G TECH INFRASTRUCTURE

G-TECH INFRASTRUCTURE PRIVATE LIMITED, INDIA

RISK MANAGEMENT POLICY

1. INTRODUCTION

G-Tech Infrastructure Private Limited (G-Tech Infrastructure) (the "Company") recognises that risk is an integral part of business in today's dynamic environment. We are committed to identifying, assessing, and managing risk in a proactive and effective manner, ensuring that uncertainty is addressed responsibly to protect value, enhance resilience, and support long-term growth. Risk is understood as the effect of uncertainty on our business activities and projects, where consequences may be either positive or negative. Our focus is on building a strong risk-aware culture that encourages accountability, compliance with laws and governance standards, and informed decision-making at every level.

Our Risk Management Policy provides a structured framework that integrates values, processes, and systems to anticipate challenges, limit potential losses, and harness opportunities for competitive advantage. By embedding risk considerations into strategy and operations, the Company safeguards its reputation, strengthens stakeholder trust, and ensures that risks are managed not as obstacles but as enablers of sustainable success.

2. PURPOSE

The main purpose of Risk Management Policy (herein after referred to as "the Policy") is to ensure:

i. Existing and potential material risks that could impact the achievement of corporate objectives are identified, managed or mitigated.

ii. Techniques to manage risks (avoidance, reduction, retention, etc.) are applied appropriately.

iii. Appropriate controls are in place for controllable, accepted risk areas.

iv. Non-controllable risks are identified, monitored, understood and mitigated, as appropriate.

3. DEFINITIONS

Risk: An event or cause leading to uncertainty in the outcome of business operations; measured in terms of impact and likelihood. Though there are various risks involved in any business operations, various categories of risks have been identified under this Policy. The same are enclosed as Annexure A.

i. **Risk Management**: Coordinated activities aimed to direct and control the organisation with regard to risk. Risk management is not a standalone activity but is an integral part of all organisational processes including strategic planning and all project processes.

ii. **Risk Register:** A Risk Management tool for operational risk assessments. It acts as a central repository for all risks identified by the project or organisation and for each risk, includes information such as risk probability, impact, countermeasures, risk owner and so on. The format of Risk Register along-with probability and impact setting is enclosed as Annexure B.

4. REFERENCES

i. IS/ ISO 9001:2015 – Requirements

ii. IS/ ISO 31000:2018 – Indian Standard Risk Management: Principles and Guidelines

iii. Corporate Governance Voluntary Guidelines - 2009, Ministry of Corporate Affairs, Government of India

5. SCOPE

This policy applies to management of Risk Register and risk assessment carried out for the following:

a. Processes and Departments
b. Projects.

This policy applies to risk to the Company arising from activities that are delivered in associations/ joint venture partnerships.

6. POLICY

6.1 Statement

G-Tech Infrastructure will seek to identify various risks including threats and vulnerabilities at the earliest opportunity and then measure their likely effect on the achievement of its business goals. Wherever practicable, the Company will endeavour to apply a proportionate level of resources to control known risks in order to preserve the quality of its service provision and at the same time maintaining value for money.

6.2 Roles & Responsibilities

i. Managing Director

- As a custodian of this policy, Managing Director is responsible for approving and authorising the implementation of this Policy.
- Reviewing risk registers that identify the principal risks to the Company and the mitigation strategies in place.

ii. Audit Committee (AC)

- The provision of advice on the strategic process for risk, control and governance and the Statement on Internal Control.
- Identification of additional corporate risks in line with the Scope of Audit Committee.

iii. Vice President

- Ensuring that a system is in place to identify the principal risks to the Company and practical procedures are in place to monitor and mitigate the risks.
- Identifying all significant risks to the Company's business and ensuring that procedures are established to mitigate the impact of the risks in the best interest of all stakeholders.

iii. Manager - Finance

- Identifying the principal risks to the business and ensuring that the Company has implemented appropriate systems and effective risk management programs to manage these risks.
- Overseeing annual review of this Policy for approval of Senior Management.
- Reporting the Company's principal consolidated risks and mitigation strategies on a quarterly/ annual basis (as appropriate) to the Senior Management.

iv. Department Heads/ Project Managers

- Identifying risks and developing and implementing risk management practices, including mitigation strategies, controls and business continuity plans specific to their respective departments, which are aligned with and complementary to the Policy.

