

# ManDev Ltd 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 ManDev Ltd.
- 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 ManDev Ltd if they contained any ManDev Ltd documents or any confidential information.
- All ManDev Ltd documents must be backed up. A copy will be held at a ManDev Ltd 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.

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.

*January 2009*