В качестве мер обеспечения безопасности при работе в системе ДБО Faktura.ru **рекомендуется:**

1. Исключить возможность неправомерного получения персональной информации пользователей систем ДБО (коды и пароли доступа). Не передавать такую информацию другим лицам, в том числе сотрудникам Вашей организации. Не записывать коды и пароли на бумажных носителях, доступных другим лицам. Не сообщать пароль IT-специалистам для проверки работы системы. При необходимости таких проверок владелец средств доступа обязан лично вводить свои логин и пароль в системе ДБО.
2. Обеспечить безопасное хранение секретных ключей электронно-цифровой подписи на внешнем носителе в недоступном месте: в сейфе или запираемом металлическом шкафу и т.п.
3. Не использовать внешние носители с ключами ЭП для каких-либо других целей, в частности, не хранить на них информацию произвольного содержания, не относящуюся к системе ДБО.
4. Никогда не копировать секретный ключ ЭП на жесткий диск компьютера.
5. Вставлять внешний носитель с ЭП только в момент подписания документов. Не оставлять внешний носитель с ключами ЭП постоянно подключенными к компьютеру. По завершении подписания документов отключите внешний носитель с ключами ЭП от компьютера.
6. Ограничить доступ к компьютеру (в том числе по локальной сети или для дистанционной поддержки), используемому Вами для работы с системой ДБО, обеспечить безопасность помещения, в котором он установлен. Если есть возможность, использовать для работы в системе ДБО отдельный компьютер. Сообщить в НКО Красноярский Краевой Расчетный Центр ООО диапазон допустимых IP-адресов и MAC-адресов, с которых будет выполняться подключение к системе ДБО.
7. Контролировать действия IT-специалистов, особенно внештатных, в момент технического обслуживания, установки программного обеспечения на компьютере, используемом для работы с системой ДБО.
8. Осуществлять постоянный контроль за отправляемыми платежными документами при работе с системой ДБО, а также состоянием Вашего счета.
9. Разграничить права на создание документа в системе ДБО и право его подписи с использованием ЭП.
10. Регулярно, не реже одного раза в месяц, производить смену паролей доступа в систему ДБО, при этом пароли должны содержать не менее 10 знаков (сложные сочетания букв и цифр), не должны иметь логической закономерности. В качестве пароля не следует использовать имена и даты рождения родственников, клички животных и т.п., не следует назначать пароль, используемый в системе ДБО, в любых других системах и сервисах.
11. Регулярно, не реже одного раза в год, производить перегенерацию ключей ЭП.
12. **В обязательном порядке производить перегенерацию ключей ЭП и смену паролей в следующих случаях:**

• при смене ответственных лиц, имеющих права доступа в систему ДБО;
• при обнаружении фактов доступа неуполномоченных лиц к ключевой информации (а также при подозрении о таком доступе, в том числе и удаленном доступе по сети);

13. Обеспечить защиту компьютера, с которого Вы работаете с системой ДБО:

• исключить с этого компьютера доступ в сеть Интернет за исключением адресов системы ДБО;
• не пользоваться на этом компьютере сервисами обмена мгновенными сообщениями (ICQ, Skype, Mail.Ru-Агент и т.п.)
• установить антивирусную программу и персональный межсетевой экран (firewall), регулярно

обновлять антивирусную базу;
• обеспечить защиту компьютера от несанкционированного доступа – настроить политики безопасности, обеспечить своевременную установку обновлений безопасности операционной системы, браузера Internet Explorer и прикладных программ;
• учетная запись Гость должна быть выключена;
• использовать только лицензионное программное обеспечение, полученное из доверенных источников и реально необходимое для работы на компьютере, на котором установлена система ДБО;
• устанавливать все официальные обновления к используемой операционной системе;
• при работе с электронной почтой обращать особое внимание на отправителя сообщения. Если отправитель Вам неизвестен - открывать вложения и иные присланные файлы категорически не рекомендуется, что бы ни было написано в тексте сообщения.
• не устанавливать и не сохранять подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных web-сайтов, присланные по электронной почте и т.д. В случае необходимости загрузки файла, обязательно проверьте его антивирусом перед использованием.
• не отвечать на подозрительные письма с просьбой выслать секретный ключ электронной цифровой подписи, пароль и другие конфиденциальные данные. Подобное письмо гарантированно создано злоумышленниками. Банк ни при каких обстоятельствах и ни в какой форме не запрашивает у клиентов конфиденциальную информацию о секретных ключах и паролях.

При обнаружении Вами попыток несанкционированного доступа или в случае мотивированных опасений, что такие попытки могут быть осуществлены, просим Вас:

• немедленно сообщить об этом в НКО Красноярский Краевой Расчетный Центр ООО по телефону *(391) 274-95-73 (доб. 159)*;
• блокировать технические средства, используемые для работы в системах ДБО;
• представить в НКО Красноярский Краевой Расчетный Центр ООО подробное письменное описание обстоятельств компрометации ключей или несанкционированного доступа.
Убедительно просим Вас неукоснительно соблюдать правила безопасности работы в системе ДБО.