего личного характера;

14) не вкладывайте текстовую информацию в виде файла, если ее можно указать текстом в теле письма;

15) перед отправкой ответа проанализируйте – необходим ли ваш ответ;

16) например, если вы получили письмо в результате верной рассылки, не стоит извещать каждого из адресатов о своем отношении – лучше отправить письмо непосредственно автору;

17) электронная переписка заканчивается по правилам телефонного

этикета: кто первый начал переписку, тот ее первый и заканчивает.

Пользователям сервиса корпоративной электронной почты не рекомендуется переходить по ссылкам, а также просматривать вложения почтовых сообщений, поступивших от неизвестного отправителя, либо сообщений сомнительного содержания.

Для обеспечения информационной безопасности в Центре ДПО осуществляется проверка входящих сообщений с целью обнаружения и блокировки писем, идентифицированных как спам, а также антивирусный контроль почтовых сообщений для обнаружения и блокировки писем, содержащих вирусы.

Центр ДПО оставляет за собой право просматривать, контролировать, изымать и разглашать все сообщения, созданные, полученные или переданные с помощью системы корпоративной электронной почты с целью обеспечения информационной безопасности Центра ДПО.

При увольнении пользователя адрес его электронной почты блокируется. Содержимое почтового ящика хранится в течение 2 месяцев и может быть предоставлено руководителю структурного подразделения, в котором работал пользователь по служебной записке на имя директора. По окончании данного срока выполняется безвозвратное удаление содержимого почтового ящика.

4. Сервисы мгновенных сообщений

Агенты сервисов мгновенных сообщений (например, ICQ), а также сервисов интернет-телефонии (например, Skype) могут быть установлены на рабочие станции работников по согласованию с директором.

В Центре ДПО запрещено использование сервисов мгновенных сообщений для передачи информации ограниченного доступа.

Пользователям сервисов мгновенных сообщений запрещается:

1) рассылать серийные номера к коммерческим программным продуктам и программы для их генерации, пароли и прочие средства для доступа к ресурсам ИС Центра ДПО;

2) передавать информацию, способную скомпрометировать Центр ДПО, а также ее руководство и работников;

3) рассылать материалы, содержащие вредоносное программное обеспечение, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности компьютерного или телекоммуникационного оборудования, программы для осуществления несанкционированного доступа к информации;

4) переходить по ссылкам, а также просматривать вложения информационных сообщений, поступивших от неизвестного отправителя, либо сообщений сомнительного содержания;

5) осуществлять незаконную, неэтичную или иную несанкционированную деятельность.

5. Сеть интернет

Ресурсы сети Интернет в Центре ДПО используются в следующих целях:

1) для обеспечения дистанционного банковского обслуживания;

2) для обеспечения взаимодействия с контрагентами в рамках существующих процессов;

3) для получения и распространения информации, связанной с служебной деятельностью;

4) для обеспечения взаимодействия с внешними ИС, связанным с служебной деятельностью;

5) для информационно-аналитической работы в интересах организации;

6) ведения собственной хозяйственной деятельности;

7) для обмена почтовыми и мгновенными сообщениями в рабочих целях.

Иное использование ресурсов сети Интернет, решение о котором не принято руководством Центра ДПО, рассматривается как нарушение ИБ.

При работе с сетью Интернет работникам запрещено:

1) распространять информацию ограниченного доступа Учреждения в сети Интернет (публикация информации на сайтах, форумах, блогах, социальных сетях, в файлообменных сетях и прочее);

2) выкладывать и хранить информацию ограниченного доступа Центра ДПО в облачных хранилищах (например, Dropbox, Google Drive и прочее);

3) изменять настройки программного обеспечения, с помощью которого осуществляется доступ к сети Интернет;

4) использовать анонимайзеры (анонимные прокси-серверов), TOR-сети и торрент-сети;

5) использовать специализированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к сети Интернет (в том числе USB-модемы, персональные wifi-точки доступа и другое);

6) скачивать и выкладывать в сеть Интернет файлы, защищенные авторским правом (например, программное обеспечение, аудио и видео файлы);

7) скачивать и устанавливать на рабочий компьютер дополнительное программное обеспечение;

8) посещать ресурсы, не имеющие непосредственного отношения к работе и служебным обязанностям;

9) осуществлять подписку на рассылку информации непроизводственного характера;

10) использовать сеть Интернет для получения материальной выгоды.

Центр ДПО оставляет за собой право блокирования доступа к

определенным категориям сайтов сети Интернет. Перечень сайтов и/или категорий таких сайтов определяется директором.

