TIM GROUP
CRISIS MANAGEMENT POLICY

ISSUED BY THE SECURITY FUNCTION
ABSTRACT

OCTOBER 2020

Introduction

As part of its **fundamental values, TIM Group aims to protect human resources both inside and outside the organization, to safeguard the value of tangible and intangible assets, both its own and those of third parties, and to ensure continuity in the provision of telecommunication services.**

These values are also affirmed in TIM Group's Code of Ethics, which sets out its inspiring business principles, with respect to the main internal and external stakeholders with whom the Group interacts daily: employees, customers, shareholders, investors, communities, local, national and supranational institutions, suppliers, business partners.

The protection of human, tangible and intangible resources also involves managing a variety of **"Non-competitive" risks** to which these resources are exposed. These risk scenarios are constantly evolving and must be neutralized as far as possible through risk mitigation and management strategies and tools.

The communication network has always been a **strategic infrastructure** for the national economy; as such, it is interdependent on other critical infrastructures. Communication services are considered **essential services** in emergency management. For this reason, the TIM Group is required to participate in Crisis Units that are set up at an institutional level.

Specifically, the purpose of the **TIM Group Crisis Management System** is to limit both direct and indirect tangible and intangible damage caused by exceptional adverse events on company resources (human resources, tangible and intangible assets), in order to ensure continuity and quality of telecommunication services in emergency situations, to quickly bring back the infrastructure processes and functions to their pre-crisis conditions, to safeguard the corporate image and reputation, to contribute to the Group's sustainability.

As such, it is crucial for the TIM Group to put in place and maintain an efficient Crisis Management System: preventing an emergency or crisis situation and, where this is not possible, managing and successfully dealing with it contributes, both directly and indirectly, to protecting the value of the Group's companies and to comply with TIM fundamental principles.

Purpose and scope of application

The Crisis Management System is an essential tool for generating the necessary organizational response to an emergency/crisis, through the planning and application of methods and techniques that are capable of coping, in a very short time, with very serious events, while minimizing their long and short-term effects.

The scope of application is therefore limited to **critical events that are potentially capable of generating an emergency/crisis**, which show a significant combination of the following elements:

- **SEVERITY** intended as a metric of the direct and indirect damage suffered by the Group's assets;
- Radical and extensive **INAPPLICABILITY** of ordinary behaviour, as the management of the event cannot rely on normal operating procedures;
- **TIME PRESSURE**, which requires quick decisions and actions, moreover in combination across multiple organizations.

Of all the potential scenarios that this Policy is intended to address, there are some that

can be outlined in advance due to their frequency and potential impact on the Group's operations and image. These scenarios, albeit not exclusively, are the subject of the Crisis Management System:

- **defence and civil protection emergencies/crises** (e.g.: natural disasters, accidents of anthropogenic or accidental origin, terrorist attacks);
- **emergencies/crises involving employees and/or other resources abroad** (e.g.: natural disasters, kidnappings, epidemics, pandemics, sabotage, wars, terrorism);
- **ICT security emergencies/crises, caused by significant failures and malfunctions, also due to malicious actions** (e.g.: IT intrusion in ICT systems, malware propagation that causes blocks to IT systems and/or Office Automation tools, DDOS attacks).

The Crisis Management System is also triggered during major institutional events in Italy.

This Policy applies to the TIM Group companies in Italy and abroad.

Description of the System and Responsibilities

The Crisis Management System outlines the set of specific actions comprised in the various steps and **the extraordinary and provisional organization** which, limited to the period of emergency management, overlaps with the ordinary organization.

The emergency organization is modular in nature and planned methodologies and tools are simple and flexible, as they must be immediately applicable to events that occur in different contexts and which are unpredictable and non-preventable as to their specific characteristics.

Emergency planning provides criteria and guidelines for the management of critical events, **regardless of the extent, severity, cause of the events and the number of persons (internal and external) involved.** Crisis Management procedures and instructions use simple language and clear terminology, to allow and encourage straightforward communication and efficient collaboration among all corporate functions involved in the management and overcoming of the emergency / crisis.

The Crisis Management System rests on three pillars:

- adequate **TRAINING**;
- a specific **ORGANIZATION MODEL**;
- a **REGULATORY FRAMEWORK** comprising specific different types of critical events, emergencies/crises.

Training

The awareness that well-prepared and trained human resources are key to successfully managing an emergency is the basis of the Crisis Management System.

The aim of the theoretical and practical training of staff involved in emergency management is to develop within the TIM Group **a culture of risk prevention and of safeguard of corporate resources as well as to share and consolidate best practices in responding to different types of emergencies/crises.**

To this end, **awareness-raising and updating events** are periodically organized among the Functions involved in crisis management, while specific exercises are organised independently or in agreement with the Institutions in charge of emergency/crisis management, assuming different scenarios from time to time, in order to verify the state of readiness (preparation, readiness and

speed) of the corporate units expected to be involved in the successful management of an emergency situation.

Responsibility for maintaining a state of readiness rests with the individual Functions, which are called upon for various reasons to manage the emergency/crisis; said functions must ensure their processes and tools are fully effective and efficient and must implement the individual procedures and instructions.

Organisational Model: **roles, responsibilities and tools**

Crisis management is implemented on the basis of a pre-established governance system, which ensures the ability to make adequate and timely decisions, by adopting logical and organizational physical countermeasures suitable for countering and overcoming the emergency/crisis in the shortest possible time. Therefore, an **organizational model** has been designed which comprises:

- a **Crisis Management Committee** that sets out emergency/crisis management strategies;
- **Operational Crisis Teams**, responsible for the operational coordination of management activities with respect to the various types of critical events;
- the **Company Representative** representing TIM vis à vis the Institutional Bodies;
- management **tools**.

Regulatory framework

A structured procedural approach is essential for dealing with the various emergency scenarios; such an approach is mainly based on the use of management tools, usually computer tools, which immediately suggest procedural steps in the use of all human, technological and instrumental resources that are suitable to counter, manage and overcome the adverse event.

Sequence of steps of the management system

The management system comprises the following steps:

- **planning**, which takes place during the ordinary course of business, also called peacetime;
- **pre-emergency/crisis**, from the occurrence of the critical event up to its escalation (if any) to an emergency / crisis;
- **emergency/crisis**, when the extraordinary organisation and procedures are triggered;
- **post-emergency/crisis**, after the events have been fully successfully dealt with and, therefore, the emergency/crisis is closed and the status quo ante has been reinstated.

Note that, owing to the **flexibility of the Crisis Management System**, the relevant corporate functions are able, during the various management steps, to decide - from time to time, according to the type, geographical extension, and severity of the event as well as the requests from Institutions - the **organizational configuration and operational safeguards that are most effective** in fighting and successfully dealing with the events, (e.g.: simple supervision, local operational safeguards, activation of one or more OCTs, activation of the CMC).