Appendix
to the Order of Kazakhtelecom JSC
dated __ _____ 2022
No. _____

Clean Desk and Clean Screen Policy in Kazakhtelecom JSC

Almaty, 2022

Contents

1. General Provisions

1. The Clean Desk and Clean Screen Policy (hereinafter referred to as the Policy) is designed to exclude information leakage due to improper storage of documents on the desktop containing confidential information, as well as to reduce risks in terms of uncontrolled use of personal computers in Kazakhtelecom JSC.
2. The Policy is a fundamental document reflecting the essence of work with documents, electronic media using PCs at the workplace (including remotely) when the Company's employees perform their official duties in their daily activities.
3. This document is developed in accordance with the requirements of the regulator, standards of the Republic of Kazakhstan: ST RK ISO/IEC 27001-2015 "Information technology. Methods and means of ensuring security. Information security management systems. Requirements", ST RK ISO/IEC 27002-20-15 "Information technology. Means of ensuring. Code of rules for information protection management". ST RK ISO/IEC 27003-2012 "Information technology. Methods of ensuring security. Guidelines for the implementation of information security management system".
4. The requirements of this Policy are an integral part of the Company's information security and protection measures.
5. The Policy shall apply to all employees of the Company's structural subdivisions, as well as employees of third-party organizations using the Company's computer equipment (hereinafter referred to as "CE") in their work and shall apply to all computer equipment operated by the Company.

2. Terms, Definitions and Abbreviations

6. Company - Kazakhtelecom JSC;
7. CE – computer equipment (stationary computers or workstations, portable computers or laptops, etc.);
8. SS - structural subdivision of the Company;
9. SS IS - a structural subdivision of information security.
10. IS - information security.
11. PC - personal computer.
12. User - an employee of the Company or a representative of a third party working with the Company's IS and using its information resource in accordance with the established rights and rules of access to information;
13. Information - information (messages, data) irrespective of the form of its presentation.
14. Information systems (hereinafter referred to as IS) - a system designed for storage, retrieval and processing of information, and relevant organizational resources (human, technical, financial, etc.) that provide and disseminate information.

3. Risks of Violating the Clean Desk and Clean Screen Policies

15. In case of violation of this policy, there are high risks of unauthorized access to data in the Company's IS, and as a consequence - their leakage, as well as intruder's penetration into the Company's internal network in order to carry out illegal activities.
16. High risks of dissemination of proprietary and restricted information.
17. In the course of work when using personal confidential data, proprietary and vulnerable information, it is important to be vigilant in order to reduce the risk of unauthorized persons “viewing” documents. Exercise caution when using a PC to prevent unauthorized persons from viewing the monitor.

4. Policy requirements

18. Employees of the Company are prohibited to leave documents containing confidential information in easily accessible places (on the desk, in unclosed nightstands and cabinets, etc.) in their absence or outside working hours;
19. Users of the Company are prohibited to leave (keep) logins and passwords on paper in accessible places (on stickers attached to monitors, desktops), nightstands, cabinets and other unprotected places.
20. In the absence of an employee at his/her workplace or outside working hours, documents containing confidential information shall be stored in drawers, cabinets, safes and/or other devices that exclude the possibility of their visual viewing and/or access by unauthorized persons;
21. While working with confidential information in the presence of unauthorized persons, employees shall take measures to protect themselves from visual viewing and/or access to these documents;
22. Paper shredders shall be used to dispose of confidential documents;
23. PC users are prohibited to leave an unlocked personal computer or laptop unattended. In case of absence from the workplace, users must log out of the system and/or activate system means of protection against unauthorized access (temporary screen locking);
24. To prevent unauthorized persons from viewing electronic documents, users are prohibited to save electronic documents containing confidential information on the “desktop” of a personal computer, laptop;
25. Users are prohibited from storing confidential data in handwritten and/or electronic drafts (postal drafts);
26. Documents containing sensitive information must be removed from printers immediately (Including unprinted copies from the print queue);
27. Printed documents containing confidential information should be removed from printers immediately;

5. Responsibilities

28. Control over compliance with the requirements and rules of the Policy shall be vested in the SS IS.
29. Responsibility for keeping the Policy up-to-date, as well as for making amendments to it, shall be vested in the SS IS.
30. Responsibility for ensuring compliance with the requirements of the Policy shall be vested in all SSs within the scope of their authority and in accordance with the provisions set forth in the Policy and the documents developed on its basis.
31. Heads of the SS shall be responsible for timely communication of the Policy requirements to the employees of their subdivisions and/or third party representatives as they relate to them and for compliance by the employees of their subdivisions and/or third party representatives with the requirements of the Policy.
32. In case of detection of violations of the requirements of this Policy by the Company's employees, including any intentional action taken with the purpose to violate the requirements of this Policy, which have caused or may have caused serious damage to the Company's business activities, an internal investigation shall be initiated and conducted by the SS IS.
33. Failure to comply with the measures stipulated by this Policy shall entail liability in accordance with the applicable laws of the Republic of Kazakhstan and internal documents of the Company.