



Information Security Policy

Diligent Developments Ltd Limited is trading as Diligent Developments Ltd
Company Number – 5323384
Registered Office – Office 6, 78-88 Bensham Grove, Thornton Heath, CR7 8DB



Our Information Security Policy

External, Deliberate or Accidental.

Diligent Developments Ltd has devised an Information Security Policy document which ensures that:

- 1) Confidentiality of information is assured
- 2) Integrity of information and service is maintained
- 3) Availability of information and service is maintained
- 4) Information is protected against unauthorised access
- 5) Authentication ensures only authorised user access
- 6) Regulatory and legislative requirements are met
- 7) Business continuity plans are produced, maintained and tested
- 8) Information security training is available to all staff
- 9) All breaches of information security, actual or suspected, are reported to the Director, and investigated by the ISM.
- 10) Valuable or sensitive information is protected from unauthorised disclosure or intelligible interruption.
- 11) Accuracy and completeness of information is safeguarded by protecting against unauthorised modification.
- 12) This applies to record keeping and most controls will already be in place; it includes the requirements of legislation such as the companies act and the data protection act.
- 13) This will ensure that information and vital services are available to users when and where they need them.
- 14) Business requirements for availability of information and information systems are met.
- 15) The information security manager (ism) has direct responsibility for maintaining the policy and providing advice and guidance on its implementation.
- 16) The information security group (isg) comprising the senior management team (smt) has agreed any changes to this policy and/or system and the risk manager has authorised any changes to this policy and/or system.
- 17) Any changes to the network, system, internal and external connections to the system, products used within the system, system operating procedures must be agreed with the isg and approved by the risk manager.
- 18) All managers are directly responsible for implementing the policy within their business areas, and for adherence by their staff.
- 19) Each member of staff understands they are responsible for adhering to the policy.
- 20) An assessment of the security measures required to protect assets has been conducted and documented. This includes any business domain, risk assessment and an assurance level requirement. Any use of the Diligent Developments Ltd system or its data outside the uk mainland must be referred to and agreed by the risk manager.
- 21) This information security policy document will be reviewed bi-annually by the information security manager and the risk manager, from the date of approval and complete signatories

This policy is reviewed for continuing adequacy and suitability at management review.



(Director) Date: 19/11/2011

Sebastian Stephenson.