APPROVED

By order No. 8 of 14 July 2026

of the director of
Korporativ Maslahat Tizimlari LLC

PRIVACY POLICY

Korporativ Maslahat Tizimlari LLC

KMT-PP-004 / Version 1.0

Bukhara 2026

PASSPORT OF THE DOCUMENT

Document title	Privacy Policy
Document code	KMT-PP-004
Version	1.0
Document status	Active
Document type	Local regulatory act
Organization	Korporativ Maslahat Tizimlari LLC
Scope of application	All structural divisions and employees of the Company
Approved	By order of the director of Korporativ Maslahat Tizimlari LLC No. 8 dated July 14, 2026.
Put into effect	July 15, 2026
Developed by	Director of Korporativ Maslahat Tizimlari LLC
Checked	Director of Korporativ Maslahat Tizimlari LLC
Approved	Director of Korporativ Maslahat Tizimlari LLC
Next revision	No later than January 1, 2029, or in the event of a change in the legislation of the Republic of Uzbekistan or the internal requirements of the Company
Cancellation of a document	Until replaced by a new version or cancelled by order of the director
Number of pages	27
Number of applications	3

Director's address

Dear colleagues, clients and partners!

Trust is one of the main values of Korporativ Maslahat Tizimlari LLC. Our activities are based on the principles of professional independence, objectivity, integrity, and strict confidentiality of information obtained in the provision of appraisal, consulting, and other professional services.

Every day, we receive documents containing commercial, financial, technical, investment, and other sensitive information. We recognize our responsibility for its security and consider information protection an integral part of the quality of our services.

This Privacy Policy sets forth uniform corporate requirements for the processing, storage, use and protection of information accessed by the Company's employees in the performance of their official duties.

Each employee of the Company is obliged to comply with the requirements of this Policy, regardless of the position held, length of service, or nature of the functions performed.

We believe that maintaining confidentiality is essential to maintaining the trust of our clients, partners, investors, government agencies, and other stakeholders.

Director
of Korporativ Maslahat Tizimlari LLC

Table of contents

Document status 6
Privacy Policy 7
Chapter 1. General Provisions 8
Article 1. Subject of regulation 8
Article 2. Objectives of Policy 8
Article 3. Scope of Policy 9
Chapter 2. Basic concepts and principles of ensuring confidentiality 9
Article 4. Basic concepts 9
Article 5. Principles of Ensuring Confidentiality 10
Article 6. Categories of confidential information 11
Article 7. Confidentiality of Client Information 12
Article 8. Commercial secrets of the Company 12
Article 9. Processing of confidential information 13
Article 10. Storage of confidential information 14
Article 11. Transfer of confidential information 14
Article 12. Destruction of confidential information 15
Chapter 5. Confidentiality in the Provision of Professional Services 15
Article 13. Confidentiality in the implementation of appraisal activities 15
Article 14. Confidentiality in the provision of consulting services 16
Article 15. Confidentiality of investment projects 17
Article 16. Confidentiality of negotiations and business correspondence 17
Chapter 6. Information Security and Information Protection 18
Article 17. Organizational measures for information protection 18
Article 18. Protection of paper documents 19
Article 19. Protection of electronic documents and information systems 19
Article 20. Use of e-mail, cloud services and communication tools 20
Article 21. Actions in case of violation of confidentiality 20
Chapter 7. Rights, Duties and Responsibilities 20
Article 22. Employees' rights in the field of confidentiality 21
Article 23. Duties of Company Employees 21
Article 24. Duties of managers 21

Article 25. Liability for Violation of Policy 22
Chapter 8. Final Provisions 22
Article 26. Monitoring the implementation of Policy 22
Article 27. Revision of Policy 23
Article 28. Final Provisions 23
Corporate Declaration 24
Official publication 24
Appendix No. 1 25
Appendix No. 2 26
Appendix No. 3 27

Document status

This Privacy Policy is a local regulatory act of Korporativ Maslahat Tizimlari LLC, which defines uniform requirements for ensuring the confidentiality of information, the protection of personal data, commercial secrets and other restricted information received, processed, used and stored in the course of the Company’s activities.

