FEEDBACK FERRET'S ISO27001:2013 ISMS POLICY (V3)

OBJECTIVE

Feedback Ferret's objective of managing information security is to ensure that its core and supporting business operations continue to operate with minimal disruptions and where the business shall ensure that all information that are disbursed or produced have absolute integrity by continuing to meet its compliance obligations under ISO27001 and The General Data Protection Regulations.

Feedback Ferret shall guarantee that all relevant information is managed and stored with appropriate confidentiality procedures and that it has all the necessary technical and organisational measures to protect personal data and ensure its data security.

POLICY

- The purpose of the Policy is to protect the organisation's information assets[1] from all threats, whether internal or external, deliberate or accidental
- The CTO, CEO and Senior Management Board has approved the Information Security Policy
- It is the Policy of the organisation to ensure that:
    - Information should be made available with minimal disruption to staff, clients and the public as required by the business process[2];
    - The integrity of this information will be maintained[3];
    - Confidentiality of information (particularly information protected by means of an MNDA) will be assured [4];
    - Regulatory and legislative requirements will be met (GDPR: Data Protection Act of 2018) [5];
    - A Business Continuity Management Plan will be maintained to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters [6];
    - Information data security awareness training will continue to be made available to all staff [7];
    - All breaches of information security, actual or suspected, will be reported to, and investigated by the relevant authorities not limited to System Administration and Incident Response [8];
    - Appropriate access control will be maintained and information is protected against unauthorized access.
- Policies and Procedures not limited to Information Security will be made available in both hardcopy and online format through an intranet system to support the ISMS Policy.
- Internal Audit Unit has direct responsibility for maintaining the ISMS Policy and involved with writing and/or managing the development of relevant policies, procedures and guidelines not limited to information security.
- It is the responsibility of each member of staff to adhere to the ISMS Policy.
- The availability of information and information systems will be met as required by the core and supporting business operations.

Piers Allington

CEO

Notes:

1 Information takes many forms and includes data stored on computers or servers, transmitted across networks, printed out or written on paper, sent by fax or spoken in conversation and over the telephone.

2 This will ensure that information and vital services are available to users when and where they need them.

3 Safeguarding the accuracy and completeness of information by protecting against unauthorised modification.

4 The protection of valuable or sensitive information from unauthorised disclosure or unavoidable interruptions.

5 This will ensure that the organisation remains compliant to relevant business, national and international laws and it include meeting the requirements stated in legislations such GDPR.

6 Business Continuity Management should be implemented effectively to ensure continuity of business operations in the event of a crisis or disaster.

7 Ensure that relevant and effective trainings are provided to staff.

8 Ensure that the staff understand their roles and responsibilities in handling incidents and have a comprehensive and well-tested incident response plan ready.

The policy will be reviewed annually.