УТВЕРЖДАЮ:
Коммерческий директор

_____ Пак О. Ю.
«16» мая 2024г.

Инструкция
по безопасности информации и сети
ТОО «Школа Нового Поколения NGS» (Эн Джи Эс)

город Алматы, 2024 год

Содержание

1. Общие положения

1.1. Настоящая Инструкция по безопасности и сети является внутренним нормативным документом ТОО «Школа Нового Поколения NGS» (Эн Джи Эс) (далее – Школа).

1.2. Под обеспечением информационной безопасности понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность – в случае внесения в данные исключительно авторизованных изменений, доступность – обеспечении возможности получения доступа к данным авторизованным лицам в нужное для них время.

1.3. Целью обеспечения информационной безопасности является минимизация экономического, финансового, социального ущерба от реализации угроз информационной безопасности, а также повышение общего уровня конфиденциальности, целостности и доступности информации.

1.4. Настоящая инструкция устанавливает порядок действий работников и учащихся Школы при работе с ресурсами и сервисами сети Интернет.

1.5. Ознакомление с инструкцией и ее соблюдение обязательны для всех работников и учеников Школы, а также иных лиц, допускаемых к работе с ресурсами и сервисами сети Интернет.

2. Организация использования сети Интернет в Школе

2.1. В целях обеспечения безопасности сети регулярно проводятся проверки на предмет выявления уязвимости и обновления безопасности. Данные меры минимизируют риски и обеспечивают надёжную защиту информационных ресурсов Школы.

2.2. На всех компьютерах установлены антивирусные программы, которые регулярно обновляются и сканируют систему на наличие вредоносных программ. Также используются программы для блокировки рекламы и отслеживания, что способствует повышению уровня безопасности и конфиденциальности данных.

2.3. Настройки сети выполнены с учетом ограничения доступа к потенциально вредоносным или неподходящим сайтам. Сетевой трафик маршрутизируется через защищенные соединения, что обеспечивает дополнительный уровень безопасности и конфиденциальности данных в сети.

2.4. Доступ к информационным ресурсам для работников, чья трудовая деятельность не связана напрямую с образовательным процессом, должен быть ограничен в соответствии с их должностными обязанностями. Использование ресурсов, не относящихся к трудовой деятельности работников Школы запрещено.

2.5. При использовании сети Интернет работниками Школы и учащимися, предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Республики Казахстан и которые имеют прямое отношение к образовательному процессу.

2.6. При использовании ресурсов сети обязательным является соблюдение законодательства об интеллектуальных правах и иного применимого законодательства.

2.7. При использовании сетевых сервисов, предполагающих авторизацию, запрещается пользоваться чужими учетными данными.

3. Обязательства IT департамента

3.1. IT-департамент Школы должен регулярно мониторить использование сети для обеспечения соблюдения установленных правил и обнаружения любых необычных или подозрительных действий. Это включает в себя проверку трафика, использования пропускной способности и попыток доступа к заблокированным сайтам.

3.2. IT-департамент Школы отвечает за обеспечение безопасности сети, включая установку и обновление защитного программного обеспечения, обеспечение регулярного резервного копирования данных и обучение работников и учащихся Школы безопасному использованию Интернета.

3.3. IT-департамент Школы обеспечивает техническую поддержку всем пользователям сети, помогая им решать проблемы и отвечая на вопросы о правильном использовании сети и оборудования.

3.4. IT-департамент Школы обеспечивает обязательность процедуры идентификации и аутентификации для доступа к ресурсам информационных систем.

3.5. IT-департамент Школы обязуется не допускать получения права доступа к информационным системам неавторизированным пользователям и представлять пользователям входные имена и начальные пароли только после заполнения установленных регистрационных форм.

3.6. IT-департамент Школы обеспечивает защиту оборудования Школы.

3.7. IT-департамент Школы обязуется оперативно и эффективно реагировать на события, содержащие угрозу, принимать меры по отражению угрозы и выявлению нарушителей, фиксировать и информировать специалистов, отвечающие за информационную безопасность о попытках нарушения защиты.

