



## Information Security and Acceptable Use of IT Policy 11/2025

### Introduction

TropicalAstral relies heavily on digital tools, online platforms and remote collaboration. Protecting our data, systems and the information entrusted to us by clients, learners and partners is essential.

### 1. Purpose

This policy provides simple rules for using IT equipment, software, internet, email and collaboration tools in a secure and responsible way.

### 2. Scope

Applies to all TropicalAstral staff, freelancers, interns and any person using company accounts or devices.

### 3. General rules

- Company accounts (email, project platforms, cloud storage) must only be used by the person assigned to them.
- Passwords must be strong, unique and not shared with others. Where possible, two-factor authentication should be used.
- Devices used for work (laptops, phones, tablets) must be protected with a screen lock and kept updated.

### 4. Use of email and communication tools

- Work email and messaging tools must be used respectfully and professionally.
- Phishing and suspicious emails must not be opened; links and attachments should be checked carefully.
- Confidential or sensitive information should not be shared via unsecured channels. If needed, encryption or password-protected files should be used.

### 5. Cloud storage and file management

- Only approved cloud services should be used to store work-related documents.
- Shared folders must be organised logically, with access granted only to those who need it.
- Files containing personal data or sensitive information must be clearly labelled and stored in restricted folders.

### 6. Acceptable use of internet and social media

- Internet access and social media may be used for reasonable personal purposes as long as it does not interfere with work and does not violate any law or company policy.
- Users must not visit illegal or clearly inappropriate websites using company connections or devices.
- When representing TropicalAstral online, staff must follow the Social Media & Communication guidelines (see Code of Conduct).



### **7. Security incidents**

- Any suspected data breach, loss of device or security incident must be reported immediately to management.
- We will investigate and, where required, notify affected parties and authorities.

### **8. Monitoring and review**

TropicalAstral may monitor system usage at an aggregate level to ensure security and performance. This policy is reviewed regularly together with the Data Protection Policy.