Policy: Information Security

Department: IT

Date: **Approved October 2016** **Review Date:** **January 2018**

1.0 Purpose

This policy affirms that information is an essential asset to 110% Ltd requiring protection against threats which could result in loss of opportunity, financial loss, reputational damage or legal risk.

2.0 Scope

This Policy applies to:

- All approved users of 110% Ltd information including all employees and clients of 110% Ltd, contractors, suppliers, 110% Ltd partners and external researchers who may be authorised access to 110% Ltd information.
- All information created, received or retained in the course of 110% Ltd business which must be protected according to its sensitivity, criticality, and value, regardless of the media on which it is stored or the location of the data. See the Data Protection Policy for further details.
- All locations from which 110% Ltd information is accessed including home and offsite/remote use.

3.0 Principles and Guidelines

The Information Security Policy is in line with the principles & guidelines set out in the industry standard ISO 27001. This will be achieved through the implementation of controls and responsibilities within 110% Ltd in line with the standards.

This includes responsibilities and measures to ensure:

- Information will be protected in line with all relevant 110% Ltd policies and legislation, notably those relating to Data Protection, human rights and Freedom of Information.
- Each information asset 110% Ltd will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.
- Information will be made available solely to those who have a legitimate need for access.
- The integrity of information will be maintained.
- It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.
- Information will be protected against unauthorised access.

- All authorised individuals within 110% Ltd must comply with UK & EU law which applies to Information in all its forms.
- Compliance with the Information Security policy will be enforced.

Regular risk assessments must be carried out to monitor and mitigate against the impact of potential security failures. Such risk assessment should be embedded within normal working practices across all departments (please ask the Data Protection Officer for assistance if you do not have these measures in place).

4.0 Responsibility and Governance

Everyone has a responsibility to make informed decisions to protect confidential or personal information and keep it safe. All staff and clients and other approved users of 110% Ltd information must:

- Demonstrate competence in their understanding of data protection laws and good practice applicable to the performance of their 110% Ltd responsibilities, as described in the policies, procedures and guidelines established to protect information and must seek advice and guidance if in any doubt.
- Report any actual or suspected breach in information security, working practices which may risk information loss or accidental near miss incidents.
- Dispose of physical records containing personal data using the confidential shredding bags.
- Use their own login details to access systems and files. Login details must not be shared. Passwords should be changed periodically and immediately if an individual feels they may have become compromised.
- Ensure records are secure and protected.
- Store data on network drives and servers or secure physical locations on campus. Off-site storage must be approved by the Data Protection Officer following the Off-site Processing procedures

Please contact the Data Protection Officer for advice or guidance on any of the points above. Compliance with this policy is mandatory and non-compliance must be reported to the Data Protection Officer to record the incidence and escalate to the appropriate authority to determine the action to be taken. Non-compliance with this policy is subject to 110% Ltd's disciplinary procedures for staff and clients.

5.0 Monitoring and auditing

This policy and its implementation will be subject to internal monitoring and auditing, and the outcomes from these processes will inform and improve practices as part of a commitment to continual improvement. 110% Ltd will also undertake appropriate benchmarking and external auditing exercises as may be applicable periodically.

6.0 Associated documents

Please refer to:

- ISO 27001 guidelines
- Data Protection Act 1998
- Freedom of Information Policy
- Data Protection Policy

7.0 Review of policy

This policy will be reviewed at least every two years or when there are significant changes to it.

8.0 Contact list for queries related to this policy

Data Protection Officer
Chief Information Officer

9.0 Authority for this policy

Senior Management Team