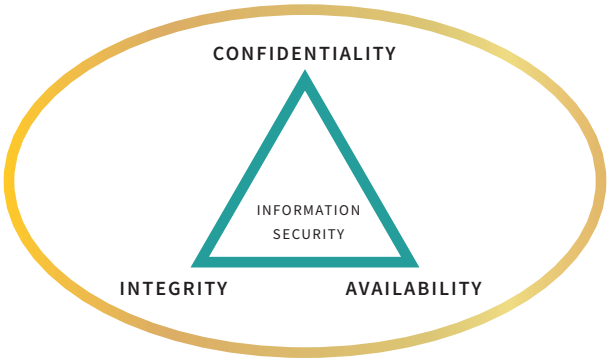
INFORMATION SECURITY



CONFIDENTIALITY

Information must not be made available or disclosed to unauthorised persons, entities or processes.

- Customer data - Not to be taken offsite unless explicitly requested.
- Trade Secrets - All work is kept confidential.
- Financials - Never share any financial data outside what is permissible.
- Information sent to wrong persons - Make sure emails and messages are sent to the correct persons.
- Divulge information - Keep customer information private and never reveal or write down any passwords.
- Stolen or lost computer / memory stick - Never take any data offsite unless required by the customer.
- Photocopier / Printers - Don't print anything and leave it on the printer.

INTEGRITY

The integrity of information is about the accuracy and completeness of information.

- Incorrect input – Human error; check spelling, punctuation, grammar, numbers etc .
- Processing issues – Check code, scripts and configs. Check IP addresses, gateways, DNS entries etc.
- Presentation of data – Reports must be clear, fully completed and unambiguous.
- System data – Check updates are correct, get permission before patching any system, don't restore the wrong file, make sure all files are from legitimate sources.

AVAILABILITY

Making information, data and services accessible and useable upon demand by an authorised entity.

- Unintended causes – Check when patching network cables ports are correct. Check when removing cables the correct one is pulled.
- Technical malfunction – In the case of a system malfunction due to an incorrect activity or incompatibility, inform the manager and if possible reverse the activity that caused the failure.
- IT System capacity and capability – Be aware of the effect that any additional resource, patch or upgrade will cause to the infrastructure so a system does not fail.
- Knowledge – Check with the local contact or a manager if instructions are not clear or if you feel there may be a risk attached to the task.