Smarttech
YOUR 24/7 SECURITY PARTNER

Information Security Policy

Policy Statement

Smarttech247 recognizes that through the day-to-day operation of its business, we have an impact on our internal and external environment. Also, we ensure that due consideration is given to the potential impact that Information Security aspects may have on the operation of our core processes. As a result, Smarttech247 has established this Information Security Policy Statement, to communicate awareness and understanding of Information Security aspects throughout the business.

Information Security Leadership

Smarttech247 has appointed Raluca Saceanu to develop and implement company initiatives to help us achieve our Information Security goals. Their role will also involve communicating Smarttech247's policies to all interested parties through the delivery of internal presentations and promoting awareness externally as appropriate. Information Security aspects are considered at our regular management meetings and risk assessment meetings.
While Smarttech247 ensures that all personnel consider process related Information Security impacts, we also have identified the following aspects for particular attention:

- Smarttech247 ensures that we meet relevant regulatory requirements and minimise any adverse Information Security effects caused as a result of our activities
- That we raise awareness, provide knowledge and support to employees on Information Security management
- Give training on the importance of protecting business and customer information throughout our business
- Promote an awareness of Information Security objectives
- Regularly review our Information Security practices and policy in accordance with the principles ISO 27001
- Establish performance objectives, targets and management programmes to achieve these
- Smarttech247 is committed to continual improvement of the ISMS

Smarttech247's current business strategy and framework for risk management are the guidelines for identifying, assessing, evaluating and controlling information related risks through establishing and maintaining the information security policy. All risk assessments are carried out with the main objective being to manage the Confidentiality, Integrity and Availability of company information and systems. The detailed arrangements for implementation of this policy and objectives are defined in the relevant TMS documentation, which is available to all interested parties upon request.

Relevant Policies

SMA-TMS 01(b)-3 Statement of Applicability
SMA-TMS 02c-4 Business Continuity Policy
SMA-TMS 05-4 Mobile Device Policy
SMA-TMS 06-1 Health & Safety Statement
SMA-TMS 08-2 Supplier Security Requirements
SMA- TMS 09-2 Media Disposal Policy
SMA- TMS 10-2 Clear Desk Clear Screen
SMA- TMS 11-2 Teleworking Policy
SMA -TMS 12-1 Acceptable Use of Assets
SMA-TMS 13-2 Access Control Policy
SMA-TMS 15-2 Cryptographic Controls
SMA-TMS 16-1 Copyright & Intellectual Property
SMA-TMS 17-2 Physical Security Policy
SMA-TMS 18-2 Data Retention Policy
SMA-TMS 19-2 Data Protection Policy
SMA-TMS 20-2 Website Privacy Policy
SMA-TMS 21-2 Password Policy
SMA-TMS 22-1 Employee Privacy Notice
SMA-TMS 23-2 Information Classification Policy