

Employment Risk Management Policy



HT SOLUTIONS



CONTENTS

Foreword	3
Policy statement	4
Scope and applicability	4
Definitions	5
Personal data protection	6
a. Data protection principles	6
b. Legitimate business purposes	6
c. Specific purposes for processing sensitive data	7
d. Controlling your personal information	8
Anti-Bribery and Corruption	8
a. Unacceptable Gifts, Entertainment and Hospitality	9
b. Accounting and Payment Practices	9
Conflict of Interest	9
Compliance Officer	10
Risk Management Framework	11
a. The brief summary of procedure	11
b. The structure of the framework	12
1. Establishing the context and scope	12
2. Risk assessment	12
i. Risk identification	12
ii. Risk analysis	12
iii. Risk evaluation	13
3. Monitoring and reporting	13
4. Risk treatment	14
5. Communication and consultation	15
Policy Revision	15
Feedback and questions about the policy	15
Contact	15
Annex I	16
Annex II	20
Annex III	21

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 a number of 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 the business 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 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 an employment 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, the assessment shall be conducted in a multidisciplinary approach. Specifically, the incorporated system encompasses a number of 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

High-tech Solutions LLC is committed to express our conviction that our company's success depends on the performance of dedicated employees; HT Solutions strives to be a company that enjoys the pride of its employees by offering an innovative workplace with the expectation that everybody contributes to the success of the company. This policy outlines a procedure for the employment relationship, 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 High-Tech Solutions through the visit, call, letter or email. In accordance with the Labour Code of Georgia, it is the purpose of this policy to effectuate these principles and define our expectations of our current and future employees.

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 recognize the connection between service quality and the management of workforce issues.
- to secure compliance with our duty to provide works that demonstrate the best value, whilst ensuring that our policies support diversity and do not lead to unfair discrimination or social exclusion.

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

Scope and Applicability

This policy, associated procedures, and its attachments apply to all employees and job candidates of the company 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

Definitions

Bribery - anything of value given in an attempt to affect a person's actions or decisions in order to gain or retain a business advantage.

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.

Corruption - the misuse of power to influence an outcome or to encourage a form of behavior which may not have occurred otherwise.

Due Diligence Questionnaire - specially created questionnaire that shall be sent to each prospective employee, which shall be used in the evaluation of potential risks posed by the partners mentioned (AnnexI).

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 in order 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 Protection¹ and under the standards stipulated in EU's General Data Protection Regulation (GDPR)²³ in respect of data privacy and security.

a. Data Protection Principles

Personal data must be processed transparently 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:

- Entering into and executing agreements with Employees, as well as carrying out payment transfers.
- Relationship management for team-building activities including processing necessary for performing analyses with respect to 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 addresses activities such as those involving safety and health, the protection of Employees' assets, and the authentication of Employees' status and access rights.
- Compliance with legal obligations, which addresses the Processing of Personal Data as necessary for compliance with laws and regulations.

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>>

³ Although the GDPR does not apply directly in Georgia, due to the DCFTA, we consider it expedient to take into consideration the standards set by the latter, in the course of our business performance.

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 employees and to comply with legal obligations (e.g. due diligence screenings).
- Physical or mental health data; for assessing and accepting employees, entering into and executing an agreement with an employee and for carrying out payment transfers, etc
- 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 Employees' 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.

Anti-Bribery and Corruption

The policy requires compliance with all applicable laws and regulations on bribery and corruption, including, but not limited to, Georgian Law on Conflict of Interest and Corruption¹ and other applicable national anti-bribery laws. Any attempt to pay, authorize, or promise a bribe, kickback, or any other form of corrupt payment in any amount is strictly prohibited. The prohibition covers cash payments, benefits and favours. In certain circumstances, it also covers otherwise legitimate business expenditures such as gifts, entertainment, travel, donations, sponsorships or training.

In particular, this policy prohibits:

- directly or indirectly the offer, promise or payment of bribes;
- assisting in, abetting or facilitating any such conduct (active bribery);
- the request, solicitation, agreement to accept or receipt of bribes (passive bribery).

¹ Georgian Law on Conflict of Interest and Corruption <https://matsne.gov.ge/ka/document/view/33550>

No HT Solutions management or employees intermediary shall pay, authorize, or promise to give anything of value in order to improperly influence any person or entity to act favorably towards Company. It does not matter if the intended recipient of the bribe works in the public or private sector. It does not matter if the intended recipient conducts business in a country where paying bribes is a common practice.

This policy does not prohibit reasonable and proportionate gifts, entertainment and hospitality being give that are legal and directly related to the promotion or demonstration of the HT Solutions's services or the performance of a particular contract with a government or state-owned entity and received from third parties. Moreover, Employees should consult with their manager or Compliance officer for further guidance on giving or accepting gifts or forms of entertainment or hospitality in most circumstances, but they must consult with their manager or Compliance officer to providing any gifts or entertainment to any Public Official. Also, shall take into consideration that the received and / or issued benefits:

- is aimed at nothing more than general relationship building;
- could not be perceived as an attempt to gain influence in respect of any particular matter;
- complies with HT Solution's Code of Conduct, Internal Policy documents and applicable laws

a. Unacceptable Gifts, Entertainment and Hospitality

Gifts, entertainment and hospitality are commonly offered as gestures of gratitude or tokens of appreciation. HT Solutions allows these tokens and gestures when they are reasonable, proportional, made in good faith and in compliance with the Company's Code of Conduct and and this Policy.

