Information Security Policy

Document Reference:	Information Security Policy - 1.5
Confidentiality Level:	External
Document Owner:	Data Security Officer
Version:	1.5
Date of Version:	03/11/2022
Replaces Version:	1.4
Document Author:	Gerry Forde
Approved by:	Fintan Healy
Date of Approval:	27/10/2017
Reviewed by:	Liam Carolan
Next Review date:	03/11/2023

Revision History

Version	Date	Revision Author	Summary of Changes
1.2	27/01/2017	Gerry Forde	Published V1.2
1.3	07/09/2020	Jack Rawlings	Moved to new template and updated
1.4	18/08/2021	Liam Carolan	Update for clarity in 4.0

Distribution

Location/Holders	Updated/Notified by
Live Documents Drive	Data Security Officer
Update on Internal Training	General Manager
EssentialSkillz Website	Data Security Officer

Approval

Name:	Fintan Healy
Role:	Chief Operations Officer
Signature:	*Fintan Healy*
Date:	27/10/2017

Table of Contents

1.0 Introduction

EssentialSkillz provides 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.

1.1 Purpose

This document defines EssentialSkillz policy on Information Security, and will thus provide a framework on which company policies, procedures and operations will be based.

1.2 Scope

This policy applies to:

- All staff, contractors and third parties involved in processing EssentialSkillz information
- All information assets owned or managed by the organisation
- Access rights and controls to information
- Security of services and information systems
- Business continuity and disaster recovery of information
- Appropriate controls to meet regulatory, legislative and contractual requirements
- Framework for third parties and Essentialskillz staff to adhere to
- Promotion of security and guidance and advice where appropriate
- Processes to deal with security breaches

1.3 Users

Users of this document are all employees of EssentialSkillz. It is an *External* facing document and may be shared with clients and other external bodies.

It will also be available publicly on www.essentialskillz.com

2.0 Reference Documents and Resources

- No linked documents

3.0 Information Security Policy

This policy is applicable to EssentialSkillz full time and temporary employees, third party contractors and consultants (hereafter referred to as "Staff"). Management 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 and our Information Security Management System (ISMS) 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 and 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 and our ISMS. 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.

EssentialSkillz is committed to working towards the establishment of a robust Information Security Management System (ISMS) that maps to ISO 27001. Our policy framework is currently certified IASME Governance (self-assessed).

We are also committed to the 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

3.1 CIA Triad

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

3.2 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

3.3 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.

4.0 Responsibilities

Ultimate responsibility for the execution of this policy rests with the Head of Operation and the Data Security Officer.

The Head of Operations, assisted by the Data Security Officer, is responsible for the production and maintenance of:

- EssentialSkillz security policies;
- Controls to enforce these policies;
- Guidance on the implementation and maintenance of these controls.

All breaches of information security will be reported to the Data Security Officer, and will be investigated by appropriate staff.

It is the responsibility of all staff, contractors and visitors to adhere to this policy and all EssentialSkillz policies, procedures and statements. Failure to comply with this policy, the policies that constitute our ISMS, or other policies (eg health and safety, human resources) could lead to disciplinary procedures.

Management and Team Leads are responsible for implementing the policy within their areas of responsibility, and for ensuring the adherence of their reporting staff to the policy.

EssentialSkillz reserves the right to inspect any data stored on its computer or telecommunication systems, or transmitted or received via the organisation's networks, in the course of investigating security incidents, or safeguarding against security threats.

4.1 Responsibility Ownership overview

Responsibility	**Owner**
Execution and Sponsorship of this policy.	Head of Operations
Production, maintenance, controls and guidance of this policy.	Data Security Officer
Protection of information systems and assurance that security processes and controls have been carried out.	Information system owner (Head of Department managing the system)
Initiation, coordination and investigation of potential breaches in policy.	Data Security Officer
Ensuring staff have an awareness of and put appropriate controls in place to adhere to the policy.	Management and Team Leads

Provide advice, guidance, training and support on information security.	Data Security Officer
Adherence to policies and procedures.	All staff, contractors and visitors

5.0 Validity and Document Evaluation

This document is valid as of 07/09/2020.

The owner of this document is the *Chief Operations Officer* who must review and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Significant changes in:
    - Work processes
    - Organisational structure
    - Relevant Legislation or Standards
    - Contractual Obligations
- Shortcomings or gaps in policy implementation and maintenance
- Lack of clarity regarding responsibilities for ISMS implementation
- Results of Information Security Audits, both internal and external