- Maintaining risk management reports detailing the principal business risks for the department and making them available to Risk Committee for review and for consolidation at the corporate level.

v. Employees

- In alignment with the values and principles embodied in the Company's core values, this Risk Management Policy commits all staff to consistently apply risk assessment processes and to take professionally assessed risks based upon high-quality work.
- The employees are encouraged to contribute assessed risks to the Risk Register available with Manager – Quality Assurance.

vi. Risk Committee

- The Senior Management is collectively responsible for developing the Company's risk management principles and risk management expectations as well as defining the Company's risk appetite and tolerances.
- Risk Committee may be established by Managing Director from members of Senior Management to address specific risk areas.

vii. Risk Manager

- The management of the Company has delegated an additional responsibility of **Risk Manager** to Vice President.
- Risk Manager will be the custodian of Risk Register and monitoring overall compliance with the Policy.

6.3 Why we need to manage risk

As an infrastructure development organisation, we carry a responsibility to provide clear assurance to our employees, clients, and other stakeholders that risks are being identified, assessed, and managed in a structured manner. Formalising our approach allows us to anticipate challenges, define appropriate mitigating actions, and demonstrate accountability and transparency in all that we do. By embedding risk management into our culture and operations, the Company strengthens resilience, builds trust, and safeguards the long-term sustainability of its business.

6.4 Who should think about risk?

As described under Roles and Responsibilities, the main responsibility for identifying risks lies with Department Heads/ Project Managers. Department Heads/ Project Managers should consider both existing risks and any perceived risk. Inputs by Department/ Project Managers is important as members are well placed to identify and monitor corporate and project risks.

Risk Committee also has a role in providing oversight of risk. Because of this, the risk register needs to be shared with the relevant groups, as appropriate.

6.5 When to consider risk?

Risk needs to be considered when decisions are made. In particular, as corporate goals develop during the planning round, Department/ Project Managers need to consider afresh existing corporate/ other risks; looking at what we want to do over the next few years and identifying risks which may arise.

6.6 Project and department risks

Individual projects may have their own risk registers. Where a project risk is considered high priority, it should be included in the Risk Register. It is the responsibility of Project Manager that concerned Department/ Project Manager & Team Lead stay informed of any such risks.

Individual Managers may also identify risks to their department's objectives. Mitigating actions should be included in risk registers of the relevant Department, as appropriate.

6.7 Risk appetite

"Risk appetite" defines the level and type of risk the Company is willing to accept in pursuit of its objectives. It may vary across time, projects, and business functions depending on strategic priorities and operating conditions. By clearly articulating risk appetite, the Company enables employees to make informed decisions that balance opportunity with responsibility.

Department and Project Managers play a central role in discussing and expressing risk appetite within their teams, ensuring alignment and consistency across the organisation. When updating the risk register, risk owners are expected to assess not only the current and residual risk levels after mitigation but also the **final tolerable risk status** (the point at which the risk is considered acceptable within the Company's appetite.) This structured approach ensures that risk-taking remains deliberate, measured, and aligned with long-term business objectives.

6.8 Reporting risk

All the risks, whether significant or low will be recorded in the Risk Register available with Risk Manager.

The identified risks will be reviewed by risk committee and define the risks and ownership for mitigation of the same. The review shall include assessing the efficacy and usefulness of risk indicators; and where necessary amendments are to be made to the Risk Register.

The Risk register is reviewed on annual basis and/or whenever the following situation arises:

- when new process\department\new externally provided processes (agency) is introduced in the Company
- when there is change in the existing process
- when there is delay in project timeline.

6.9 Options for dealing with risk

There are various options for dealing with risk.

