

# Security Policy Statement

## TelecityGroup Information

Version No: 1.1  
Owner: Group Security Manager  
Document Number: TCG-SEC-STA-002  
For Display on notice boards TCG-POL-004



### Statement

TelecityGroup is a leading independent provider of colocation, managed data centre, hosting and connectivity services in Europe. TelecityGroup specialises in the design, build, and management of business-critical web infrastructures, helping companies reduce the cost, complexity and security risks associated with maintaining web and online environments. TelecityGroup services are underpinned by solid infrastructure, which includes multiple high-tech data centres across Europe.

### Objectives

The objective of managing information security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents. In deploying the TelecityGroup Information Security Management System ("ISMS"), the Management Team aim to maintain existing known risks at their current low level and ensure that new and changing risks are managed in an equally consistent and professional manner.

### Purpose

The purpose of the Policy is to protect both TelecityGroup and its Customers Assets from all threats, whether internal or external, deliberate or accidental. Protection of information is set out in terms of:

- Confidentiality: ensuring only persons who are authorised have access to information.
- Integrity: ensuring the purity, accuracy and completeness of information.
- Availability: ensuring information, associated assets, and systems can be accessed when required by authorised persons.
- Regulatory: regarding regulations, laws and codes of practice in each country where it operates as a minimum standard in its Information security management standard.

### In particular TelecityGroup will:

- Ensure that TelecityGroup management and employees comply with the requirements of the security policy.
- Minimise the risk of damage to company assets, information, reputation, hardware, software or data.
- Ensure that TelecityGroup people and computer systems do not infringe any copyright, licensing or laws.
- Set out clearly the company's policies relating to all aspects of the management of information, hardware, firmware and software.
- Define a systematic approach to risk assessment by Identifying a method of that is suited to the ISMS, the identified business information security, legal and regulatory requirements.
- Setting policy and objectives for the ISMS to reduce risks to acceptable levels. Determining criteria for accepting the risks and identify the acceptable levels of risk.

**The Security Manager has direct responsibility for maintaining the Security Policy and providing advice and guidance on its implementation.**

**All managers are directly responsible for implementing the Security Policy within their business areas, and for adherence by their staff.**

**It is the responsibility of each member of staff to adhere to the Security Policy. Failure to do so may result in disciplinary action.**

Signed:

Michael Tobin  
CEO (TelecityGroup)  
Dated: January 2012