However, it is not acceptable for Employees (or anyone acting on Employees behalf) to:

- Give, promise to give, or offer, a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given;
- Give, promise to give, or offer, a payment, gift or hospitality to a government official, agent or expedite a routine procedure;
- Accept any benefit from a third party that you know or suspect is offered with the expectation that it will obtain a business advantage for them.
- Disproportionate entertainment or hospitality compared to the value of the business relationship .

b. Accounting and Payment Practices

In order to prevent the possibility of bribes and kickbacks being paid or accepted, all transactions must be recorded accurately and with sufficient detail to identify the actual purpose for each payment. Secret, unrecorded or unreported transactions are prohibited

Any employee who witnesses a breach of this principle is obliged to promptly contact Compliance Officer. Any employee who is in doubt, suspects that this policy has been breached or has concerns about past or proposed actions by anyone in the HT Solutions, or any third party working with the Company, is encouraged to contact the Compliance Officer.

Conflict of Interest

HT Solutions employees are obligated to avoid and disclose ethical, legal, financial, or other conflicts of interest involving the company, and remove themselves from a position of decision-making authority with respect to any conflict situation involving the HT Solutions.

Generally, employees are in a conflict of interest when they get, or hope to get, some personal gain by using: their position or influence, company information or material or facilities. In addition a conflict of interest may occur if an interest or activity influences or appears to influence the ability of an individual to exercise objectivity or impairs the individual's ability to perform his or her employment responsibilities in the best interests of the Company. An individual is considered to have a potential conflict of interest when:

- He or she or any member of his or her family may receive a financial or other significant benefit as a result of the individual's position at the company;
- The individual has the opportunity to influence the company's granting, business, administrative, or other material decisions in a manner that leads to personal gain or advantage;
- The individual has an existing or potential financial or other significant interest which impairs or might appear to impair the individual's independence in the discharge of their responsibilities to the Company.

HT Solutions has delegated authority to the Compliance officer to investigate, manage, resolve, and report all Conflicts of Interest. Once a Conflict of Interest is disclosed, in consultation with the Compliance Officer, it will determine the next steps with respect to the Conflict. It may determine that the Conflict of Interest will be managed, reduced, or eliminated. The director of the company, in consultation with the CO and the lawyers, retains final authority to determine appropriate disciplinary measures for failure to comply with the terms of this policy.

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 the 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;

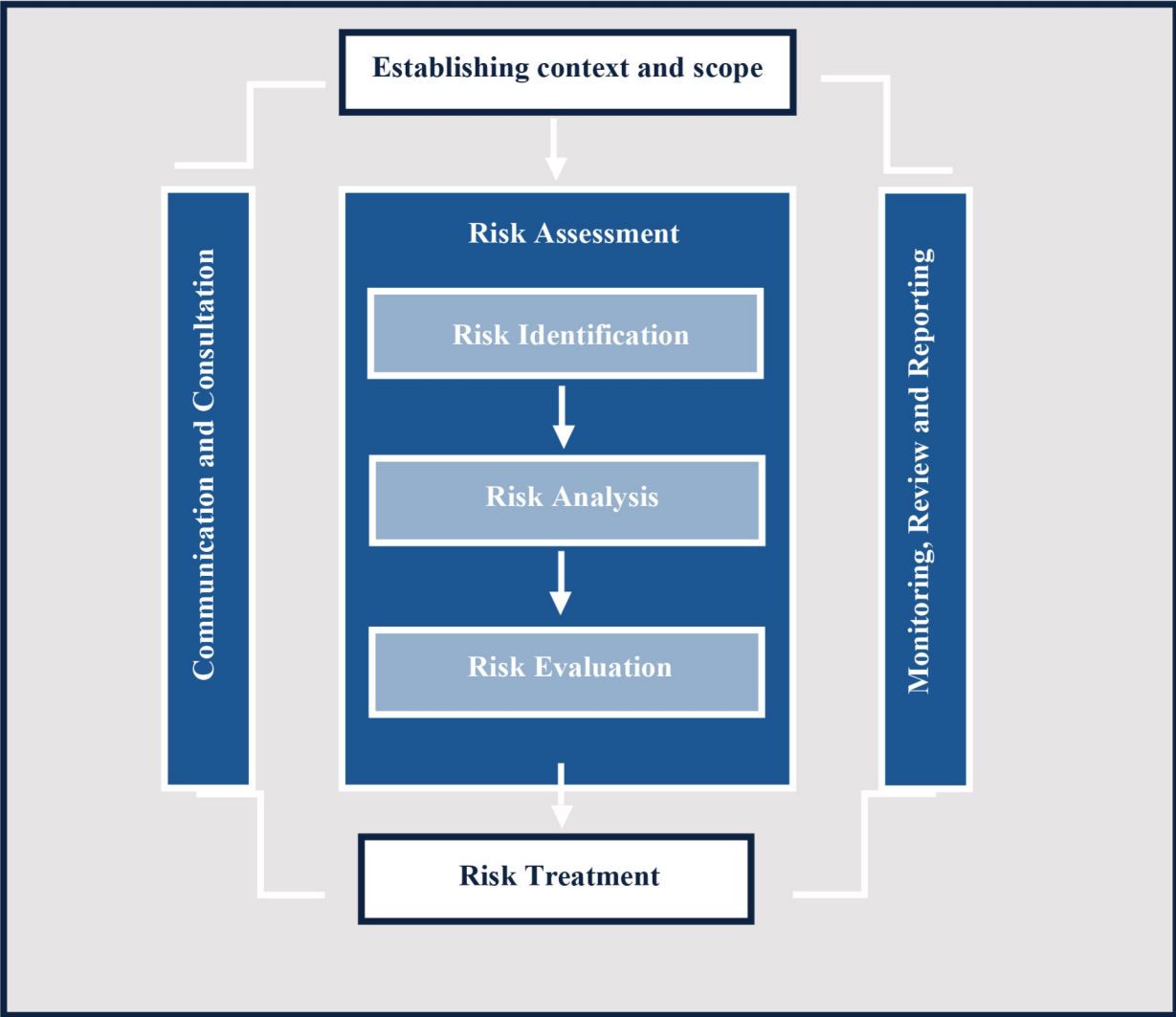
- Reporting each and every trigger incident and detailed information on the new risks posed to the director of the company;
- Attending interviews with job candidates where necessary;
- Ensuring implementation of risk treatment options;
- Recording the new risks in the Risk Database regularly;
- Performing the reviews of Risk Database annually;
- Conducting risk management trainings for staff and management annually;
- Making recommendations, based on the participants feedback in the course of the training;