- **Tolerate** – if we cannot reduce the risk in a specific area (or if doing so is out of proportion to the risk) we can decide to tolerate the risk, i.e. do nothing further to reduce the risk. Tolerated risks are simply listed in the Risk Register. If the risk is shown as "green" and "yellow" after existing mitigating actions are taken it can probably be tolerated.
- **Treat** – if we can reduce the risk in a sensible way by identifying mitigating actions and implementing them, we should do so. For most of the risks in the Risk Register this is what we are doing.
- **Transfer** – here risks might be transferred to other organisations, for example by use of insurance or transferring out an area of work.
- **Terminate** – this applies to risks we cannot mitigate other than by not doing work in that specific area. For example, if a particular project is very high risk and these risks cannot be mitigated, we might decide to cancel the project.

6.10 Risk Status

"Risk status" is an assessment of the risk's seriousness. We assign a status as open or close, so that risks can be prioritised. A high impact high likelihood risk should be given more attention than a high impact low likelihood risk which is usually tolerated. Risk matrix is used to show the risk status. Annexure B provides risk matrix and risk settings on probability of risk materialising and associated impact.

ANNEXURE A

RISK CATEGORIES

<table>
<tr><th>CATEGORY OF RISKS</th><th>SUB-CATEGORY</th></tr>
<tr><td><b>Market</b></td><td>▪ Client
▪ Competition
▪ Technological Innovation</td></tr>
<tr><td colspan="2"><i>Example 1: Negative impact on revenues due to inability to adapt to changes in client's preferences for the Company solutions.</i>
<i>Example 2: New competitors may serve to lower fees.</i></td></tr>
<tr><td><b>Third Party</b></td><td>▪ Partnerships
▪ Associations
▪ Consultants
▪ Suppliers, Vendors</td></tr>
<tr><td colspan="2"><i>Example 1: G-Tech Infrastructure partner fails to meet timelines for deliverables, damaging the Company's reputation.</i>
<i>Example 2: Sub-consultant provides sub-par data resulting in delay in submission of deliverable to the Client.</i></td></tr>
<tr><td><b>Human Resources</b></td><td>▪ Talent Acquisition
▪ Talent Retention
▪ Agreements
▪ Fraud</td></tr>
<tr><td colspan="2"><i>Example 1: Negative performance and client satisfaction due to the inability to attract and retain qualified personnel.</i>
<i>Example 2: Submission of fake qualification certificates/ salary slip resulting in high compensation.</i></td></tr>
<tr><td><b>Regulatory/ Legal</b></td><td>▪ Compliance
▪ Legislative Change
▪ Political Change
▪ Litigation
▪ Intellectual Property</td></tr>
<tr><td colspan="2"><i>Example 1: International location's government changes its laws or regulations making it difficult or impossible to do business or withdraw capital.</i>
<i>Example 2: Material adverse impact to operations, cash flows or financial position due to the outcome of tax and/or legal proceedings.</i></td></tr>
<tr><td><b>Economic/ Financial</b></td><td>▪ Credit Environment
▪ Liquidity
▪ Capital Availability
▪ Capital Allocation
▪ Interest Rates</td></tr>
<tr><td colspan="2"><i>Example 1: Slowdown in economic growth reduces the growth of business environment.</i>
<i>Example 2: Negative impact and disruption to the business due to acquisitions or divestitures.</i>
<i>Example 3: Negative impact to the business as a result of increase in interest rates.</i></td></tr>
</table>

CATEGORY OF RISKS	SUB-CATEGORY
Example 4: Negative impact to growth plans because capital is not available for investment as anticipated.	
Project	▪ Operational Execution ▪ Process Design ▪ Data Integrity
Example 1: Inability to achieve desired financial targets due to non-conformance to the budgetary allocation. *Example 2: Inability to achieve successful strategy implementation due to poor execution of implementation plan.* *Example 3: Negative impact to business due to poor project management and/or outdated technology platforms.*	
Business Interruption	▪ Epidemic ▪ Fire ▪ Natural Disaster ▪ Act of God
Example 1: Inability to continue business operations due to loss of key assets, including interruption of telecommunications links, the internet or power sources.	

