Risk Management Policy

For business partners

HT SOLUTIONS

CONTENTS

Foreword

High-Tech Solutions (hereinafter referred to as "HT Solutions" or "Company") LLC is a company with 12 years of experience that provides informational technology services. It has implemented numerous successful projects and indubitably is one of the strongest actors in the respective field.

In February 2021, some major changes occurred within the ownership and management of the company. In particular, the acquisition of all the shares was executed by one shareholder, and a new shareholder was introduced to the company (who concurrently, became the director of HT Solutions). Under the new management, significant and progressive developments ensued. All of the alterations implemented strive to improve the overall functionality of HT Solutions and ensure superior protection to the assets of the company and its current and prospective business partners.

Organizations of all types and sizes face internal and external factors that may influence the ability to achieve the objectives envisioned. The effect these uncertainties have on purposes of business is known as the "Risk." In recent times, various organizations in different sectors of the economy have shifted their focus towards the management of risk as a core driver to making businesses successful in delivering the principal objectives. Considering that the challenging landscape in the region and the onset of obstacles caused by the ongoing pandemic may trigger the risk of exposure to different types of losses, necessary precautions must be adopted.

HT Solutions reflects the best international practice and recognizes that navigating through this complexity of multiple uncertainties is an intrinsic part of proper management practice. As the latter plays an essential role in achieving business goals and maximizes the safety of the conducted activities, the company intends to align its governance, strategy, processes, people, and corporate culture to risk management procedures.

Consequently, to prevent the potential threats and ensure HT Solutions' further growth and development, it is of the essence to implement a vigilant and formalized organizational risk framework. Thus, this document aims to authorize a risk management policy and reflect the company's principal priorities to identify, manage, mitigate and prevent feasible risks. Moreover, it sets a strategic foundation and organizational arrangement to continually improve the risk management approach in the future.

To provide holistic, integrated, structured, and disciplined prevention of the prospective threats posed, an assessment shall be conducted in a multidisciplinary approach. Specifically, the incorporated system encompasses several elements that together form an effective and efficient control, while enabling the company to swiftly respond to a variety of risks.

Nino Gvazava
Director at High-Tech Solutions

Policy Statement

HT Solutions is committed to ensuring that business excellence is an integral part of the planning, resourcing, and delivery of all services in the IT industry. This policy outlines a procedure for the relationship with business partners and clients, including means of communication and personal data protection, risk management in conjunction with carrying out due diligence and monitoring measures by our compliance officer, reporting violations and suspicious activity, responding to complaints, requests for service and questions that come to the HT Solutions through a client visit, call, letter or email. The purpose of this policy is to establish uniform standards and procedures for responding to client feedback, thus making sure those responses are timely.

Doing what we like and what we are best at, assisting our Clients to achieve business objectives through the use of cutting-edge Information Technology to get a quick return on investment.

It is in our utmost interests:

- to guarantee product safety and full compliance by respecting our policies, principles, and standards with full transparency.
- to strive for zero shortcomings and no waste by constantly looking for opportunities to apply our continuous improvement approach to deliver competitive advantage.

To ensure effective and efficient operations of the company and provide the best possible work environment, the company expects business partners and clients to adhere to the standards outlined in this policy.

Scope and Applicability

This policy, associated procedures, and its attachments apply globally to the business partners, subcontractors, providers/vendors, consultants, volunteers, governmental agencies management, employees, contract clients of all entities and third parties irrespective of citizenship, domicile, or location. Where HT Solutions participates in existing joint ventures as a non-controlling shareholder, the other shareholder(s) shall be made specifically aware of the significance of this policy and shall be encouraged to a similar standard to the joint venture. The Policy applies regardless of the length of time since the conducted activity occurred.

Above stated natural or legal persons must abide by all applicable laws, including the local laws in every country in which the company is doing business (for instance, state, regional, federal, provincial laws, etc).

Definitions

Compliance Officer (CO) - a person who is responsible for designing, implementing, and monitoring risk management policy. The CO oversees and manages compliance issues within the company, evaluates and analysis trigger incidents posed by the current and prospective business partners creates risk register and database, issues annual reports on questionnaire answers received, provides a detailed overview of the potential outcome of trigger incidents, and presents recommendations.

Due Diligence Questionnaire - specially created questionnaire that shall be sent to each prospective business partner and client, which shall be used in the evaluation of potential risks posed by the partners mentioned (Annex I).