The CO is fully authorized to conduct research independently or through respective third parties on current and/or potential employees, who 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

e. 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)

f. 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.

Impact	High			
	Moderate			
	Low			
		Low	Moderate	High
Likelihood				

(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 with a view to remedying these situations and, therefore, we have a positive commitment and open approach to reporting.

Our aspiration is 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 employees must adhere to HT Solutions' commitment to conduct its business and affairs in a lawful and ethical manner. All employees 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 the HT Solutions's 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 cause 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. 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.

Questions about the Policy

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 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 Employment 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 shall not necessarily hinder the conclusion of an employment contract. 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 Protection¹ 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 CEO of the company.

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>>

1. GENERAL INFORMATION

Name	
Date of birth	
Physical address	
Telephone number	
Position in the company	

2. GOVERNMENT

Have you ever been employed in any of the governmental bodies that have influence over the company’s area of business?

Yes No

If yes, please detail the position and duration of the employment.

...

Are you 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

...

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

Have you ever been investigated for, charged with, convicted or otherwise implicated in criminal offence, corrupt, unethical or unlawful conduct?

Yes No

Have you ever been convicted for:

Fraud:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Bribery:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Corruption:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Coercion:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Money Laundering:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Human Rights Violations:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Modern Slavery:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Human trafficking:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Non-payment of taxes:	<input type="checkbox"/> Yes <input type="checkbox"/> No

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

...

Are you prepared to adhere to HT Solutions zero tolerance policy on anti-bribery & anti-corruption?

Yes No

CERTIFICATION

The signatory certifies and affirms as to the matters set forth in this questionnaire, as follows:

- 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 my personally identifiable data 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:	Signature:	Date:

Annex II: Risk Categories*

Social Risks	<ul style="list-style-type: none"> ○ Health and safety ○ Labor policy ○ Human rights violations ○ Discriminatory practices 	<ul style="list-style-type: none"> ○ Recruitment and allocation of resources ○ Workplace Violence and Harassment 	
Operational Risks	<ul style="list-style-type: none"> ○ Management ○ Communication ○ Capacity development ○ Human Resources 	<ul style="list-style-type: none"> ○ Project implementation ○ Accountability ○ Internal control ○ Training and development 	<ul style="list-style-type: none"> ○ Performance and productivity ○ Conflict of interest
Financial Risks**	<ul style="list-style-type: none"> ○ Corruption ○ Fraud ○ Misuse of funds ○ Fraud 		
Regulatory Risks	<ul style="list-style-type: none"> ○ Changes in legislation ○ Regulatory compliance 		
Political Risks	<ul style="list-style-type: none"> ○ Political turmoil ○ Social unrest 		
Safety and Security Risks	<ul style="list-style-type: none"> ○ Civil unrest ○ Armed conflict ○ Natural hazards ○ Terrorism 	<ul style="list-style-type: none"> ○ Crime 	
Environmental Risks	<ul style="list-style-type: none"> ○ Sudden catastrophes ○ Pandemic ○ Natural disasters 		

* 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 employees 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							