Plasser UK

Information Security Policy

The Company has determined external and internal issues relevant to its purpose and strategic direction, and has determined interested parties and their expectations, relevant to its ability to meet customer and regulatory requirements.

Top management is committed to its information security policy that provides the framework for setting the following information security objectives.

The Company is committed to the continual improvement of its information management system through the application of the appropriate requirements of the BS ISO/IEC 27001:The Company recognises the role of information security in ensuring that users have access to the information they require in order to carry out their work. Computer and information systems underpin all the Company's activities and are essential to its operational and administrative functions. Any reduction in the confidentiality, integrity or availability of information could prevent the Company from functioning effectively and efficiently. In addition, the loss or unauthorised disclosure of information has the potential to damage the Company's reputation and cause financial loss. To mitigate these risks, information security must be an integral part of information management, whether the information is held in electronic or hard-copy form.

The Company is committed to protecting the security of its information and information systems in order to ensure that: the integrity of information is maintained, so that it is accurate, up to date and 'fit for purpose'; information is always available to those who need it and there is no disruption to the business of the Company; confidentiality is not breached, so that information is accessed only by those authorised to do so; the Company meets its legal requirements, including those applicable to personal data under the General Data Protection Regulations (GDPR); and the reputation of the Company is safeguarded.

Information security risk assessments should be performed for all information systems on a regular basis in order to identify key information risks and determine the controls required to keep those risks within acceptable limits.

The Company is committed to providing sufficient education and training to users to ensure they understand the importance of information security and, in particular, exercise appropriate care when handling confidential information.

The Company has established and maintains appropriate contacts with interested parties such as other organisations, law enforcement authorities, regulatory bodies, and network and telecommunications operators in respect of its information security policy. Breaches of information security must be recorded and reported to appropriate top management in the Company, who will take action and inform the relevant authorities.

In achieving these objectives, the Information Security Management System operated by the Company is designed to control all aspects of contract review; the provision and control of process and the training of personnel. The system shall be constantly monitored so that improvements in these operations can be identified and implemented.

This policy provides a framework for the management of information security throughout the Company. It applies to all those with access to the Company information systems, including staff, visitors and contractors; any systems attached to the Company's computer or telephone networks and any systems supplied by the Company; all information (data) processed by the Company pursuant to its operational activities, regardless of whether it is processed electronically or in paper (hard copy) form, any communications sent to or from the Company and any Company information (data) held on systems external to the Company's network; all external parties that provide services to the Company in respect of information processing facilities and business activities and principal information assets including the physical locations from which the Company operates.

In carrying out work on a client's behalf, the Company shall proceed in a professional manner and shall control its operations in line with applicable requirements of relevant legislation including, but not limited to:

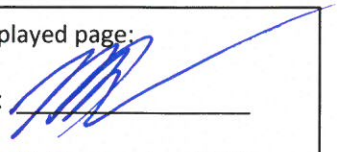
- The Computer Misuse Act (1990)
- General Data Protection Regs.
- The Regulation of Investigatory Powers Act (2000)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000)
- The Freedom of Information Act (2000)

The information security policy is available as documented information, is communicated within the organization and is available to appropriate interested parties, on request. Management shall ensure that this policy statement is implemented, maintained and regularly reviewed.

Mark Simmons

Managing Director
Plasser UK

For the displayed page:

Signature: 

Date: 01/September/2023