Personal Data - any information relating to an identified or identifiable natural person **("Data Subject")** who can be identified, directly or indirectly, in particular by an identification number or by any physical, physiological, psychological, economic, cultural or social features specific to this person.

Risk - may be defined as circumstances events, or conditions that may occur, and whose occurrence, can prevent, hinder, fail to further, or otherwise obstruct the company in achieving its objectives. Risk can cause financial disadvantage, for instance, loss of assets or funds or additional costs. It has the potential to incur damage, quantifiable and/or reputational, loss of value, and/or opportunity to promote the company's activities or operations.

Risk Categories - risk categories that may occur throughout the company's business operations (Annex II).

Risk Database - records activities and/or events that present a threat to the company's standards and objectives, the risk classification specificities (the particular degree of the threat posed), and actions being taken to manage, mitigate and prevent the respective threats. It is perceived as a working document that is updated to reflect the current circumstances (Annex III).

Risk Reporting Form – a special form that is used by the CO to record the risks encountered throughout the business activities (Annex III).

Risk Management - identification, assessment, and prioritization of risks followed by a coordinated strategy to minimize, monitor, and control the likelihood and/or impact of adverse uncertain conditions.

Risk Source - the origin/source of the trigger incident.

Trigger Incident - circumstance, event or condition that may trigger the risk.

Personal Data Protection

We use the information at our disposal to verify activities, to prevent dangerous or harmful behavior, to detect and prevent undesirable content and all other negative experiences, to preserve the integrity and improve the safety and security of our Services. HT Solutions takes the security and privacy of your data seriously. We need to gather and use information or "data" about you as part of legitimate business purposes to manage our relationship with you in a manner you deem appropriate.

We intend to comply with our legal obligations under the Law of Georgia on Personal Data Protection[1] and the standards stipulated in EU's General Data Protection Regulation (GDPR)[2] in respect of data privacy and security.

a. Data Protection Principles

Personal data must be processed in a transparent manner in relation to the data subject and in accordance with Data Protection Principles: It shall:

- be processed fairly, lawfully, and transparently;
- be collected and processed only for specified, explicit, and legitimate purposes;
- be adequate, relevant, and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- be processed securely.

b. Legitimate Business Purposes

Personal Data shall be collected, used, stored, or otherwise Processed if necessary, within the framework of responsible, efficient, and effective business management, specifically for the following activities:

- Performing agreements assessing and accepting Business Partners, entering into and execution agreements with Business Partners and Clients as well as carrying out payment transfers and other financial transactions and recording and financially settling delivered services, products and communication with Individuals and other parties involved in contracts and responding to requests for (further) information from Clients, Business Partners, dispute resolution and litigation.
- Relationship management and marketing for commercial activities including processing necessary for the development and improvement of HT Solutions products and/or services, account management, client service, and the performance of (targeted) marketing activities to establish a relationship with a Client and/or maintaining as well as extending a relationship

[1] The Law of Georgia on Personal Data Protection: <https://matsne.gov.ge/en/document/view/1561437?publication=9>

[2] General Data Protection Regulation (GDPR): <https://gdpr-info.eu>

with a Client or Business Partner and for performing analyses concerning personal data for statistical purposes.

- Business process execution, internal management, and management reporting addressing activities such as managing finance, implementing business controls, and Processing Personal Data for management reporting and analysis.
- Safety and security this purpose address activities such as those involving safety and health, the protection of Client or Business Partner assets, and the authentication of Client, or Business Partner status and access rights.
- Compliance with legal obligations, which concerns the Processing of Personal Data as necessary for compliance with laws and regulations.

c. Specific purposes for Processing Sensitive Data

HT Solutions shall Process Sensitive Data only to the extent necessary to serve the applicable legitimate purposes and only to the extent that this is needed for the relevant Business Purpose. The following categories of Sensitive Data may be collected, used, or otherwise Processed for one (or more) of the purposes specified below:

- HT Solutions may process photos and video images of Individuals for inclusion in Client, or Business Partner directories and to comply with legal obligations (e.g. due to diligence screenings).
- Physical or mental health data; for assessing and accepting Clients, entering into and executing an agreement with a Client, and for carrying out payment transfers and other financial transactions.
- Criminal data (including data relating to criminal behavior, criminal records, or proceedings regarding criminal or unlawful behavior); for protecting the interests of HT Solutions with respect to criminal offenses that have been or, given the relevant circumstances are suspected to be, committed against HT Solutions.

d. Controlling your personal information

HT Solutions is committed to protecting our Business Partners' personal data. It will not sell, distribute or lease your personal information to third parties unless we have your permission or are required by law to do so.

