

# Framework Business Consultancy Limited I.T. Security Policy

The purpose of this Policy is to encourage staff to use general I.T. Guidelines.

## ***Procedures and Processes***

- Passwords should be 6+ characters in length using 1 number and should not contain all the same characters, e.g. bbbb. They should not be names of children, partners or other relatives or sequenced such as password 1, password 2 etc. They should not be written down or divulged to anyone outside of Framework Business Consultancy Limited.
- Laptops should not be left unattended and/or logged on for extended periods at client's premises.
- Laptops should not be left in unattended vehicles.
- Any Laptop thefts must be communicated to Framework Business Consultancy Limited if they contained any Framework Business Consultancy Limited documents or any confidential information.
- All Framework Business Consultancy Limited documents must be backed up. A copy will be held at a Framework Business Consultancy Limited office PC.
- Any documents carried on a USB Key/Flash drive should be password protected or use fingerprint recognition for security purposes
- All Laptops used by any staff must have anti-virus software installed to prevent access of any viruses.
- No-one is to open an attachment on an email unless they are certain where the email is from.
- The internet should be used in a responsible manner.

This policy is fully supported by Angie Ingman. We will ensure that all our staff, customers and clients are aware of the Policy, and that staff understands that they are responsible for observing it.

Our I.T Security Policy action plan outlines the steps we will take to give effect to this Policy. We will monitor the action plan and review the progress we have made each year, to make sure the Policy is achieving its aims.

# Framework Business Consultancy Limited I.T. Security Policy

## Action Plan

- Angie Ingman is responsible for the I.T. Security policy and for putting the action plan into practice.
- We will circulate our I.T. Security policy to all staff by means of a Policy Handbook and via the Company Website.
- We will ensure that all staff sign a declaration that they have read, understood and accepted individual responsibility for this Policy.
- We will keep records of all staff acknowledgements.
- We will keep abreast of any I.T. Security developments and incorporate any practical actions into the plan.
- We review all our Policies every six months.
- We welcome feedback from our clients, associates and other interested bodies, implementing any procedures that will improve our Policies.