RISK MANAGEMENT POLICY AND PROCEDURE

1. INTRODUCTION

1.1 Purpose

All activities of GTN Limited (**GTN**) and its subsidiaries – including The Australia Traffic Network Pty Limited, Canadian Traffic Network ULC, Global Traffic Network UK (Commercial) Limited and BTN Servicos de Informacao do Transito Ltda (**GTN Group**) – carry elements of risk.

The exposure to these risks is managed through the practice of 'risk management'. Effective risk management allows GTN to mitigate potential adverse effects while also leveraging opportunities.

This Policy outlines GTN's risk management framework and sets out the responsibilities of the Board, the Audit and Risk Committee, senior management and others within the GTN Group.

1.2 Policy owner

GTN's Chief Financial Officer (**CFO**) and Chief General Counsel are the owners of this Policy, with the CFO responsible for the oversight of GTN's risk management framework.

2. UNDERSTANDING RISK MANAGEMENT

Risk is defined as the likelihood that an event may occur which impacts the GTN Group's objectives.

GTN's risks may come from any internal or external event which, if it occurs, may affect the ability to efficiently and effectively operate. Risks may arise from:

- **Internal risks** – those risks that specifically relate to GTN's business itself and, as such, are generally within its control. They include risks such as employee conduct risks, strategic risks, and financial risks.
- **External risks** – those risks that are outside the control of GTN. They include risks such as market conditions, digital disruption, cyber-security, privacy and data breaches, sustainability, climate change and legislative change.

Risk management refers to the culture, processes and structures used to identify, assess and manage risks – maximising opportunities while minimising adverse effects.

GTN's risk management framework is designed to identify and assess risks across the GTN Group and put measures in place to reduce them to acceptable levels. To do so, each business unit will maintain a risk register (see **Appendix A** for risk register template), with risks owned by designated individuals (**Risk Owners**). Risks are assessed using GTN's Risk Assessment Matrix (see **Appendix B**), ensuring consistency across the GTN Group.

GTN manages risks through the effective implementation of various controls, which includes:

- A Board-approved risk management framework;
- Documented policies and procedures;
- Maintenance of risk registers;
- Risk-based systems for monitoring and compliance;
- Ongoing review of regulatory obligations;
- Internal reporting.

3. ROLES AND RESPONSIBILITY

3.1. Board & ARC

The role of the GTN Board is to set the risk appetite for the GTN Group, to oversee its risk management framework and satisfy itself that the framework is sound.

The Audit and Risk Committee, has responsibility under its Charter to:

(a) oversee that management designs and implements an appropriate and effective risk management framework;

(b) review the risk management framework at least annually to determine that it continues to be sound and that the GTN Group is operating with due regard to the risk appetite set by the Board, and effectively identifies all areas of potential risks;

(c) ensure adequate policies and processes have been designed and implemented to manage identified risks;

(d) ensure proper remedial action is undertaken to redress areas of weakness; and

(e) report and make recommendations to the Board on risk management issues.

3.2. Chief Financial Officer

The CFO is responsible for:

(a) monitoring compliance with this Policy;

(b) reporting on compliance with this Policy to the Board;

(c) developing, implementing and monitoring risk management systems, policies and procedures;

(d) facilitating regular reviews of the risk management framework; and

(e) maintaining the risk registers.

3.3. Risk Owners

Risk Owners are responsible for the day-to-day management of specific risks, including:

(a) implementing operational procedures and controls;

(b) monitoring effectiveness of those controls;

(c) escalating risks to the CFO when existing treatments are insufficient; and

(d) recommending alternative treatments or controls when necessary to the CFO.

3.4. Management and Employees

All GTN Group employees are responsible for identifying and reporting potential risks and supporting implementation of controls.

Management is accountable for identifying and managing risks within their area, incorporating risk considerations into planning and operations, implementing mitigation strategies and promoting a culture of risk awareness.

Where there is legislation in place for the management of specific risks (such as Workplace Health and Safety), this Policy does not relieve GTN of its responsibility to comply with that legislation.

4. RISK MANAGEMENT FRAMEWORK AND METHODOLOGY

GTN's risk management framework is dynamic and designed to adapt to the GTN Group's developments and changes in risk profile.

GTN's risk management framework and methodology include the following steps:

(A) **Establish the context** – establish the external, internal and risk management context in which the rest of the process will take place – the criteria against which risk will be evaluated should be established and the structure of the analysis defined.

(B) **Communicate and consult** – engage with stakeholders throughout the process.

(C) **Identify risks** – determine where, when, why and how events could impact GTN's objectives or activities by considering all relevant business categories and asking: *what could happen, how and why could it happen?*

(D) **Analyse risks** –

i. Rate the likelihood of occurrence of the risk (**Almost Certain**, **Likely**, **Possible**, **Unlikely** or **Rare**).

ii. Assess the consequences of the risk (**Catastrophic**, **Major**, **Severe**, **Serious**, **Minor**).

iii. Determine the inherent risk rating based on likelihood x consequence (**Critical**, **High**, **Medium** or **Low**).

iv. Identify and assess existing controls and risk treatment plans, and determine the residual rating of each risk .