Any person to whom the policy applies has the right to information about what personal data we process, how and on what basis as set out in this policy. Right to access his own personal data by way of a subject access request. If you believe that any information we are holding on you is incorrect or incomplete, please contact us. We will promptly correct any information found to be incorrect.

Compliance Officer

Compliance Officer (CO) plays a pivotal role in the oversight and implementation of risk management policy. The CO for HT Solutions shall be "J&T Consulting" LLC, which shall design, implement, monitor, and amend the following risk management policy in line with the company's principal objectives.

The primary responsibilities of Compliance Officer include:

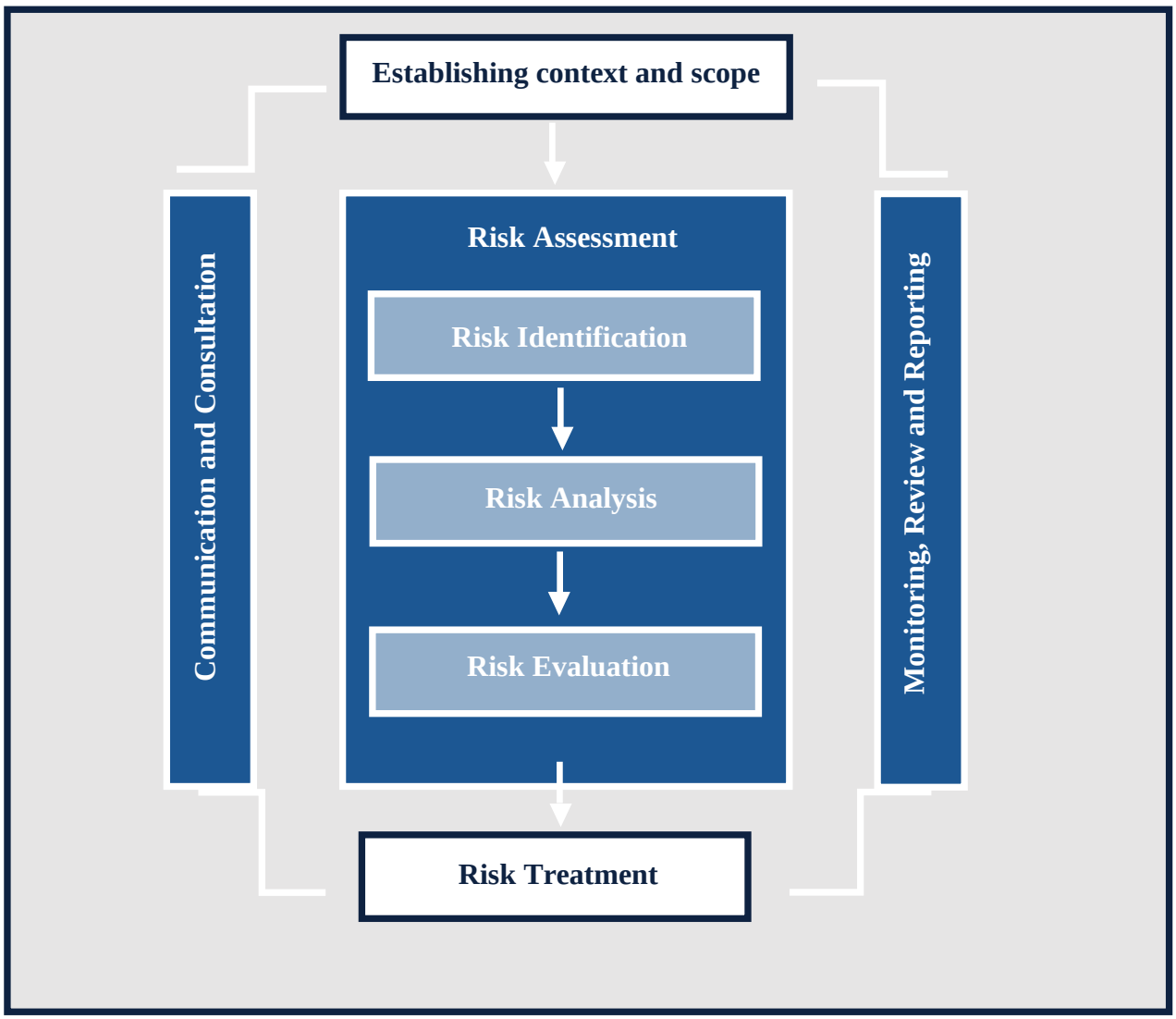
- Developing the risk management policy and ensuring that it is effective, relevant, and corresponds to the company's objectives;
- Implementing, monitoring, and amending the presented policy;
- Identification of new risks;
- Reviewing and discussing significant risk issues and ensuring horizontal collaboration in the development of the risk treatment strategies;
- Rating the risks according to the established criteria. Such categorization shall be made by taking into consideration the potential impact that the risk being realized shall have and the likelihood of it being materialized. The CO is authorized to use his experience and the best judgment to calculate the rating of each individual risk;
- Reporting each and every trigger incident and detailed information on the new risks posed to the director of the company;
- Ensuring implementation of risk treatment options;
- Recording the new risks in the Risk Database regularly;
- Performing the reviews of Risk Database annually;
- Attending meetings with current and/or prospective business partners where necessary;

