ИНСТРУКЦИЯ ПО БЕЗОПАСНОСТИ *
Рекомендации для пользователей, работающих с Системой.

Для обеспечения максимальной защищенности пользователей Системы на стороне Клиента Банк рекомендует придерживаться следующих условий:

1. Система должна содержаться в соответствующем защищенном месте и не должна быть доступна третьим лицам.
2. Запрещается хранение ключевого носителя в местах, к которым не ограничен доступ третьих лиц;
3. Пользователи Системы не должны:

- вывешивать на рабочих местах в виде подсказок, записок, сохранять на любых носителях сведения о логинах и паролях, технологических шагах пользователей Системы, которые могут стать доступны третьим лицам, не обладающим правами пользователей в Системе;
- передавать, пересылать данные о логинах, паролях, ключевые носители третьим лицам;
- использовать личную информацию в пароле (дату рождения, имена, номера телефонов и т.п.), а так же пароли которые использовались ранее в Системе или других приложениях;
- передавать компьютеры для исправления технических проблем посторонним лицам вместе с ключевыми носителями;
- хранить закрытые ключи ЭЦП на любых носителях информации кроме тех, что предоставил Банк.

4. В случае, если Вам по телефону или по каким либо другим каналам обращается человек, который представляется сотрудником банка, ни при каких обстоятельствах не передавайте ему конфиденциальные данные, такие как ключевой носитель с ключами ЭЦП, логин и пароль для входа в Систему. Сообщите в Банк о данном случае, так как сотрудники банка никогда не будут запрашивать подобные данные.

5. В случае, если компьютер, с которого производится работа в Системе, неожиданно перестал запускаться или выдает непонятные сообщения, рекомендуется незамедлительно связаться со службой технической поддержки Банка и заблокировать работу Системы.

6. При возникновении подозрений, что кто-либо владеет информацией о Вашем пароле, необходимо самостоятельно сменить пароль или обратиться в Банк для блокировки учетной записи пользователя.

7. Если Вами было получено электронное сообщение с неизвестным вложением или со ссылкой на неизвестный Вам ресурс, необходимо удалить это сообщение, не открывая вложения и не активируя ссылку (особенно если в сообщении указано, что проблема безотлагательная, и при этом просят срочно открыть приложенный файл), так как эти вложения или ссылки могут содержать как сами вирусы, так и ссылки для скачивания и установки вредоносного кода. Кроме того, рекомендуется после получения такого письма провести полную проверку компьютера антивирусным средством.

8. При загрузке Системы обязательно проверяйте, что соединение установлено именно с сервером Банка и именно по адресу https://www.qazaqonline.kz для удостоверения, что вы работаете с сервисом Банка просмотрите сертификат SSL соединения

9. Для защиты компьютера от угроз из сети Интернет используйте лицензионную антивирусную систему со встроенным фаерволом (firewall) или установите отдельно лицензионный фаервол.

10. Проводите регулярные проверки компьютера, на котором установлена Система на предмет наличия вирусов с использованием обновленных антивирусных баз (рекомендуемая периодичность проверки не реже 1 раза в неделю, и обновление баз антивирусной системы по мере выпуска обновлений сигнатур).

11. Блокируйте компьютер и не оставляйте без присмотра Ключевой носитель.

12. Извлеките Ключевой носитель из USB порта каждый раз когда требуется покинуть рабочее место.

13. Используйте ключевой носитель только для работы в Системе.

14. Никогда не оставляйте ключевой носитель постоянно подключенным к компьютеру.