The Policy establishes uniform principles and requirements for the processing, use, storage, transfer, and protection of confidential information, defines the responsibilities of the Company's employees to maintain confidentiality, and also measures aimed at preventing unauthorized access, disclosure, loss, modification, or destruction of information.

The provisions of this Policy are binding on all Company employees, regardless of their position, the nature of their work, the type of employment relationship, or their length of service. The requirements of this Policy are also taken into account when interacting with clients, business partners, contractors, and other individuals who have access to the Company's confidential information.

This Policy is applied in conjunction with the Anti-Corruption Policy, the Code of Professional Ethics, the Quality Policy, the Internal Labor Regulations and other internal regulatory documents of Korporativ Maslahat Tizimlari LLC.

The privacy policy is one of the key elements of the corporate governance system of Korporativ Maslahat Tizimlari LLC and reflects the Company's commitment to the principles of legality, professional responsibility, information protection, respect for customer rights, information security and maintaining the trust of all stakeholders.

Privacy Policy

Korporativ Maslahat Tizimlari LLC considers ensuring the confidentiality of information as one of the key elements of corporate governance, professional activity and the internal control system.

We undertake the following obligations:

- ensure the protection of information of clients, partners and the Company;
- comply with the requirements of the legislation of the Republic of Uzbekistan in the field of information and personal data protection;
- prevent unauthorized access to documents and information;
- use confidential information solely for the purpose of fulfilling professional duties;
- ensure the safety of documents regardless of the form in which they are stored;
- continuously improve internal information security procedures;
- regularly raise the level of awareness of employees on information security issues;
- minimize the risks of information leakage;
- apply modern organizational and technical measures to protect information;
- ensure transparency of internal information management processes.

The Company's management guarantees that compliance with the requirements of this Policy is a mandatory condition for the company's activities and one of the most important factors in maintaining the business reputation of Korporativ Maslahat Tizimlari LLC.

Chapter 1. General Provisions

Article 1. Subject of regulation

1. This Privacy Policy (hereinafter referred to as **the Policy**) defines the uniform corporate requirements of Korporativ Maslahat Tizimlari LLC (hereinafter referred to as **the Company**) to ensure the confidentiality of information, the protection of personal data, commercial secrets and other restricted information received, created, processed, used and stored in the course of professional activities.

2. This Policy governs relations related to the collection, receipt, registration, processing, use, transfer, storage, archiving, protection and destruction of information, access to which is restricted by the legislation of the Republic of Uzbekistan, contractual obligations or internal regulatory documents of the Company.

3. The policy is aimed at ensuring the legitimate interests of the Company, its clients, business partners, employees, investors, banks, government agencies and other interested parties by creating a unified system for ensuring information confidentiality.

4. The requirements of this Policy apply to all types of professional activities of the Company, including the provision of services for property and business valuation, business consulting, development of business plans, preparation of feasibility studies (FS), financial modeling, support of investment projects, development of development strategies, as well as other types of activities carried out by the Company.

5. This Policy is mandatory for all employees of the Company, regardless of the position they hold, the nature of the work they perform, the type of employment relationship, length of service, and the place where their job responsibilities are performed.

6. The requirements of this Policy also apply to consultants, experts, interns, contractors, temporary workers, representatives of counterparties and other persons who have been granted access to the Company's confidential information in accordance with the established procedure.

Article 2. Objectives of the Policy

7. The main objectives of this Policy are:

- ensuring reliable protection of the Company’s confidential information;
- compliance with the requirements of the legislation of the Republic of Uzbekistan in the field of information and personal data protection;
- protection of the legal rights and interests of the Company’s clients, partners and employees;
- preventing unauthorized access, use, disclosure, modification, destruction or loss of confidential information;
- establishing uniform corporate requirements for handling restricted information;
- minimizing the risks of information leakage;

- strengthening the trust of customers, banks, investors, government agencies and business partners;
- Ensuring a high level of information security for the Company;
- increasing the responsibility of employees for maintaining confidentiality;
- improving the corporate governance system in the field of information security.

