HIGH TABLE

How to Deploy and Implement Policies

How to go about implementing the policy pack

Document Version Control

	Last Modified	Last Modified by	Document Changes
1	8 January 2021	HIGH TABLE	Document first created
2	30 June 2021	HIGH TABLE	Cosmetic Changes

Document Contents Page

Introduction

Welcome to the policy pack. This document is to act as a guide when deploying the policies. It is not a substitute for real world experience. The guide is based on need and the need is based on your business. If you understand your business, you are in a great position.

When developing policies, we would in the normal course of events produce them as part of a structured process. The first step being to develop the Context of Business. This is not covered in this document, but it is assumed, that to a greater or lesser or extent, you have completed that step.

If you have purchased a stand alone policy, this document still applies, but you should consider the heavily discounted Policy Pack of all 26 required policies for ISO 27001 - https://hightable.io/product/iso-27001-policy-template-pack/

It is going to save you over 90 hours of research and writing.

If you ever have any questions, you can reach out to Stuart on LinkedIn: https://www.linkedin.com/in/stuartabarker/

Now, lets look at how we deploy these policies…

Building Your Policy Pack

Creating a folder on your file storage drive called policies is a great place to start. We would advocate at this stage a sub folder for each version and iteration of signed off policies. For now, create your base folder and copy the templates to there. You will always have the foundation and something to come back to.

What are Policies?

Policies are statements of what you do. They are not how you do it. How you do it is covered in the process documents of the business. We would advise maintaining this logical separation.

Confusing policies and processes into one document will add complexity such as when asked to share your policies with third parties. Sharing documents that contain potentially staff contact details or propriety process steps is not advised if it can be avoided. Keep them logically separate.

What are these policies?

These policies are what good looks like. There is nothing in here that you should not be able to do as a business. Remember it is not saying how you do it. This is best practice based on industry standard and ISO 27001.

They are your starting point. You are going to review each policy for what it says that you do and check that you either can or will do it. If you cannot or will not, then you have work to do to understand the changes required to the policy. It is not unreasonable to change them. That is the art of the implementation.

Variables to Change.

There are variables within the policies that either require your attention, a change, an acceptance, or some information.

Light Blue Text

Whilst all text should be considered for review, text that is in **LIGHT BLUE** denotes that you have action to take or something to do. This text maybe an example, an instruction or text that requires you to confirm you do it. This is **LIGHT BLUE** to draw your attention. Once you have made your change, added your information or to accept the text, set the text to BLACK.

There should be no **LIGHT BLUE** text in a document when the time comes to sign off and release it.

[Text in Brackets]

[Text in Brackets] often refers to a place holder that requires your actual information. They are self explanatory. Make the change and remove the brackets so the text flows.

Which Policies Do I Actually Need?

Potentially all of them. Remembering that these are information security policies. They rely on other company policies to satisfy the requirements of an effective ISMS. Most notably would be your HR policies and documents such as Company Handbook, Grievance Policy and more.

If you have a GDPR or Data Protection implementation already you are not going to need the Data Protection Policy and Data Retention Policy.

The policies are modular to meet the requirements of many standards. To meet those standards, you may need tweaks. They fully satisfy ISO 27001 and the foundation of any good ISMS.

As discussed, the policies are based on the Context of Organisation. Specifically, the statement of applicability will be a guide. If you do not have one, have not completed a Context of Organisation or this concept is alien to you then the simple approach is to look at each policy and ask your self – does this look like it applies here?

Let us take the Secure Development Policy as an example. If you do not do Secure Development, then it is unlikely this policy is needed for you.

The Process

- tweak your policies to meet the needs of the business.
- share them for review and update as needed.
- set the version control for a stable version.
- hold a Management Review Team Meeting and record in the minutes that you reviewed and approved the Policies with a list of the policies and versions in the minutes.
- make the policies available.
- communicate that the new version of policies is available, where they are and direct people to read them.
- include them in your communication plan and training plan for the year.
- review them annually or after a significant change and repeat the process.

Before You Sign Off or Make Live – Checklist

- Is all the guidance text and text in **Light Blue** now updated and turned to black text?
- Have you updated all the [Text in Brackets] and removed the Brackets?
- Have you set the Last Review date to the date of the Management Review Meeting that signed the policies off?
- Have you update the document version control to the correct version number, with the changes that you have made, the author and the date?
- Have you checked Header and Footers and set Document Owners, Version Numbers and Classification?

- Does the Version Number in the Header match the Version Number in the Document Version Control Table?

How Often Should Policies be Updated, Review and Re-Issued?

At least annually within a 12-month period. Or when a significant change occurs.

How Policies Fail Audits – Shooting Fish in a Barrel

The first thing any auditor is going to do is look at the document mark up. 99 times out of 100 hundred this is wrong in some way. It is an easy win.

What is the Version number of the document? Is it the same in the header and footer and document version control?

When was the document last signed off? Was it within the last year?

Does the document have an owner, and do they still work here if a named person?

GOOD LUCK WITH YOUR IMPLEMENTATION

Remember to check out the policy bundle for all other polices:

https://hightable.io/product/iso-27001-policy-template-pack/