The above list is not exhaustive. Other risks shall be included, upon review, as necessary.

ANNEXURE B

FORMAT OF RISK REGISTER

	RISK IDENTIFICATION						EXISTING CONTROL MECHANISM						ACTIONABLES		MITIGATION MANAGEMENT							OPPORTUNITY	OPEN / CLOSED
	RISK ID	RISK OWNER	RISK EVENT	CATEGORY	RISK CAUSE	PROBABLE IMPACT(S)/ CONSEQUENCE (S)	EXISTING MITIGATIONS	CURRENT RISK RATING (Risk rating based on effectiveness of current controls at the time of the initial risk assessment)				ADEQUACY OF EXISTING MITIGATIONS	ACTION REQUIRED	ACTION OWNER	ADDITIONAL MITIGATIONS	TIMELINES	TARGET RISK RATING (Risk rating that you wish to manage the risk down to that level)				TRACKING		
								P (1-4)	I (1-3)	SUM	RISK RATING						P (1-4)	I (1-3)	SUM	RISK RATING	PROGRESS %		OPEN / CLOSED
Input serial no.	*State the risk ID. Risk IDs are denoted by . abbreviated form of the project followed by risk no. for that project*	*Who is responsible for management, monitoring and control of identified risk, including implementation of mitigating actions*	*Describe the risk event. Risks are future events that could interfere with achievement of objectives.*	*Include risk category for the stated risk (refer sheet 3)*	*What are the triggers, sources or circumstances that could act alone or together to increase the likelihood of the Risk Event occurring? There are usually multiple causes leading to a Risk Event.*	*If this Risk Event did occur, how would it impact objectives? What are the longer-term or cumulative consequences?*	*What are you doing now to reduce the likelihood or impact of the event?*	*How likely?*	*How severe?*	*Sum (P*I)*	*Rating*	*Non-existent, Inadequate, Adequate, Robust, Excessive*	*Will you treat, monitor, transfer or avoid the risk?*	*Who will take the lead on this mitigation?*	*What else are you going to do to better manage the risk?*	*When will be the mitigation actions ready?*	*How likely?*	*How severe?*	*Sum (P*I)*	*Rating*	*What is the progress to date of mitigating action?*	*Describe the opportunity associated with risk and as a favorable or advantageous circumstance. Can lead to the adoption of new practices or other desirable and viable possibilities to address the company/ department needs.*	*State whether the risk status is open or closed i.e. whether the risk has been mitigated.*
										0	UNRATED								0	UNRATED			
										0	UNRATED								0	UNRATED			

Risk Probability Setting

Rating	Probability	Criteria
1	Low	Unlikely to occur but not impossible. *Incidents of this nature are uncommon but there is a genuine chance that we may experience them at some future point.*
2	Medium	Less likely than not. *It is distinctly possible that we may experience incidents of this nature.*
3	High	More likely to occur than not. *We are likely to experience incidents of this nature before long.*
4	Extreme	Very likely though not certain. *We are bound to experience incident(s) of this nature but not certain when.*

Risk Impact Setting

Rating	Impact	Criteria
1	Minor	Likely to have minor impact in one or a few areas.
2	Moderate	Likely to have major impact in one or a few areas.
3	Significant	Likely to have substantial impact.

Probability – Impact Matrix

Probability					
Low (1)	Medium (2)	High (3)	Very High (4)	▨	Impact
Low Risk (3)	Medium Risk (6)	High Risk (9)	High Risk (12)	Significant (3)	
Low Risk (2)	Low Risk (4)	Medium Risk (6)	Medium Risk (8)	Moderate (2)	
Low Risk (1)	Low Risk (2)	Low Risk (3)	Low Risk (4)	Minor (1)	

If risk rating (Probability * Impact) is coming as low risk, then no further action and mitigation management is required.