The CO is fully authorized to conduct research independently or through respective third parties on current and/or prospective partners, which constitute a potential risk source and may cause the trigger incident and/or the risk itself. The conducted research shall cover the relevant issues pertaining to the following policy and information gained shall be used to ensure the best possible protection of HT Solutions and its current and/or prospective business partners. The CO obtains and holds personal data where necessary and only processes and uses the data for a specific and legitimate purpose. Personal data that is acquired through research shall be kept securely and confidentially.

Risk Management Framework

a. The brief summary of procedure

The risk management framework involves systematic and strategic application of the established policy and practices. It is duly realized by the Compliance Officer, which designs, monitors, and observes the whole process and reports all and every suspicious activity through special reporting forms. The brief summary of the procedure is depicted as follows and covers establishing the context and scope, risk assessment process (which includes risk identification, risk analysis, risk evaluation), monitoring, review and reporting, communication, and consultation.



(Figure 1, Source International Standard ISO 31 000, 2018)

b. The structure of framework

6. Establishing the context and scope

Establishing the context and scope of the risks posed is an integral part of the formalized risk management framework that ultimately strives to optimize foresight and risk-informed decisions across all levels of the company. The presented component of the policy provides a groundwork for the procedure and enables the CO to prioritize and label the risks encountered.

To establish the nature of the threats confronted, it is necessary to understand the external and internal context. **External context** covers but is not limited to cultural, environmental, political, social, technological, financial, legal, and economic factors. Furthermore, under the umbrella of external context are included the relationships and perceptions of the third parties and current and/or prospective business partners.

Internal context combines the company's procedures, structures, strategy, and culture. Internal context is correlated to everything that influences or has the potential to influence the risk management framework. Therefore, it includes but is not limited to the company's governance, roles, and accountabilities, standards, objectives, policies, resources available (in terms of people, monetary assets, time, and technological assets), relationships with the shareholders, and managers, etc.

7. Risk Assessment

The risk assessment incorporates risk identification, analysis, and evaluation. This specific stage of the risk management framework aims to address particular risks that arise throughout the company's business operations. After conducting the respective risk assessment, the CO fills out the risk database, in which threats posed are categorized and labeled with detailed relevant recommendations and subsequent action plans.