Article 3. Scope of the Policy

8. This Policy applies to all structural divisions of the Company and extends to all processes related to the creation, receipt, processing, use, transfer, storage and destruction of information, regardless of the form in which it is presented.

9. The requirements of this Policy apply to information contained:

- in paper documents;
- in electronic documents;
- in information systems;
- in corporate email;
- in cloud services;
- on removable storage media;
- in official correspondence;
- in audio, photo and video materials;
- in presentations, reports, conclusions and other documents of the Company.

10. This Policy shall be applied in conjunction with the Anti-Corruption Policy, the Code of Professional Ethics, the Quality Policy, the Internal Labor Regulations, and other internal regulatory documents of the Company.

11. If an international treaty of the Republic of Uzbekistan or the legislation of the Republic of Uzbekistan establishes other requirements for ensuring the confidentiality of information, the provisions of the relevant international treaty or legislation shall apply.

12. Compliance with the requirements of this Policy is one of the mandatory conditions for carrying out professional activities in the Company and is considered the most important element of the corporate culture, risk management system, quality management system and business reputation of the Company.

Chapter 2. Basic concepts and principles of confidentiality

Article 4. Basic concepts

13. For the purposes of this Policy, the following basic concepts are used:

1) confidential information – any information, regardless of the form of its presentation, access to which is restricted by the legislation of the Republic of Uzbekistan, contractual

obligations or internal regulatory documents of the Company and the disclosure of which may cause damage to the Company, its clients, partners or other interested parties;

2) personal data – information relating to a specific individual or allowing his/her identification, the processing of which is carried out in accordance with the legislation of the Republic of Uzbekistan;

3) commercial secret – information that has actual or potential commercial value due to its being unknown to third parties, to which there is no free access on legal grounds and in relation to which the Company takes measures to maintain its confidentiality;

4) information processing – any action or set of actions performed with or without the use of automation tools, including collection, receipt, registration, systematization, accumulation, storage, clarification, modification, use, transfer, depersonalization, archiving, destruction and other actions with information;

5) dissemination of information – actions aimed at disclosing information to an indefinite number of persons;

6) provision of information – transfer of information to a specific person or a specific group of persons on legal grounds;

7) information security – the state of protection of information, information resources and information systems of the Company from unauthorized access, use, modification, destruction, blocking, copying, distribution or other illegal actions;

8) information carrier – any material or electronic object intended for storing, transmitting or processing information, including paper documents, electronic files, databases, servers, cloud services, removable storage media and other technical means;

9) confidentiality regime – a set of organizational, legal and technical measures aimed at restricting access to confidential information and ensuring its protection;

10) third party – any individual or legal entity that is not the Company or its employee and does not have legal grounds for access to the relevant information.

Article 5. Principles of Ensuring Confidentiality

14. The Company ensures the protection of confidential information based on the following principles:

- legality;
- good faith;
- professional responsibility;
- restrictions on access to information;
- minimum required access;
- protection of the rights and legitimate interests of clients;
- information security;
- reliability of information;

- integrity of information;
- continuity of information security;
- personal responsibility of employees;
- continuous improvement of the information security system.

15. The Company processes confidential information only to the extent necessary to fulfill contractual obligations, comply with the requirements of the legislation of the Republic of Uzbekistan, ensure its business activities and achieve the legitimate purposes of information processing.

16. Access to confidential information is granted exclusively to those employees who need such information to perform their job duties.

17. Each employee of the Company is obliged to maintain confidentiality regardless of the method of obtaining information, the form of its storage, the period of document creation, and the duration of the employment relationship with the Company.

18. The transfer of confidential information is permitted only if there are legal grounds, contractual obligations, or a written decision of an authorized official of the Company.

19. The Company shall take the necessary organizational, administrative, technical and legal measures to prevent the loss, misuse, modification, destruction, blocking, copying or disclosure of confidential information.

20. The Company's management considers ensuring the confidentiality of information as one of the key elements of corporate governance, risk management, the quality management system and sustainable development of the Company.

21. Compliance with the principles established by this Policy is a mandatory condition for the performance of professional activities by all employees of the Company and one of the main factors in maintaining the trust of clients, partners, investors, banks, government agencies and other interested parties.

