Information Security Policy

Public

May 2024

Digital Catapult Information Security Policy

Purpose

To ensure all employees and relevant subcontractors at Digital Catapult are actively engaged with the Information Security Management System (ISMS) which is designed to protect the confidentiality, integrity and availability of information.

The purpose of the ISMS is to continually assess and manage risk in order to protect the Digital Catapult information assets from all threats whether internal or external, deliberate or accidental.

Terms and Definitions

Information Security Management System - A set of policies, procedures, processes and systems which provide a systematic approach for managing an organisation's information security

Senior Leadership Team Commitment

The Senior Leadership Team is committed to protecting the confidentiality, integrity and availability of information by;

- Ensuring that information security objectives are established and are compatible with the overall strategic direction of digital catapult.
- Ensuring all statutory and regulatory requirements are consistently met.
- Ensuring that interested parties are made aware of any information security incidents and threats where appropriate.
- Ensuring the integration of ISO 27001:2022 requirements into Digital Catapult's processes.
- Ensuring that the resources needed for the ISMS are available.
- Communicating the importance of an effective ISMS and conforming to the ISMS's requirements.
- Ensuring ISMS objectives are monitored, measured and achieved.
- Ensuring all employees & contractors receive basic Information Security training to allow them to contribute to the overall effectiveness of the ISMS.
- Ensuring that regular risk assessments and risk treatments are conducted to facilitate continual improvement
- Promoting continual improvement of the ISMS.
- Supporting managers across Digital Catapult to enable them and their teams to understand and follow ISMS processes within their areas of responsibility.

Employee & Subcontractor Commitment

All employees & subcontractors are required to make a commitment to adhering to the ISMS by;

- Ensuring they are aware and have understood this policy.
- Ensuring they are aware and have understood all information security policies and procedures that apply to them, including those listed in the Employee Handbook.
- Ensuring that they undertake the information security awareness training provided, both on joining the company and at least annually.
- Ensuring they understand their duty to safeguard assets, including locations, hardware, software, systems or information, in their care and to report any suspected breach in security without delay, to the IT team. Staff attending sites that are not occupied by the Organisation must ensure the security of the Organisation’s data and access their systems by taking particular care of laptop and similar computers and of any information on other media that they have in their possession.

Breach of the Information Security policies and procedures by employees or subcontractors may result in disciplinary action, including dismissal.

Signed,
Joe Butler
CTO