TALON GLOBAL

POLICY

# Information Security Policy

Our clients trust Talon Global with the records that prove their compliance. Protecting the confidentiality, integrity and availability of that information, and of our own, is a condition of being in this business, not an extra.

## WE COMMIT TO

01 Protect client and Talon information so only the right people and systems can reach it, and every access to a client's data leaves a record.

02 Meet the legal, regulatory and contractual information security requirements that apply to us and to the data our clients entrust to us.

03 Find and fix security weaknesses quickly, within the times we set and measure.

04 Make sure we can recover: our backups are tested and proven, not assumed.

05 Test our controls on schedule, act on what the tests show, and keep improving our information security management system.

This policy applies to everyone who works for or on behalf of Talon Global, and to every system and supplier that handles our information or our clients'. It is published on talon.ae, acknowledged by everyone it applies to, and reviewed at least once a year and at every management review.

APPROVED BY

**Darren Watts**
Founder, Talon Global · 16 Nov 2026



QR

HOW THIS POLICY WORKS

# Information Security Policy

## Objectives

Our information security objectives are set by top management and held in the Objectives Register (TG-INT-REG-010): no client data lost or exposed, critical vulnerabilities fixed within 24 hours and high within 72, a successful restore test every quarter, 90% or more of control tests completed on schedule, and every data subject request answered within the legal deadline.

## How we manage it

We assess information security risks against defined criteria and treat them with controls chosen against ISO/IEC 27001 Annex A, recorded in our Statement of Applicability (TG-ISM-REG-002). Each control is evidenced by the records it produces as it runs, and tested by sampling those records.

## Topic policies

Specific rules for acceptable use, cloud services, remote working, clear desk and screen, and cryptography are set out in our Information Security Topic Policies (TG-ISM-POL-002), which sit under this policy.

## Suppliers

We evaluate every supplier and subprocessor for security and privacy before we use them, bind them by agreement, and review them at least once a year.

## Incidents

Anyone who sees or suspects a security event reports it straight away. We assess it, contain it, keep the evidence, notify those we must within the legal time, and change the system so it does not happen again.

## Review

Top management reviews this policy at least once a year, at every management review, and whenever a significant change in our risks, our systems or the law calls for it.



QR