Chapter 3. Confidential Information

Article 6. Categories of confidential information

22. The Company classifies as confidential any information, access to which is restricted by the legislation of the Republic of Uzbekistan, the terms of contracts, internal regulatory documents of the Company or the nature of professional activities and the disclosure of which may cause property, financial, reputational or other damage to the Company, its clients, partners or other interested parties.

23. The Company’s confidential information includes, but is not limited to:

- personal data of employees, clients and other individuals;
- commercial secret of the Company;
- commercial secrets of clients and business partners;

- information obtained in the performance of contractual obligations;
- restricted information provided by government agencies;
- results of professional activities of the Company's employees;
- information contained in internal information systems;
- financial, accounting and tax information;
- information about bank accounts and financial transactions;
- internal reports, analytical materials and official correspondence;
- information, access to which is restricted by confidentiality agreements (NDA);
- other information classified by the Company as confidential.

24. The Company has the right to classify other information as confidential if the need to protect it is determined by the requirements of the legislation of the Republic of Uzbekistan, contractual obligations, or the interests of ensuring the security and sustainable operations of the Company.

Article 7. Confidentiality of client information

25. The Company guarantees the confidentiality of information received from clients when providing professional services.

26. Client information is used solely for the purpose of fulfilling contractual obligations, preparing reports, opinions, analytical materials and other documents stipulated by the terms of the contract or legal requirements.

27. The Company does not disclose information about clients, the content of projects carried out, the cost of services, assessment results, financial indicators, investment projects, business plans, feasibility studies, financial models, development strategies and other documents without the written consent of the client, except in cases stipulated by the legislation of the Republic of Uzbekistan.

28. The Company's employees are not entitled to use clients' information for personal interests, transfer it to third parties, or use it after termination of employment with the Company.

29. All materials received from the client are subject to storage in accordance with the Company's internal rules and the requirements of the legislation of the Republic of Uzbekistan.

Article 8. Commercial secrets of the Company

30. The Company takes the necessary measures to protect information constituting a commercial secret in order to maintain its competitiveness, business reputation and economic stability.

31. The Company's commercial secrets may include:

- business strategies;

- Company development strategies;
- financial plans;
- internal budgets;
- methods of performing work;
- own methodological developments;
- customer databases;
- partner databases;
- information about suppliers;
- internal regulations and technologies for performing work;
- marketing research;
- results of analytical studies;
- internal commercial proposals;
- terms of contracts;
- information about negotiations;
- pricing information;
- proprietary software;
- objects of intellectual property;
- other information recognized by the Company as a commercial secret.

32. The list of information constituting a commercial secret may be specified by the Company's internal regulatory documents.

33. Employees of the Company are obliged to ensure the safety of commercial secrets both during the period of work in the Company and after the termination of employment, unless otherwise provided by the legislation of the Republic of Uzbekistan or concluded agreements.

34. The transfer of information constituting a commercial secret is permitted only in cases stipulated by the legislation of the Republic of Uzbekistan, the terms of the agreement, or on the basis of a written decision of the Director of the Company.

35. The Company has the right to apply organizational, legal and technical measures to protect commercial secrets provided for by the legislation of the Republic of Uzbekistan and the internal regulatory documents of the Company.

Chapter 4. Processing and protection of confidential information

Article 9. Processing of confidential information

36. The Company processes confidential information solely on legal grounds, within the limits of its authority, and only to the extent necessary to achieve the goals associated with the performance of its professional activities.

37. Processing of confidential information is carried out in accordance with the legislation of the Republic of Uzbekistan, the terms of concluded agreements, the internal regulatory documents of the Company and this Policy.

38. The Company ensures the legality, reliability, relevance and sufficiency of the information processed, excluding the processing of information not related to the achievement of the stated goals.

39. When processing confidential information, the Company takes measures to prevent its accidental or unlawful destruction, modification, blocking, copying, distribution or other illegal actions.

40. The Company's employees are obliged to use confidential information only within the limits of the powers granted to them and only for the performance of their official duties.

Article 10. Storage of confidential information

41. The Company shall organize the storage of confidential information in a manner that ensures its safety, integrity, accessibility for authorized persons, and protection from unauthorized access.