(E) **Evaluate risks** – compare estimated levels of risk against the pre-established criteria and consider the balance between potential benefits and adverse outcomes. This enables decisions to be made about the extent and nature of treatments required and about priorities.

(F) **Treat risks** –implement cost-effective risk treatments and mitigation strategies.

(G) **Record risks** – document all identified risks, controls and treatments in the relevant risk register, with a designated Risk Owner assigned to each risk.

(H) **Monitor and review** – routinely review risks and effectiveness of treatment measures.

(I) **Communicate to the Board** – provide reports to the Board and Audit and Risk Committee at agreed times.

Appendix A – Risk Register Template

Risk Category	Risk Title	Risk Description	Root Cause	Inherent Likelihood	Inherent Consequence	Inherent Risk Rating	Existing Controls	Residual Likelihood	Residual Consequence	Residual Risk Rating	Treatment Plan	Risk Owner
E.g. Financial				*E.g. Possible*	*E.g. Major*	*E.g. High*		*E.g. Unlikely*	*E.g. Major*	*E.g. Medium*		

Appendix B – Risk Assessment Matrix

Consequence Table

	Regulatory Compliance	People & Safety	Financial	Brand & Reputation	Service Delivery
Catastrophic	Mandatory notifiable incident reporting. Revocation of licences/ accreditation, resulting in long term inability to perform core ops. Significant fines incurred and criminal prosecutions. Major breach resulting in severe penalties/ damages.	Death, permanent disability or significant physical and/or psychological harm to individuals. Loss of key personnel. Impact on organisational culture. Multiple extended workers' compensation claims.	Loss of revenue, which leads to going concern/ viability of the company.	Significant adverse media coverage and other exposure (e.g. enquiries and Royal Commissions) causing irreparable damage to the brand.	Normal daily operations shut down for an extended period (> 2 mths) and a permanent loss of assets and critical information (e.g. client/ personnel data). Inability to meet key contractual agreements/ obligations.
Major	Mandatory notifiable incident reporting. Temporary halt to operations to support investigation. Substantial fines incurred and criminal prosecutions.	Life threatening injury or multiple injuries requiring admission to hospital. Impact on organisational culture and recovery processes.	Loss of revenue, which leads to a reduction in business capacity. Cost of investigations/ external inquiries and business disruptions. Major costs of business continuity of service delivery. >$10m impact	Media coverage causing short term adverse public, stakeholder, regulator and government attention.	Normal daily operations cannot be performed for a prolonged period. Key data requires extended period of time to restore.
Severe	Mandatory notifiable incident reporting and investigations.	Inquiry requiring admission to hospital.	Moderate loss of revenue, which leads to a reduction of some business capacity. Resolution of issue diverts resources away from	Adverse regional media coverage and community uproar.	Normal key daily operations cannot be performed (for up to 1 week). Majority of key data restored, loss restricted to one area of the organisation.

			BAU and service delivery. $5m-$10m impact		
Serious	Compliance notification unlikely to be required where non-compliance is only minor and can be resolved internally.	Minor illness or injury requiring medical attention (e.g. first aid).	Costs of business continuity are manageable within existing resources. $1m-$5m impact	Sector knowledge of incident, however no media attention. Some impact on community support.	Minor operational problems – normal operations can be restored within 1 day. No loss of key data.
Minor	No compliance / regulatory notification. Event that may be resolved without legal remedy. Incident managed internally with no adverse effects.	Illness or injury that does not require medical attention. Adverse impacts result in minimal change to work conditions (e.g. near miss).	Insignificant financial impact or costs. Operations continued to be delivered with some minor budgetary impact. <$1m impact	Reputation intact. Minimal impact on stakeholders (i.e. affiliates/ advertisers).	Minimal impact on key operational area – full operations can be restored within a few hours and/or delivered by alternative means.

Likelihood Probability & Frequency Table

Probability Factor	Description	Frequency (of occurring in next 12 months)
Almost Certain	Known to happen often	> 95%
Likely	Could easily happen	50% - 95%
Possible	Could happen & has occurred before	15% - 50%
Unlikely	Hasn't happened yet but could	5% - 15%
Rare	Conceivable, but only in extreme circumstances	> 5%

Risk Assessment Matrix

LIKELIHOOD	CONSEQUENCE				
Probability Factor	**Minor**	**Serious**	**Severe**	**Major**	**Catastrophic**
Almost Certain	Medium	High	High	Critical	Critical
Likely	Medium	Medium	High	High	Critical
Possible	Low	Medium	Medium	High	High
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Low	Medium	Medium

Risk Rating Table

Critical	Extreme risk - detailed research and management planning required at senior levels
High	High risk- immediate senior management attention needed
Medium	Moderate risk - management responsibility must be specified
Low	Low risk - managed by routine procedures