

# INFORMATION SECURITY POLICY

Treadwells is committed to safeguarding information belonging to Treadwells, clients, and third parties, within a secure system. This Policy sets out how Treadwells Partners and Staff are required to use Treadwells' systems to ensure information is kept secure.

Treadwells aims to ensure that:

- Information is protected against unauthorised access or misuse;
- Information is at all times kept confidential and secure;
- Regulatory and legal requirements are complied with;
- Files and any other information is disposed of in an appropriate manner when required;
- Physical and digital security systems are maintained and systems are adequately protected from unauthorised access;
- Electronic data can be recovered in the event of a system failure;
- Any third parties entrusted with Treadwells' information understand and uphold their responsibilities with respect to maintaining security; and
- Systems are used for their intended purpose and any information security incident is dealt with appropriately.

In this Policy, information includes the following:

- All electronic information systems and computer networks owned and/or used by Treadwells whether accessed on or off site; and
- Software and data owned by Treadwells whether in electronic or paper-based form.

Treadwells requires all users to exercise a duty of care in relation to its systems and information handling.

All users are authorised by appointment as a member of staff, or by other process specifically authorised by Treadwells. Authorised users must not disclose any password associated with their individual user identity. Authorised users will ensure they protect Treadwells' information and uphold the principles of confidentiality and privacy.