6. Сетевые диски и файловые хранилища

Доступ к информационным ресурсам на сетевых дисках и файловых хранилищах, необходимый для выполнения служебных обязанностей, предоставляется работникам Центра ДПО в соответствии с «Политикой управления доступом».

Пользователям запрещается:

1) хранить личную информацию и информации развлекательного характера;

2) хранить информацию, нарушающую авторские права ее владельцев;

3) хранить информацию ограниченного доступа в общедоступных папках.

7. Сетевая печать и копировально-множительная техника

Доступ к сетевой печати, необходимый для выполнения служебных обязанностей, предоставляется работникам Центра ДПО в соответствии с «Политикой управления доступом».

При использовании копировально-множительной техники для печати/копирования документов, содержащих информацию ограниченного доступа, работнику необходимо незамедлительно забирать печатные материалы из принтера. Ненужные копии и черновики документов должны быть уничтожены с использованием шредера.

Распечатка/копирование материалов общим объемом более 500 листов должна согласовываться с непосредственным руководителем (в свободной форме).

Пользователям сервиса запрещается:

1) использовать копировально-множительную технику для печати/копирования материалов развлекательного характера и/или, не связанных с выполнением должностных обязанностей;

2) самостоятельно осуществлять ремонт копировально-множительной техники, в том числе и производить замену картриджей с краской.

8. Удаленный доступ к информационным ресурсам

Удаленный доступ (доступ из-за границы корпоративной сети) к информационным ресурсам Центра ДПО, необходимый для выполнения служебных обязанностей, предоставляется работникам Центра ДПО в соответствии с «Политикой управления доступом к информационным ресурсам».

1) с использованием удаленного VPN соединения к серверу vpn;

2) с использованием протокола HTTPS к серверу электронной почты.

При использовании удаленного доступа Усиленной аутентификации не требуется.

9. Корпоративные рабочие станции

Корпоративными рабочими станциями (персональными компьютерами) обеспечиваются все работники Центра ДПО, которым в рамках своих должностных обязанностей необходимо иметь доступ к информационным ресурсам Центра ДПО.

Состав аппаратной части корпоративных рабочих станций работников Центра ДПО определяется директором.

В Центре ДПО определены Перечни разрешенного ПО, устанавливаемого по заявкам работников Центра ДПО и согласованию с директором.

Пользователям запрещается:

1) использовать корпоративные рабочие станции для развлечений и других действий, не связанных не связанных с выполнением должностных обязанностей Центра ДПО, и/или способных нанести ущерб Центру ДПО;
2) самостоятельно устанавливать дополнительное программного обеспечения;
3) отключать средства защиты информации;
4) вносить изменения в настройки операционной системы и другого программного обеспечения, способные повлиять на состояние информационной безопасности Центра ДПО;
5) вскрывать системные блоки и самостоятельно производить ремонт;
6) устанавливать и запускать средства мониторинга и сканирования сети, программы, содержащие вредоносное программное обеспечение;
7) выносить корпоративные рабочие станции за пределы контролируемой зоны организации без согласования с директором.

10. Мобильные устройства и съёмные носители информации

Под использованием мобильных устройств и носителей информации в ИС Центра ДПО понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и мобильными устройствами, а также носителями информации.

Использование личных мобильных устройств допускается только после согласования с директором.

При использовании мобильных устройств необходимо соблюдать правила об обязательной парольной блокировке доступа к устройству и конфиденциальность при работе с ним.

Заявка на предоставление мобильного устройства и/или носителя информации работнику, направляется Инициатором с подробным обоснованием директору.

При использовании предоставленных Центром ДПО мобильных

устройств и носителей информации необходимо:

1) использовать мобильные устройства и носители информации исключительно для выполнения своих должностных обязанностей;

2) бережно относится к мобильным устройствам и носителям информации предоставленных Центром ДПО;

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

4) обеспечивать физическую безопасность мобильных устройств и носителей информации;

5) в случае утери или кражи мобильного устройства и/или носителя информации, необходимо в срочном порядке по электронной почте оповестить пояснительной запиской.

При использовании предоставленных работникам Центра ДПО мобильных устройств и носителей информации запрещено:

1) использовать мобильные устройства и носители информации в личных целях;

2) передавать мобильные устройства и носители информации другим лицам;

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

При подозрении работника Центра ДПО в несанкционированном и/или нецелевом использовании мобильных устройств и носителей информации инициализируется служебная проверка, проводимая комиссией, состав которой определяется директором Центра ДПО.

По факту выясненных обстоятельств составляется акт расследования инцидента и передается директору для принятия мер согласно организационно-распорядительным документам Центра ДПО и действующему законодательству. Акт расследования инцидента и сведения о принятых мерах подлежат передаче.

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