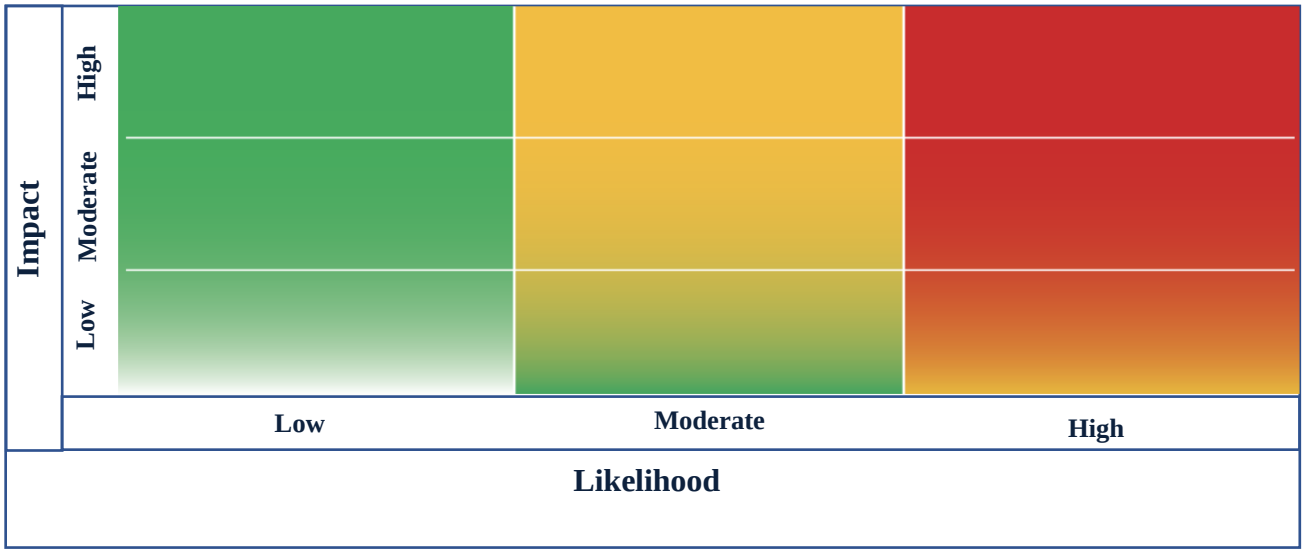
i. Risk Identification

An essential factor of assessing the risk is the identification of its nature (context and scope), source, and type of impact that the risk might have on a company's business operation. Risk inherently is an effect of uncertainty, which if realized has the potential to prevent, hinder, fail to further, or otherwise obstruct the company in achieving its objectives. Risk can cause financial disadvantage, for instance, loss of assets or funds or additional costs. It has the potential to incur damage, quantifiable and/or reputational, loss of value, and/or opportunity to promote the company's activities or operations. The stage of risk identification is focused on future events and on the possible impacts that certain risks pose to the normal functioning of the company. Therefore, to properly conduct the risk identification, the context, scope, knowledge of chronological preconditions, and foresight thinking are necessary.

Potential risks that may be encountered throughout HT Solutions' business activities are detailed in Annex II. All of them shall be considered in the risk assessment procedure. After identification of each risk, its category, source, possible impact, and probabilities of it occurring, the CO records relevant information in the risk database with a respective recommendation

ii. Risk Analysis

Risk analysis requires the assessment of the likelihood of the risk being realized and its potential impact on the objectives of the company. The following analysis shall utilize a risk rating matrix that consists of likelihood and impact consists of three different levels (High, Moderate, and Low) and is depicted below. It shall be respectively considered during each and every risk assessment procedure. The conducted review shall clarify the extent and degree of the threat encountered at various sectors of the performed activities. In cases where it is objectively impossible to estimate the approximate likelihood and/or impact of the threats encountered, the worst-case scenario shall be utilized to calculate the probable volume and scope of the potential risk. This precautionary approach shall ensure the most effective risk management and the optimal protection of the business operations. Furthermore, if more information is available during the assessment process, calculations and recommendations shall be updated and adjusted accordingly.



(*Figure 2, Risk Rating Scale*)

iii. Risk Evaluation

The risk evaluation strategy aims to determine the hazardous level of the threats posed based on the risk analysis. After such estimation the risks shall be categorized as follows:

Critical	Constitutes a **high risk** and requires immediate and priority response from the management.
Considerable	Constitutes a **moderate risk.** While immediate intervention is not required, constant monitoring is necessitated.
Acceptable	Constitutes a **low risk** and does not require any intervention or monitoring. The identified risks shall be reviewed annually to record any and all changes in status.

(*Figure 3, Risk Evaluation Scale*)

The risk that constitutes a potential for fraud, misuse of funds, or similar violation that may harm the company and/or its current and/or prospective clients, are automatically labeled as critical and require immediate, direct, and swift attention from the management.