42. Paper documents containing confidential information must be stored in premises that prevent access by unauthorized persons.

43. Electronic documents are stored in corporate information systems protected by technical means of access restriction.

44. The storage periods for documents are determined by the legislation of the Republic of Uzbekistan, the terms of contracts, the internal regulatory documents of the Company and the nomenclature of cases.

45. Upon expiration of the established storage periods, documents are destroyed or transferred to the archive in accordance with the procedure established by the Company's internal regulatory documents.

Article 11. Transfer of confidential information

46. The transfer of confidential information is permitted only if there are legal grounds and only to the extent necessary to achieve the specific purpose of the transfer.

47. The transfer of information to government agencies is carried out in cases and in the manner stipulated by the legislation of the Republic of Uzbekistan.

48. The transfer of information to clients, partners, auditors, consultants, experts and other persons is carried out in accordance with concluded contracts, confidentiality agreements or other legal grounds.

49. The Company's employees are prohibited from transmitting confidential information via unsecured communication channels or using for these purposes personal email

accounts, unauthorized cloud services, and other information resources not approved by the Company.

50. Any transfer of confidential information must be carried out in compliance with the principle of the minimum necessary volume of disclosed information.

Article 12. Destruction of confidential information

51. Destruction of documents and other information carriers is carried out after the expiration of the established storage periods or when there is no need for their further use, unless otherwise provided by the legislation of the Republic of Uzbekistan.

52. Destruction of confidential information must exclude the possibility of its subsequent recovery or use by third parties.

53. Paper documents are destroyed in a manner that makes it impossible to read the information they contain.

54. Electronic information carriers are subject to erasure or destruction using methods that make it impossible to recover the information.

55. Responsibility for compliance with the established procedure for the destruction of confidential information lies with the Company's employees authorized to perform the relevant actions, as well as their immediate supervisors.

Chapter 5. Confidentiality in the Provision of Professional Services

Article 13. Confidentiality in the implementation of appraisal activities

56. The Company ensures the confidentiality of all information received during the provision of services for the valuation of property, business, property rights, intellectual property, financial assets and other objects of valuation.

57. Confidential information during the implementation of assessment activities includes:

- documents provided by the customer;
- information about property owners;
- financial statements;
- accounting documents;
- tax information;
- technical documentation;
- design documentation;
- results of inspections of the assessed objects;
- cost calculations;
- working materials of appraisers;

- draft reports;
- final assessment reports;
- information on the cost of services;
- correspondence with the customer;
- other information obtained during the assessment process.

58. The Company does not disclose the contents of assessment reports, interim calculations, working documents and other materials to third parties without the written consent of the customer, except in cases stipulated by the legislation of the Republic of Uzbekistan.

59. The Company's employees are obliged to use the information obtained during the assessment solely for the purpose of fulfilling the contract and are not entitled to use it for personal interests or for the interests of third parties.

Article 14. Confidentiality in the provision of consulting services

60. When providing consulting services, the Company ensures the protection of all information received from clients or created during the course of the project.

61. Confidential information when providing consulting services includes, but is not limited to:

- business plans;
- feasibility studies;
- financial models;
- investment projects;
- development strategies;
- marketing research;
- financial analysis;
- business diagnostic results;
- internal documents of the client;
- investment presentations;
- analytical materials;
- recommendations of consultants;
- results of negotiations;
- correspondence with the client;
- other project materials.

62. The Company shall not use the results of completed projects, in whole or in part, for its own commercial purposes without the prior written consent of the client, unless otherwise provided by the contract.

63. The Company's employees are obliged to ensure the safety of all project materials both during the execution of the work and after the completion of the contract.

Article 15. Confidentiality of investment projects

64. The Company considers clients' investment projects to be information with a high level of confidentiality.

65. The following are subject to special protection:

- investment concepts;
- business models;
- financial settlements;
- sources of funding;
- investment memoranda;
- negotiation materials;
- draft agreements;
- financing terms;
- investment presentations;
- information about investors;
- information about potential partners;
- results of negotiations;
- project implementation schedules;
- information on project costs;
- other materials of investment projects.

