Политика безопасности

Цели политики безопасности:

1. Не допустить распространения и разглашения конфиденциальной информации и учётным данных компании
2. Не допустить распространения и разглашения конфиденциальной информации и учётным данных клиентов
3. Обеспечить информационную безопасность и устойчивость работы ИТ инфраструктуры компании
4. Обеспечить сохранность личных данных сотрудников компании

Что нужно делать:

1. Создавать сложные пароли и менять их
2. Любую переданную информацию для работы, не разглашать за пределами компании
3. Пользоваться тем функционалом который описан в инструкциях компании
4. При любых подозрениях в нарушении информационной безопасности немедленно сообщить руководителю
5. Подключаться к клиентам используя функционал трекера
6. При получении учетных данных от клиентов, внести информацию в трекер и сразу удалить сообщение с учетными данными
7. При любом подозрении что ваши учетные данные могли быть скомпрометированы необходимо немедленно сообщить руководителю

Что нельзя делать:

1. Хранить в любом виде, любую информацию об адресах подключения, учетных данных, паролях в не зашифрованных файлах на любых компьютерах
2. Хранить файлы .rdp на рабочих компьютерах
3. Разглашать информацию о подключениях, учетных данных и.т.д
4. Хранить на личных компьютерах учетные базы и конфигурации
5. Использовать на рабочих компьютерах любые средства удаленного управления кроме стандартного rdp
6. Оставлять рабочие компьютеры не заблокированными
7. Использовать один и тот же пароль от разных элементов инфраструктуры компании
8. Записывать на бумаге учетные данные

Типичные ситуации: вопрос - ответ

1. Вопрос: Мне нужно подключиться к клиенту, как я могу это сделать? - Ответ: Если у клиента установлено подключение через VPN то необходимо сперва подключиться к VPN используя трекер, а затем в трекере нажать на кнопку «подключить по RDP»
2. Вопрос: Мне нужно подключиться к своему компьютеру из дома, как мне это сделать? - Ответ: Необходимо сначала подключиться по VPN используя свой доменный логин и пароль, а затем подключиться к своему компьютеру по IP адресу
3. Вопрос: Как узнать IP адрес своего компьютера для подключения? - Ответ: Выполнить к командной строке команду ipconfig

4. Вопрос: Где можно записать и хранить пароли от трекера и доменного пользователя? - Ответ: Хранить пароли в обычных файлах категорически запрещено! Пароли необходимо запомнить, это хоть и неудобно, но безопасность важнее. Также можно использовать менеджер паролей или зашифрованный файл
5. Вопрос: Что делать если нужно подключиться к своему компьютеру по Anydesk? - Ответ: Подключаться по Anydesk к своим рабочим компьютерам нельзя
6. Вопрос: Что делать если у клиента rdp подключение происходит по нестандартным файлам rdp или через сторонние сервисы(например Citrix)? - Отчет: Все нестандартные подключения необходимо хранить в зашифрованном виде, например архив с паролем
7. Вопрос: Можно ли хранить в файле пароли от VPN клиентов? - Нет, все логины и пароли должны храниться в трекере. Хранить пароли в файлах нельзя

1)