8. Monitoring and reporting

HT Solutions and its management are committed to promoting and maintaining the highest ethical standards in all our business, and ensuring that where problems are identified they are resolved quickly. We wish to identify situations where things have gone wrong, or wrongdoing has occurred to remedy these situations and, therefore, we have a positive commitment and open approach to reporting.

We aspire to create an atmosphere where:

- every person feels encouraged and comfortable about raising concerns with us in the first instance;
- every person is assured that if he reports wrongdoing to us, he feels supported and that he doesn't feel that raising such matters will adversely affect him.
- any such reporting will be treated as confidential to the extent permitted by law

What should you report?

All activities that may constitute:

- Accounting irregularities;
- Conflicts of interest or other unethical business conduct;
- Theft and fraud;
- Violation of laws, rules, or regulations;
- Violation of professional standards or internal policies
- Endangering the environment;
- Any other matter of concern that business partner or other third party brings forward that is believed to be inappropriate and may adversely affect the companies;

All business partners and clients must adhere to HT Solutions' commitment to conduct its business and affairs lawfully and ethically. All business partners and clients are encouraged to raise any queries with the Compliance Officer. Moreover, individual who becomes aware of any instance where HT Solutions receives a solicitation to engage in any activity prohibited by this Policy, or who becomes aware of any information suggesting that a violation of this Policy has occurred or is about to occur is required to report it to the Compliance Officer. HT solutions aim to encourage openness and will support anyone who raises genuine concerns in good faith under this Policy, even if they turn out to be mistaken. HT Solutions prohibits retaliatory action against any person who raises a concern in good faith.

A person who applies this policy shall report immediately any suspected or actual violations of this policy or relevant laws. Complaints should be made in accordance with this policy. Suspected violations will be reviewed and investigated with care and discretion. Any such reporting will be treated as confidential to the extent permitted by law.

The severity of the complaint and the level within the company at which the potential violation occurs will dictate whether the complaint is elevated to CO for investigation and relevant action. All formal complaints and their resolution will be reported annually to HT Solutions' management.

Any person who violates this policy may be subject to termination of all relationships with HT Solutions. Violations of this policy may also result in civil and criminal penalties for such individuals in accordance with applicable law.

9. Risk Treatment

Each and every identified risk shall be treated with the measure most suitable for its category and level. The CO shall indicate respective recommendations on the preferable option in the risk report form and database. The risk that constitutes a potential for corruption, fraud, misuse of funds, or similar violation that may harm the company and/or its current and/or prospective clients, shall be addressed through termination and shall be approached immediately, directly, and swiftly by the management.

Terminate	Eliminate the trigger incident that caused identified risk immediately or as soon as possible.
Mitigate	Reduce the likelihood and/or impact below the threshold of acceptability.
Tolerate	Tolerate the risk level. Annual assessments require to record any and all changes in the status.

(*Figure 4, Risk Treatment Options*)

10. Communication and consultation

Communication and consultation shall be conducted during all stages of the risk management process and are initialized by the CO. It shall address issues correlating to the risk itself, its impact, the likelihood of it being materialized, and measures being taken to treat it. Communication shall be conducted on two levels: externally and internally. External communication constitutes respective contact with current and/or prospective business partners, their employees, and other relevant third parties. Such communication shall be conducted in writing only to ensure the proper recording of all of the correspondence exchanged. Internal communication and consultation cover the constant and pertinent contact with the company’s management, shareholders, and employees. The process shall be conducted either in oral (including, by special meetings) or in writing format. However, wherever possible preference shall be given to communication in written form.

Feedback and Questions about the Policy

Current and/or prospective business partners and other relevant third parties may provide feedback on issues pertaining to the following policy. The feedback can be presented either formally or informally, either in oral or written form. However, to properly record the received comments, it is recommended to provide them formally, in written format to the CEO of the HT Solutions

The questions that arise regarding the following policy, in particular, its implementation, risk management processes (including information on risk treatment measures that are to be implemented throughout specific risk encountered), and all other relevant inquiries shall be addressed promptly to the CEO of the company.

Contact

For further information, please directly contact or send an email to the CEO of the HT Solutions - Nino Gvazava. E-mail - ngvazava@hts.ge

Annex I: Due Diligence Questionnaire

Introduction

In line with High-Tech Solutions LLC's values depicted in Risk Management Policy and in order to safeguard the company's business integrity, High-Tech Solutions is committed to and accountable for upholding the highest ethical standards. The established and formalized framework aims to avoid any involvement in fraud, corruption, coercion, money laundering, human trafficking, or terrorism, as well as any behavior, which aims at the unfair competition or gives rise to respective suspicions.

