Controls of Outsourced Process

Conforms to ISO 27001:2013

Document Ref.	Doc
Current Version:	1
Previous Version:	-
Dated:	1st February 2022
Document Author:	ISMS Manager
Document Owner:	ISMS Manager

Table of Contents

For internal use only

1. Introduction

1.1 Purpose

The purpose here is protection of the organization's valuable information and assets that are accessible to or affected by suppliers.

1.2 Scope

This procedure sets out how TrusTrace identifies, and controls outsourced processes that may pose a threat to our information security.

1.3 The Issue Status

The issue status is indicated by the version number in the footer of this document. It identifies the issue
status of this document.

When any part of this document is amended, a record is made in the Amendment Log shown below.
The Manual can be fully revised and re-issued at the discretion of the Management Team. Please
note that this Manual is only valid on the day of printing.

Issue	Amendment	Date	Initials	Authorized
1	Initial Issue	02/01/2022		ISMS Manager

3

2. Controls of Outsourced Process

We ensure that outsourced processes that may pose a threat to the information security of our business are properly identified and controlled.

An **ISMS Outsourced Process Register** is maintained by the ISMS/HR Manager
When a proposal is made to outsource a new process, which may have implications for information security, the responsible manager informs the ISMS Manager and discusses the need for any information security related controls.

The ISMS Manager determines if the proposed outsourcing poses any threat to information security and, where a threat is identified, an agreement is reached between the responsible manager and the ISMS Manager on the controls to be implemented.

The ISMS Manager ensures that the new agreement is recorded on the **ISMS Outsourced Process Register**.

The responsible manager ensures that the agreed controls are implemented and maintained.

Note that the need for placing information security controls on an outsourced process, may also be identified during internal / external audits.