THE
DIVERSITY TRUST
INFLUENCING SOCIAL CHANGE

Information Security Policy

1. Purpose

The purpose of this document is to define the role that The Diversity Trust CIC's takes in ensuring commitment to information security, the development and propagation of this policy, and the assignment of appropriate information security roles, responsibilities and authorities to protect The Diversity Trust CIC's assets from all relevant threats, whether internal or external, deliberate or accidental. This policy operates in conjunction with the Privacy Policy.

2. Objective

The Diversity Trust CIC, which provides training and consultancy services specialising in Equality, Diversity, Equity and Inclusion, is committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets (information assets include data or other knowledge stored in any format on any system that has value to an organisation, and should be logged) throughout the organisation in order to compete in the marketplace and maintain its legal, regulatory and contractual compliance and commercial image.

To achieve this, The Diversity Trust CIC has implemented an information security management system (ISMS) in accordance with the international standard ISO/IEC 27001:2013 requirements. The ISMS is subject to continual, systematic review and improvement.

3. Roles and responsibilities

- The Board of Directors is responsible for setting and approving the Information Security Policy.
- The Chief Executive Officer (CEO) is responsible for ensuring that roles, responsibilities and authorities are appropriately assigned, maintained and updated as necessary.
- All Employees/Staff

Are responsible for adhering to the requirements of the Information Security Policy and for fulfilling any duties related to assigned roles, responsibilities or authorities. The consequences of breaching the Information Security Policy are set out in The Diversity Trust CIC's disciplinary policy and in contracts and

This document contains material that is distributed under licence from IT Governance Publishing Ltd.

agreements with third parties.

4. Policy objectives

It is the policy of The Diversity Trust CIC that:

- Information is made available to all authorised parties with minimal disruption to the business processes.

Please see our https://www.diversitytrust.org.uk/privacy-policy/

- The integrity of this information is maintained.

Please see our https://www.diversitytrust.org.uk/privacy-policy/

- The confidentiality of information is preserved.

Please see our https://www.diversitytrust.org.uk/wp-content/uploads/2022/06/Confidentiality-Policy.pdf

- The organisation ensures compliance with all legislation, regulations and codes of practice, and all other requirements applicable to its activities.

Please see our https://www.diversitytrust.org.uk/wp-content/uploads/2022/06/CODE-OF-PROFESSIONAL-PRACTICE.pdf

- Appropriate information security objectives are defined and, where practicable, measured using the SMART (Specific, Measurable, Achievable, Realistic and Timed) principles. Objectives are planned and documented, inclusive of how each is to be achieved and actions required. Subsequently, the objectives are regularly monitored and reviewed.

Please see https://www.diversitytrust.org.uk/about-us/

- Appropriate business continuity arrangements are in place to counteract interruptions to business activities and these take account of information security.

- Appropriate information security education, awareness and training is available to staff and relevant others working on the organisation's behalf.

- Breaches of information security or security incidents, actual or suspected, are reported and investigated through appropriate processes.

- Appropriate access control is maintained and information is protected against unauthorised access.

- The organisation maintains a management system that will achieve its objectives and seeks continual

This document contains material that is distributed under licence from IT Governance Publishing Ltd.

improvement in the effectiveness and performance of the management system based on risk.

- The organisation maintains awareness for continual improvement, and the ISMS is regularly reviewed at planned intervals by Senior Management to ensure it remains appropriate and suitable for the business.

This policy is approved by the Board and the Executive Director and is reviewed at regular intervals or upon significant change.

This policy is communicated to all Employees/Staff within The Diversity Trust CIC and is available to customers, suppliers, stakeholders and other interested parties upon request.

Document owner and approval

The Information Security Manager is the owner of this document and is responsible for ensuring that it is implemented. The current version of this document is available to and is published here About Us

Berkeley Wilde, Executive Director

14th June 2022

This document contains material that is distributed under licence from IT Governance Publishing Ltd.