ФГБОУ ВО «Петрозаводский государственный университет»

ДОКЛАД

по курсу организационное обеспечение информационной безопасности на тему: "Дополнительные инструкции для каждого сотрудника сервиса по ремонту бытовой техники Технический Ремонтович"

Выполнили студенты группы 22307:
Ананьин Егор, Базаров Максим, Богатырёв Павел,
Гордеев Никита, Сергин Даниил

Преподаватель
Соколов Владислав Евгеньевич

Петрозаводск,
2023

В компании работает директор, два мастера и офис-менеджер, занимающийся приёмом заказов. Ниже приведены инструкции по защите данных для каждого сотрудника:

Директор:

1. Установите пароль на свой компьютер для защиты от несанкционированного доступа.
2. Регулярно создавайте резервные копии всех важных данных на отдельных носителях или облачном хранилище.
3. Не передавайте свой пароль или доступ к компьютеру другим людям.
4. Обязательно блокируйте компьютер при покидании рабочего места или если оставляете его без присмотра на некоторое время.
5. Используйте надежные и уникальные пароли для всех ваших учетных записей и изменяйте их периодически.
6. Будьте осмотрительны при открытии вложений в электронных письмах или при посещении подозрительных веб-сайтов.
7. Не храните конфиденциальные данные на локальном компьютере, если это необходимо, используйте зашифрованные файлы или защиту паролем.
8. После завершения работы не забудьте выйти из системы и выключите компьютер.

Мастера:

1. Установите пароль на свои компьютеры для защиты от несанкционированного доступа.
2. Не открывайте вложения в электронных письмах или файлы, полученные от незнакомых или подозрительных источников.
3. Регулярно обновляйте антивирусное программное обеспечение и выполняйте полное сканирование компьютера.
4. Если вы замечаете необычную или подозрительную активность на своем компьютере или в сети, немедленно сообщите об этом директору или офис-менеджеру.
5. При работе с клиентскими данными обеспечьте их конфиденциальность: храните данные клиентов в зашифрованном виде, не передавайте их другим лицам, если данные больше не нужны – удалите их (дополнительные сведения см. в общих рекомендациях).
6. Не храните конфиденциальные данные на локальных носителях, используйте распределенные сетевые хранилища с соответствующими мерами безопасности.
7. Соблюдайте строгие меры контроля доступа при работе с техникой, содержащей конфиденциальные данные клиентов.
8. Не разглашайте информацию о клиентах и заказах третьим лицам.

Офис-менеджер:

1. Установите пароль на свой компьютер для защиты от несанкционированного доступа.
2. Регулярно обновляйте антивирусное программное обеспечение и выполняйте полное сканирование компьютера.
3. Будьте осмотрительны при открытии вложений в электронных письмах или при посещении подозрительных веб-сайтов.
4. Следите за безопасностью офиса и не позволяйте посторонним лицам получить доступ к компьютерам или конфиденциальным данным.
5. Используйте надежные и уникальные пароли для всех учетных записей и изменяйте их периодически.
6. Не храните конфиденциальные данные на локальном компьютере, используйте зашифрованные файлы или защиту паролем.

7. Выполняйте резервное копирование всех данных, связанных с клиентами и другой важной информацией, на отдельные носители или облачные хранилища.
8. В случае потери или кражи компьютера немедленно сообщите об этом директору.
9. Удостоверьтесь, что все приемы заказов и обработка информации происходят в безопасной среде.
10. Закрывайте рабочее место и блокируйте компьютер при отсутствии.

Общие рекомендации:

1. Все сотрудники должны быть осведомлены о политике безопасности и соблюдать ее положения.
2. Регулярно обучайте сотрудников основам кибербезопасности и информируйте их о новых угрозах и методах защиты данных.
3. Установите физический доступ только для авторизованного персонала и не позволяйте посторонним лицам посещать рабочую зону без разрешения.
4. Все компьютеры и серверы должны иметь установленное антивирусное программное обеспечение с регулярной установкой обновлений.
5. Для клиентских данных используйте зашифрованные каналы передачи данных и системы хранения.
6. При возникновении вопросов или подозрительной активности, связанной с безопасностью данных, обращайтесь к вышестоящим лицам.