66. The Company takes additional organizational measures to restrict access to investment project materials and provides access exclusively to employees directly involved in the implementation of the relevant project.

67. Publication of information on investment projects, use of projects in marketing materials, posting of information on the Company's official website, or use of projects as examples of completed work are permitted only with the prior written consent of the client.

Article 16. Confidentiality of negotiations and business correspondence

68. The Company ensures confidentiality of negotiations with clients, investors, government agencies, financial institutions, contractors and other business partners.

69. All business correspondence is considered confidential, regardless of the method of its implementation, including:

- email;
- official letters;
- documents transmitted through electronic document management systems;
- messages in corporate messengers;
- meeting minutes;
- minutes of negotiations;
- memos;
- other forms of official exchange of information.

70. It is prohibited to transfer the content of negotiations, correspondence or other materials to persons not involved in the relevant project without legal grounds or permission from the authorized manager.

71. The Company's employees are obliged to maintain the confidentiality of information obtained during negotiations, regardless of whether an agreement was concluded as a result of such negotiations or not.

Chapter 6. Information security and information protection

Article 17. Organizational measures for information protection

72. The Company ensures the protection of confidential information through a set of organizational, legal, administrative and technical measures aimed at preventing unauthorized access, use, disclosure, modification, destruction or loss of information.

73. Organizational measures for information protection include:

- delimitation of employees' rights of access to information;
- determination of access levels to information resources;
- maintaining confidentiality;
- familiarization of employees with the Company’s internal regulatory documents;
- conducting briefings on information security issues;
- concluding confidentiality agreements where necessary;
- monitoring compliance with the requirements of this Policy;
- Conducting internal audits of compliance with the confidentiality regime;
- application of penalties for violation of the requirements of this Policy.

74. Access to confidential information is provided only to the extent necessary for the employee to perform his or her job duties.

75. Granting, changing or terminating access rights is carried out by decision of the authorized manager in accordance with the Company's internal procedures.

Article 18. Protection of paper documents

76. Paper documents containing confidential information must be stored in conditions that prevent access by unauthorized persons.

77. The Company's employees are obliged to ensure the safety of documents both during working hours and after the end of the working day.

78. The following is not permitted:

- leave confidential documents unattended;
- transfer documents to persons who do not have the appropriate authority;
- copy documents without official need;
- take documents outside the Company without appropriate permission;
- destroy documents in violation of established procedures.

79. The transfer of paper documents is carried out in compliance with the requirements of this Policy and the internal regulatory documents of the Company.

Article 19. Protection of electronic documents and information systems

80. The Company takes the necessary measures to protect electronic documents, information systems, databases and other digital resources.

81. The following may be used to protect information:

- differentiation of user access rights;
- individual employee accounts;
- complex passwords and updating them regularly;
- antivirus protection;
- backup of information;
- user activity logs;
- encryption of information if necessary;
- corporate network protection;
- other technical means of information security.

82. The Company's employees are prohibited from:

- transfer your credentials to other persons;
- use other people's accounts;
- install unauthorized software;
- disable information security tools;

- use corporate information systems for personal purposes if this may create a threat to information security.

Article 20. Use of e-mail, cloud services and communication tools

83. Corporate email is used exclusively for official duties.

84. The transfer of confidential information by e-mail is permitted only if there is an official need and in compliance with information security requirements.

85. The use of cloud services is permitted only subject to their approval by the Company and compliance with established information security requirements.

86. The Company’s employees are prohibited from:

- forward confidential information to personal email addresses;
- storing official documents in unauthorized cloud storage;
- use personal devices to store confidential information without the permission of the Company's management;
- use unsecured communication channels to transmit restricted information.

87. The use of corporate instant messengers, video conferencing and other means of electronic interaction is carried out in compliance with the requirements of this Policy and the internal regulatory documents of the Company.

Article 21. Actions in case of violation of confidentiality

88. Each employee of the Company is obliged to immediately inform his immediate supervisor or the director of the Company of any case known to him:

- loss of documents;
- unauthorized access to information;
- disclosure of confidential information;
- attempts to obtain information by unauthorized persons;
- violations of the requirements of this Policy;
- other incidents that pose a threat to information security.