3.8. Все компьютеры, подключаемые к сети Интернет, обязаны иметь установленное, действующее и обновляющееся антивирусное программное обеспечение.

4. Права, обязанности и ответственность пользователей

4.1. В случае обнаружения нарушения безопасности сети, ответственные/уполномоченные лица должны немедленно принять следующие меры:

- определить характер нарушения, оценить его масштаб и потенциальный ущерб;
- обеспечить соблюдение конфиденциальности информация о нарушении, чтобы предотвратить дальнейшие нарушения;
- принять меры для немедленного устранения нарушения, включая изменение паролей, блокировку учетных записей или изменение настроек сети;
- провести тщательное расследование для определения причины нарушения и предотвращения подобных инцидентов в будущем;
- сообщить о нарушении руководству Школы, в зависимости от характера и масштаба нарушения, с согласия руководства Школы сообщить о нарушении соответствующим органам или сторонним организациям;

4.2. Использование ресурсов сети Интернет осуществляется в первую очередь в целях образовательного процесса. Однако, признается, что эти ресурсы могут также использоваться в рамках трудовой деятельности работников Школы, включая, но не ограничиваясь исследования, подготовку к занятиям, общение с коллегами и другие мероприятия, которые способствуют выполнению профессиональных обязанностей.

4.3. Сотрудники Школы могут бесплатно пользоваться доступом к глобальным Интернет-ресурсам по разрешению лица, назначенного ответственным за организацию работы сети Интернет и ограничению доступа.

4.4. К работе в сети Интернет допускаются лица, ознакомившиеся с настоящей инструкцией и обязавшиеся соблюдать правила работы в сети Интернет.

4.5. Пользователям запрещается:

- посещать сайты, содержание и тематика которых недопустимы для несовершеннолетних и (или) нарушают законодательство Республики Казахстан (порнография, эротика, пропаганда насилия, терроризма, политического и религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);
- загружать и распространять материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения

несанкционированного доступа к платным ресурсам в сети Интернет, а также размещение ссылок на выше указанную информацию;

- загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;
- распространять информацию, порочащую честь и достоинство граждан;
- работать с объемными ресурсами (видео, аудио, чат, фото) без согласования с лицом, назначенным ответственным за организацию работы в сети Интернет.

4.6. Пользователи несут ответственность:

- за разглашение пароля, выдаваемого для работы с информационными ресурсами Школы и её аффилированных лиц. При смене пароля, он должен состоять не менее чем из 8 символов, содержать минимум одну заглавную букву и одну строчную на латинском языке. Не желательно чтобы пароль содержал год рождения или имя;
- за содержание передаваемой, принимаемой и печатаемой информации;
- за нанесение любого ущерба оборудованию (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность в соответствии с законодательством РК;

4.7. Пользователи имеют право:

- работать в сети Интернет;
- с согласием IT департамента, сохранять полученную информацию на съемном диске (флеш-накопителе и сетевых дисках).

5. Действия во внештатных ситуациях

5.1. При утрате (в том числе частично) подключения к сети Интернет-пользователь, обнаруживший неисправность, сообщает об этом IT департаменту через IntraService.

6. С целью обеспечения компьютерной безопасности пользователь обязан

6.1. Быть крайне осторожным при работе с электронной почтой. Категорически запрещается открывать присоединенные к письмам, полученным от незнакомых лиц, файлы.

6.2. В обязательном порядке проверять антивирусным программным обеспечением любые внешние носители информации перед началом работы с ними. Антивирусная программа автоматически производит проверку всех носителей, необходимо дождаться завершение проверки, перед открытием любого накопителя.

Разработал
Директор IT департамента Кругов Е.С. / _____

Согласовано:

Директор HR департамента Хон А.Н. / _____

Юрист Басанов Е.М. / _____

Данный документ согласно пункту 1 статьи 7 ЗРК от 7 января 2003 года N370-II «Об электронном документе и электронной цифровой подписи», удостоверенный посредством электронной цифровой подписи лица, имеющего полномочия на его подписание, равнозначен подписанному документу на бумажном носителе.