Приложение
к Приказу АО «Казахтелеком»
от «__» _____ 2022 года
№ _____

Политика «чистого стола» и «чистого экрана» в АО "Казахтелеком"

Алматы, 2022

Оглавление

1. Общие положения

1. Политика «чистого стола» и «чистого экрана» (далее - Политика) разработана с целью исключить утечку информации из-за ненадлежащего хранения документов на рабочем столе, содержащих конфиденциальные сведения, а также снизить риски в части бесконтрольного использования персональных компьютеров в АО «Казахтелеком».
2. Политика является основополагающим документом, отражающим суть работы с документами, электронными носителями информации с использованием ПК на рабочем месте (в том числе удаленно) при выполнении работниками Общества служебных обязанностей в повседневной деятельности.
3. Настоящий документ разработан в соответствии с требованиями регулятора, стандартов Республики Казахстан: СТ РК ISO/IEC 27001-2015 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования», СТ РК ISO/IEC 27002-2015 «Информационная технология. Средства обеспечения. Свод правил по управлению защитой информации». СТ РК ISO/IEC 27003-2012 «Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности».
4. Требования настоящей Политики являются неотъемлемой частью комплекса мер безопасности и защиты информации в Обществе.
5. Правила распространяются на всех работников структурных подразделений Общества, а также работников сторонних организаций, использующих в работе средства вычислительной техники (далее - СВТ) Общества и должны применяться для всех средств вычислительной техники, эксплуатируемых в Обществе.

2. Термины, определения и сокращения

6. Общество – АО «Казахтелеком»;
7. СВТ – средства вычислительной техники (стационарные компьютеры или рабочие станции, переносные компьютеры или ноутбуки и т.п.);
8. СП – структурное подразделение Общества;
9. СП ИБ – структурное подразделение информационной безопасности.
10. ИБ – информационная безопасность.
11. ПК – персональный компьютер.
12. Пользователь – работник Общества или представитель третьей стороны, работающий с ИС Общества и использующий её информационным ресурсом в соответствии с установленными правами и правилами доступа к информации;

13. Информация — сведения (сообщения, данные) независимо от формы их представления.
14. Информационные системы (далее ИС) - система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

3. Риски нарушения политики «чистого стола» и «чистого экрана»

15. В случае нарушения данной политики, существуют высокие риски несанкционированного доступа к данным в ИС Общества, и как следствие - их утечка, а также проникновение злоумышленника во внутреннюю сеть Общества с целью осуществления противоправной деятельности.
16. Высокие риски распространения служебной информации и информации ограниченного распространения.
17. В процессе работы при использовании персональных конфиденциальных данных, служебной и уязвимой информации важно проявлять бдительность с целью уменьшить риск от «просмотра» документов посторонними лицами. Проявлять осторожность при использовании ПК от просмотра монитора посторонними.

4. Требования политики

18. Работникам Общества запрещается оставлять в легкодоступных местах (на рабочем столе, в не закрываемых тумбочках и шкафах и т.д.) в свое отсутствие или в нерабочее время документы, содержащие конфиденциальные сведения;
19. Пользователям Общества запрещается оставлять (хранить) логины и пароли на бумажных носителях в доступных местах (на стикерах прикрепленных к мониторам, рабочим столам), тумбочках, шкафах и в др. незащищенных местах.
20. В отсутствие работника на своем рабочем месте или в нерабочее время документы, содержащие конфиденциальные сведения, должны храниться в ящиках, шкафах, сейфах и/или других приспособлениях, исключающих возможность их визуального просмотра и/или доступа посторонними лицами;
21. Во время работы с конфиденциальной информацией в присутствии посторонних лиц, работники обязаны предпринимать меры по защите от визуального просмотра и/или доступа к этим документам;
22. Для утилизации конфиденциальных документов, должны использоваться уничтожители бумаги;
23. Пользователям ПК запрещается оставлять без присмотра разблокированный персональный компьютер, ноутбук. В случае

отсутствия на рабочем месте, пользователи обязаны выйти из системы и/или активизировать системные средства защиты от несанкционированного доступа (временная блокировка экрана);

24. Для предотвращения просмотра электронных документов посторонними лицами, пользователям запрещается сохранять электронные документы, содержащие конфиденциальные сведения, на «рабочем столе» персонального компьютера, ноутбука;
25. Пользователям запрещается хранение конфиденциальных данных в рукописных и/или электронных черновиках (почтовые черновики);
26. Документы, содержащие важную информацию, должны удаляться с принтеров немедленно (Включая ненапечатанные экземпляры из очереди на печать);
27. Напечатанные документы с конфиденциальной информацией необходимо изымать из принтеров незамедлительно;

5. Ответственность

28. Контроль за выполнением требований и правил Политики возлагается на СП ИБ.
29. Ответственность за актуальность Политики, а также внесение в нее изменений возлагается на СП ИБ.
30. Ответственность за обеспечение исполнения требований Политики возлагается на все СП в рамках их полномочий и в соответствии с положениями, установленными Политикой и разработанными на ее основе документами.
31. Руководители СП несут ответственность за своевременное доведение требований Политики до работников их подразделений и/или представителей третьих сторон в части их касающейся и за выполнение работниками их подразделений и/или представителями третьих сторон требований Политики.
32. В случае выявления нарушений требований настоящей Политики работниками Общества, включая любое преднамеренное действие, предпринимаемое с целью нарушить требования данной Политики, которые повлекли или могли повлечь серьезный ущерб бизнес-деятельности Общества, должно инициироваться и вестись служебное расследование со стороны СП ИБ.
33. Несоблюдение мер, предусмотренных настоящей Политикой, влечет за собой ответственность в соответствии с действующим законодательством РК и внутренними документами Общества.