Information Security Policy

Harbor & Pine Ltd · Policy IS-01 · Version 3.2 · Owner: Security team · Applies to all staff and contractors

1. Purpose

Harbor & Pine handles customer orders, payment details and supplier contracts every day. A single stolen laptop or a single password typed into the wrong page can expose all of it. This policy sets out the minimum habits every person at Harbor & Pine is expected to follow, and what to do when something goes wrong.

Most security incidents in companies our size do not start with a clever attack. They start with an unlocked screen, a reused password or an email that looked real enough. The rules below are written to close those three doors first.

2. Scope

This policy applies to every employee, contractor and temporary worker, on every device used for Harbor & Pine work, whether the device is owned by the company or by you. It covers work done in the office, at home, and while travelling.

3. Lock your screen, every time you step away

Lock your computer whenever you leave it, even for a minute. On Windows press Windows key + L; on a Mac press Control + Command + Q. Company laptops lock automatically after 5 minutes without activity, but do not rely on the timer. An unlocked screen gives anyone nearby the same access you have: your email, our customer records and the finance tools.

Phones used for work email must have a passcode of at least six digits or a biometric lock.

4. Turn on two-factor authentication

Every work account that supports it must use two-factor authentication (2FA): something you know (your password) plus something you have (your phone or a security key). Use the company authenticator app, not text messages, wherever the system allows it.

2FA matters because passwords leak. If a password is stolen in a breach at another website, 2FA is what stops an attacker from using it on ours. The IT desk will set it up with you in about ten minutes.

Passwords must be at least 14 characters, unique to each account and stored in the company password manager. Never reuse a work password anywhere else, and never share it, including with the IT desk. IT will never ask for your password.

5. Report phishing within one hour

Phishing emails try to make you click a link, open an attachment or send money or passwords by pretending to be someone you trust. Watch for these warning signs:

Warning sign	**Example**
Urgency or pressure	"Your account will be closed today unless you confirm your details."
A sender address that is almost right	accounts@harbor-and-pine.co instead of harborandpine.com
Unexpected attachments or links	An "invoice" from a supplier you have never ordered from
Requests to pay or change bank details	A "director" asking for an urgent transfer by email

If an email looks suspicious, do not click anything. Use the Report Phishing button in your mail app, or forward the email to security@harborandpine.example within one hour. If you already clicked a link or entered a password, report it anyway and change the password straight away. Reporting quickly is never a mistake: the sooner we know, the smaller the damage.

6. Devices and data

Keep company data on company systems. Do not copy customer data to personal email, personal cloud storage or USB drives. Company laptops are encrypted; keep them updated by restarting when prompted, at least once a week.

If a device is lost or stolen, tell the IT desk immediately so it can be locked and wiped remotely.

7. When something goes wrong

Report any security incident, or anything you are not sure about, to the security team at security@harborandpine.example or on extension 4400. You will not be blamed for reporting a mistake. You may be asked to explain later why you did not.

8. Summary

If you remember only three things from this policy, remember these: lock your screen whenever you step away, keep two-factor authentication switched on for every account, and report anything that looks like phishing within one hour.

Approved by the Harbor & Pine leadership team. Next review: March 2027.