89. Upon receiving information about a possible breach of confidentiality, the Company organizes an internal review of the circumstances of the incident, takes measures to minimize possible consequences and prevent the recurrence of similar incidents.

90. The Company’s employees are obliged to provide assistance in conducting internal investigations of incidents related to violations of the requirements of this Policy.

91. The Company takes all reasonable measures to minimize damage, restore information security, and improve the information security system based on the results of each identified incident.

Chapter 7. Rights, Duties and Responsibilities

Article 22. Employees' rights in the field of confidentiality

92. The Company's employees have the right to:

- obtain access to confidential information within the scope of their official duties;
- receive clarification on the application of this Policy;
- use corporate information resources in accordance with established powers;
- report any identified violations of the confidentiality regime to the Company's management;
- make proposals for improving the information security system;
- count on the protection of their legitimate interests if they comply in good faith with the requirements of this Policy.

Article 23. Duties of the Company's employees

93. Each employee of the Company is obliged to:

- comply with the requirements of the legislation of the Republic of Uzbekistan, this Policy and other internal regulatory documents of the Company;
- ensure the safety of confidential information that has become known to him in the performance of his official duties;
- use confidential information solely for official purposes;
- comply with the established procedure for processing, storing and transmitting information;
- take reasonable steps to prevent the loss of documents and electronic data;
- comply with information security requirements when working with corporate information systems;
- prevent the use of confidential information for personal interests or for the interests of third parties;
- immediately notify the Company's management of all cases of loss of documents, unauthorized access to information or other violations of confidentiality;
- comply with the requirements of this Policy after the termination of employment in terms of information that is not subject to disclosure in accordance with the legislation of the Republic of Uzbekistan, contracts and internal regulatory documents of the Company.

Article 24. Duties of managers

94. Heads of structural divisions are obliged to:

- ensure compliance with the requirements of this Policy by employees of the division;

- organize work with confidential information in accordance with the Company's internal regulatory documents;
- provide access to information only to authorized employees;
- monitor compliance with the confidentiality regime;
- take immediate action upon detection of violations of the requirements of this Policy;
- ensure timely conduct of briefings and familiarization of employees with internal regulatory documents;
- to promote continuous improvement of the information security system.

Article 25. Liability for Violation of the Policy Requirements

95. Persons guilty of violating the requirements of this Policy shall be liable in accordance with the legislation of the Republic of Uzbekistan, the terms of the employment contract, the internal regulatory documents of the Company and other local acts.

96. Violations of the requirements of this Policy, in particular, are recognized as:

- unlawful disclosure of confidential information;
- use of information for personal interests;
- transfer of information to third parties without legal grounds;
- violation of the established procedure for storing documents;
- failure to comply with information security requirements;
- use of unauthorized information systems or software;
- loss of documents or electronic storage media due to the employee's fault;
- failure to promptly report any violations of confidentiality;
- other actions (inactions) that resulted in a violation of the requirements of this Policy.

97. Depending on the nature and consequences of the violation, disciplinary, material, civil, administrative or other liability measures provided for by the legislation of the Republic of Uzbekistan may be applied to the guilty persons.

98. If a violation of the requirements of this Policy has caused property, financial or reputational damage to the Company, a client or another person, the guilty party may be held liable in accordance with the procedure established by the legislation of the Republic of Uzbekistan.

Chapter 8. Final Provisions

Article 26. Monitoring the implementation of the Policy

99. General control over the implementation of this Policy is exercised by the Director of the Company.

100. Heads of structural divisions ensure compliance with the requirements of this Policy by employees of the relevant divisions and carry out ongoing internal control over compliance with the confidentiality regime.

101. The Company has the right to conduct internal audits of compliance with the requirements of this Policy, analyze the effectiveness of current information security measures and make decisions on their improvement.

Article 27. Revision of Policy

102. This Policy is subject to mandatory revision in the following cases:

- changes in the legislation of the Republic of Uzbekistan;
- changes in the organizational structure of the Company;
- changes in the nature of services provided;
- implementation of new information technologies;
- changes in the Company's internal processes;
- identifying the need to improve the information security system;
- other circumstances affecting the confidentiality of information.