It is noteworthy to outline that High-Tech Solutions has a policy of zero-tolerance policy against all forms of corruption and coercion and therefore undertakes a responsibility to work with business partners that share its ethical approach and adhere to these standards.

Please complete the following questionnaire completely and truthfully to the best of your knowledge.

Instructions

Please provide answers to all questions. Some answers may simply consist of "Yes" or "No". Please do not omit any answer. If the question is not applicable, write "N/A" in the space provided. If the space provided for a question is insufficient, you may attach additional rows/pages.

Please note that answering 'No' to a question does not necessarily mean that cooperation between our companies will not be possible. It is of the essence that the questions are answered truthfully and without any omissions on your part.

If you have any questions regarding the instructions, please direct your inquiries to the CEO of the company.

Data Protection Statement

All data is processed in accordance with the Law of Georgia on Personal Data Protection[1] and in line with the standards set by the EU's General Data Protection Regulation (GDPR)[2]. High-Tech Solutions obtains and holds personal data where necessary and only processes and uses the data for a specific and legitimate purpose. Please note that personal data is kept securely and confidentially. If you have any questions regarding personal data protection, please direct your inquiries to the CEO of the company.

1. GENERAL INFORMATION

[1] The Law of Georgia on Personal Data Protection: <https://matsne.gov.ge/en/document/view/1561437?publication=9>
[2] General Data Protection Regulation (GDPR): <https://gdpr-info.eu>

Name of the company/entity	
Registeration number	
Factual address	
Date of registration	
Telephone number	
Website of the organization/company	
Names of shareholder(s)	
Identification number(s) of shareholder(s)	
Names of director(s)	
Identification numbers of director(s)	

2. BUSINESS AND FINANCIAL INFORMATION

Is any of your employee relative of government officials who have influence over your area of business?

☐ Yes ☐ No

If yes, please provide a list of who is holding which position and since when. Please indicate whether these positions are appointed or elected positions.

…

To the best of your knowledge, is any key employee or senior management member of your entity/company, related (by blood, marriage, current or past business association, or otherwise) to a public official/member of a government entity?

☐ Yes ☐ No

If yes, please describe the relationship between the person and the public official/member of the government entity

...

To the best of your knowledge, is any shareholder or partner in your entity/company, or any subsidiaries of the shareholder(s) or partner(s), owned in any part by a public official or a person related in any way to a public official/member of a government entity

☐ Yes ☐ No

If yes, please provide the name(s) of the respective public official(s)/member(s) of a government entity and indicate the total percentage of their ownership interest.

...

PLEASE NOTE:
A "public official" may be:
- a person holding legislative, administrative, military, or judicial office for any country;
- a person exercising a public function in a government or public agency of any country;
- an employee of a state-owned or controlled company;
- an official or agent of a public international organisation (e.g. UN, World Bank, International Monetary Fund and World Trade Organisation;)
- an official or agent of a political party.

A "member of a government entity" include:
- an honorary government official, member of board, official or honorary of a state-owned or state-controlled company;
- a member of a royal or ruling family.

3. ETHICAL CONDUCT

Has your entity/company or have any of its directors, 20%+ shareholders of your entity/company ever been investigated for, charged with, convicted or otherwise implicated in criminal offence, corrupt, unethical or unlawful conduct?

☐ Yes ☐ No

Has your entity/company or have any of its directors, 20%+ shareholders of your entity/company convicted for:

Fraud:	☐ Yes ☐ No
Bribery:	☐ Yes ☐ No
Corruption:	☐ Yes ☐ No
Coercion:	☐ Yes ☐ No
Money Laundering:	☐ Yes ☐ No
Human Rights Violations:	☐ Yes ☐ No
Modern Slavery:	☐ Yes ☐ No
Human trafficking:	☐ Yes ☐ No
Non-payment of taxes:	☐ Yes ☐ No

Has your entity/company or have any of its directors, 20%+ shareholders of your entity/company entered into any deferred prosecution agreement or settlement, resolution agreement or similar arrangement or voluntarily disclosed with a law enforcement, prosecutorial or regulatory agency or body relating to investigations or allegations of criminal, corrupt, unethical or unlawful conduct?

