Information Security Policy

Document Control			
Document Title		Information Security Policy	
Version	1.1	Author(s)	Gerry Forde
Date Approved	27/10/2017	Document Status	Final
Effective Date	27/01/2017	Approved By	Fintan Healy
Superseded Version	N/A	Date of Next Review	26/10/2018

Introduction

EssentialSkillz provide a hosted Health & Safety training and self assessment system for our customers. As such we recognise the vital importance that robust information security management provides for both our own business and for data we store on behalf of our customers.

This security policy is a component part of the overall set of policies EssentialSkillz have in place to ensure the preservation of data in line with the C-I-A triad:

- confidentiality - ensuring that information is accessible only to those authorised to have access

- integrity - safeguarding the accuracy and completeness of information and processing methods

- availability - ensuring that authorised users have access to information and associated assets when required

Failure to comply with this policy or any of its component policies may subject EssentialSkillz staff to disciplinary action.

Objectives

This *Information Security Policy* sets the direction, gives guidance, and defines requirements for information security processes and actions within EssentialSkillz which all staff must adhere to.

The primary objectives are to:

- meet all regulatory requirements including but not limited to GDPR
- effectively manage the risk of exposure or compromise to EssentialSkillz resources
- communicate the responsibilities of EssentialSkillz staff for the protection of information
- establish a secure and resilient processing environment
- provide security controls for internally developed software to protect unauthorized access, tampering or programming errors
- provide a formal incident management process
- promote and increase the awareness of information security

Definitions

- *authorisation* - the function of establishing an individual's privilege levels to access and/or handle information.
- *unauthorised access* - looking up, reviewing, copying, modifying, deleting, analyzing or handling information without proper authorisation and legitimate business need.
- *EssentialSkillz Information* – information that EssentialSkillz collects, possesses or has access to regardless of its source. This includes information contained in hard copy documents or other media, communicated over voice or data networks, or exchanged in conversation.

Scope

This policy is applicable to EssentialSkillz full time and temporary employees, third party contractors and consultants (hereafter referred to as "Staff"). The Security Steering Group (hereafter referred to as "SSG") is fully committed to information security and agrees that all staff or any other person working on behalf of EssentialSkillz has important responsibilities to continuously maintain the security and privacy of company data.

This Information Security Policy encompasses all systems, automated and manual, for which EssentialSkillz has administrative responsibility, including systems managed or hosted by third parties on behalf of the company. This policy applies to information in all forms, including but not limited to paper and electronic formats, created or used in support of business activities of the company. This policy must be communicated to all staff that have access to or manage company information.

Additional specific policies published by EssentialSkillz, which are associated with this policy, provide specific details for compliance with this *Information Security Policy*. Published policies reflect current practices and will be periodically reviewed and updated as necessary to meet changes in business needs, regulations, or changes in technology implemented or supported by EssentialSkillz.

Responsibilities

Management have created a Security Steering Group (SSG) and appointed a Data Security Officer (DSO) to implement this *Information Security Policy*.

The SSG is the owner of this policy with responsibility to promote information security through adoption of policies, standards, and guidelines. The SSG develops strategies for implementing and evaluating the effectiveness of information security. The SSG, with advice from the IT department, has responsibility for recommending security policies and guidelines and making available best practices to other teams within the business.

It is the responsibility of the DSO to oversee the implementation of this *Information Security Policy* which establishes and monitors the effectiveness of information security, standards and controls within EssentialSkillz. The DSO may also perform periodic reviews of company security for compliance with this and other security policies and standards.

Component Policies

The component policies of this *Information Security Policy* include:

- Information Classification Policy
- Data Protection Policy
- Acceptable Usage Policy
- Privacy Policy
- Data Breach Policy
- Business Continuity Policy
- Disaster Recovery Policy
- Physical and Environmental Security Policy

These policies are managed by the DSO and reviewed by the SSG before submission for approval by our Chief Operations Officer.

Company Statement

EssentialSkillz is committed to working towards the establishment of a robust Information Security Management System (ISMS) that maps to ISO 27001.

Continual Improvement

In this regard, we are committed to continual improvement of Information Security at EssentialSkillz and will continue to put in place policies and safeguards to further enhance the robust approach to Information and Data security within our business.