103. Amendments and additions to this Policy are approved by order of the Director of the Company and come into force on the date specified in the relevant order, unless another period is established by the order itself.

Article 28. Final Provisions

104. This Policy shall enter into force on the date established by order of the Director of the Company and shall remain in effect until a new version is approved or it is declared invalid.

105. This Policy is the official internal regulatory document of Korporativ Maslahat Tizimlari LLC and is mandatory for all employees of the Company.

106. The Company ensures that employees are familiarized with this Policy upon hiring, as well as when changes and additions are made to it.

107. The current version of this Policy is stored by the Company and posted on the Company's official website in order to ensure openness of corporate governance and inform clients, partners, government agencies and other interested parties about current corporate standards for the protection of confidential information.

108. Compliance with the requirements of this Policy is one of the main conditions for maintaining the business reputation of the Company, strengthening the trust of customers and partners, ensuring information security and sustainable development of Korporativ Maslahat Tizimlari LLC.

Corporate declaration

Korporativ Maslahat Tizimlari LLC considers this Privacy Policy to be a fundamental document of its corporate governance system, aimed at ensuring information security, strengthening customer and partner trust, and improving the Company's operational efficiency.

The Company believes that information confidentiality is not only a legal and contractual requirement, but also a fundamental principle of professional activity, business reputation, and corporate culture.

Every Company employee, regardless of their position, is personally responsible for maintaining confidentiality, safeguarding information, and preventing its unauthorized use or disclosure.

The Company continuously improves its information security system, implements modern organizational and technical information security measures, develops a corporate culture of responsible information handling, and ensures adherence to best practices in the field of confidentiality.

The Company considers compliance with this Policy to be a prerequisite for ensuring high quality services, protecting the legitimate interests of its clients, and the sustainable development of Korporativ Maslahat Tizimlari LLC.

Official publication

This document is the official version of the Privacy Policy of Korporativ Maslahat Tizimlari LLC and is posted on the Company's official website to ensure open corporate governance and inform clients, business partners, government agencies, and other stakeholders of the current principles for protecting confidential information.

The current version of this document is published on the Company's official website. In the event of discrepancies between different copies of this document, the latest version, approved by order of the director and posted on the official website of Korporativ Maslahat Tizimlari LLC, shall prevail.

© Korporativ Maslahat Tizimlari LLC, 2026. All rights reserved.

Appendix No. 1

List of confidential information

The Company's confidential information includes, but is not limited to:

- constituent and internal regulatory documents;
- personal data of employees;
- personal data of clients;
- personal data of representatives of counterparties;
- commercial secret of the Company;
- commercial secrets of clients;
- contracts and draft contracts;
- confidentiality agreements (NDAs);
- commercial proposals;
- business plans;
- feasibility studies;
- financial models;
- investment projects;
- investment presentations;
- assessment results;
- evaluation reports;
- working materials of appraisers;
- analytical materials;
- results of financial analysis;
- design documentation;
- technical documentation;
- financial statements;
- tax information;
- banking documents;
- information on the cost of services;
- internal regulations;
- internal methods;
- customer databases;
- partner databases;
- corporate correspondence;
- official correspondence;
- meeting minutes;
- information about information systems;
- user credentials;
- access passwords;
- data backups;
- other information recognized by the Company as confidential.

Appendix No. 2

Basic measures to protect confidential information

The company ensures information security through:

- delimitation of access rights;
- user identification;
- using strong passwords;
- backup of information;
- application of antivirus protection;
- corporate network protection;
- use of secure means of communication;
- access control to premises;
- storing documents in secure locations;
- destruction of documents in accordance with the established procedure;
- conducting employee training;
- internal audits of compliance with the confidentiality regime;
- continuous improvement of the information security system.

Appendix No. 3

Registration sheet of changes to the Privacy Policy of Korporativ Maslahat Tizimlari LLC

Version	Approval date	Reason (order number)	Brief description of changes	Responsible person
1.0	July 14, 2026	Order No. 8	Original version	Director