☐ Yes ☐ No

If you have answered 'Yes' to any questions from the above section please give an explanatory statement.

…

4. GOVERNANCE

Is the entity/company fully compliant with the laws, regulations, guidelines, government prevailing instructions?

☐ Yes ☐ No

Are controls in place concerning the preparation and approval of transactions, ensuring that all transactions are correctly made and adequately explained?

☐ Yes ☐ No

Are there any response measures in place to respond adequately to a critical incident?

☐ Yes ☐ No

Is the monitoring and evaluation policy framework in place?

☐ Yes ☐ No

If yes, please describe how frequent is the reporting on monitoring (monthly, quarterly) taking place? Who are involved in discussing/following up the monitoring reports and variations, if any?

…

Are internationally accepted accounting standards followed?

☐ Yes ☐ No

If yes, please specify the standards.

…

Has the entity/company developed policies and procedures for the recruitment of employees?

☐ Yes ☐ No

If yes, please describe how are the employees recruited.

…

Is there any consent document signed by employees regarding security policy?

☐ Yes ☐ No

Is there a system of periodic performance evaluation for all staff?

☐ Yes ☐ No

Do you collect, store, or transmit personally identifiable information (PII)?

☐ Yes ☐ No

Are you prepared to agree to anti-bribery & anti-corruption clauses in the agreement with HT Solutions?

☐ Yes ☐ No

CERTIFICATION

The signatory who is duly authorised and has full legal capacity to complete this questionnaire on behalf of the entity/company, certifies and affirms as to the matters set forth in this questionnaire, as follows:

- To the best of my knowledge, all information set forth in this response is truthful, accurate and complete
- I have read and understood the Data Protection statement above and expressly consent to the collections, use, processing, storage and transfer of data, including the data of my organisation/company, my personally identifiable information and that of other persons that I identify in the questionnaire, in the manner and for the purposes described in the above Data Protection Statements.

Do you certify and affirm the above statements?

☐ Yes

☐ No

Name:	Position:	Signature:	Date:

Attachments

Please attach the following documents if available:

☐ Code of Conduct

☐ Anti-Corruption Policy

Annex II: Risk Categories*

Operational Risks	○ Management ○ Communication ○ Capacity development ○ Opportunity management ○	○ Governance ○ Project implementation ○ Accountability ○ Internal control	○ Human Resources ○ Quality and evaluation ○ Competition ○ Corporate social responsibility
Financial Risks**	○ Corruption ○ Fraud ○ Misuse of funds ○ Interest rates ○ Business partners ○	○ Cost escalation ○ Fraud ○ Interest rates ○ Credit rating	○ Profitability
Regulatory Risks	○ Changes in legislation ○ Changes in international/foreign registration that is relevant to company's activities ○ Deviation from HT Solutions internal rules and regulations ○ Regulatory compliance		
Political Risks	○ Political turmoil ○ Social unrest		
Safety and Security Risks	○ Civil unrest ○ Armed conflict ○ Natural hazards ○ Terrorism	○ Crime	
Environmental Risks	○ Sudden catastrophes ○ Pandemic ○ Natural disasters ○ Climate change		

* The table shall be amended and updated as necessary to reflect each and every risk encountered.

** HT Solutions takes a zero-tolerance approach to bribery and corruption and is committed to upholding all laws relevant to countering bribery and corruption in each of the jurisdictions in which it operates. HT Solutions, its business partners and associated persons will be bound by the most stringent requirements of these laws in respect of its conduct in all jurisdictions they operate.

Annex III: Risk Reporting Forms

Risk Reporting Form		
Risk Identification		
Risk Description		
Risk Source		
Trigger Event		
Risk Category		
Risk Rating		
Proposed Risk Treatment Plan		
Status of Implementation of Risk Management Option		
Compliance Officer	**<Name>**	
/Signature/	**/Date/**	
Risk detection date:	**/Date/**	
Person who detected the risk:	**/Name/**	**/Position/**

Risk Database Form							
Risk Identification							
Risk Description							
Person who detected the risk							
Detection Date							
Risk Source							
Trigger Event							
Risk Category							
Risk Rating							
Proposed Risk Treatment Plan							
Status of Implementation of Risk Management Option							
Additional Comments							
Name of CO							
Signature of CO							