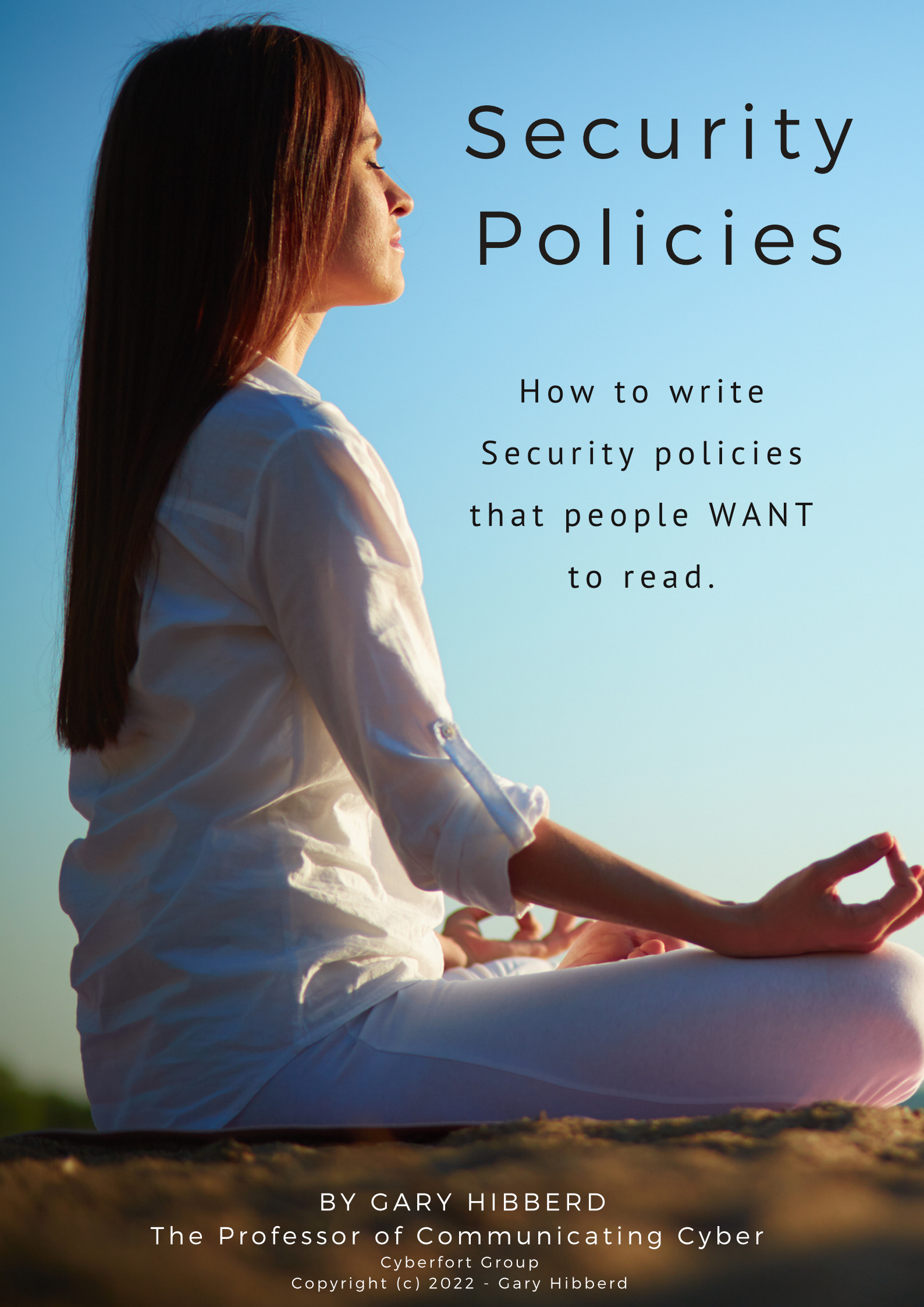


Security Policies

How to write Security policies that people WANT to read.

BY GARY HIBBERD
The Professor of Communicating Cyber
Cyberfort Group

WHO SHOULD READ THIS GUIDE?

Anyone who has struggled with writing an information security policy.

Anyone who isn't sure what is (and is not) mandatory for ISO27001:2013 and ISO27001:2022

Anyone looking for permission to do something different!

INTRODUCTION

ISO27001 POLICIES THAT WORK

Writing Information security policies is not easy, yet it's fundamentally crucial to standards like ISO27001.

The first requirement of both ISO27001:2013 and ISO27002:2022 is *"Policies for Information Security."*

But the number one issue I have (as a consultant) is seeing so many poorly written policies.

Often overly complicated, containing page after page of impenetrable blocks of text.

I want to offer this guide to help you develop policies you can be proud of.

Policies that have an impact!

Ready to get started?

GARY HIBBERD - The Professor of Communicating Cyber

Did you know...

No standard on earth said your policies need to be boring!

LETS GET STARTED

ISO27001 POLICIES THAT WORK

Information Security Policies are critical, and when it comes to ISO27001, some policies are considered mandatory. I.e. you must have a documented policy.

But no one said they had to be complicated, boring and bland.

How did we get here?

Often policies are written by lawyers and policymakers. , But Policymakers tend to be lawyers, Consultants and companies selling policy packs.

Therefore 'bigger = better', right?

Wrong!

As the statistician and economist E.F Schumacher CBE once said;

“Any intelligent fool can make things bigger, more complex, and more violent. It takes a touch of genius and a lot of courage to move in the opposite direction."

Did you know...

There are only **9** policies mandated in ISO27001:2013

MANDATED POLICIES

WHERE 'POLICY' IS CLEARLY STATED AS A REQUIREMENT IN ISO27001:2013

- Information Security 5.2
- A11.2.9 Clear Desk & Screen
- Mobile (&BYOD) A6.2.1
- A15.1.1 Supplier Relationships
- Teleworking A6.2.2
- A9.1.1 Access Control
- Backup A12.3.1
- A10.1.1 Cryptographic Control
- Key Management A10.1.2

GARY HIBBERD - The Professor of Communicating Cyber

WHAT IS A POLICY?

ISO27001 POLICIES THAT WORK

In ISO27001, a policy is defined as *"Intentions and direction of an organisation, as formally expressed by its top management"*

In short;

- Policies are based on fact.
- Policies are not a statement of future aspirations.
- Policies are not procedures.
- Policies are not guidance.
- Policies should be easy to understand

GARY HIBBERD - The Professor of Communicating Cyber

How to write a policy that provides peace of mind

HOW TO WRITE A POLICY

ISO27001 POLICIES THAT WORK

1 Start with the end in mind.

What behaviour are you trying to encourage? Think carefully about why you're writing this policy and what you want from the reader, and what you expect of them.

Think about who you are speaking to and who is speaking. Consider the following and tell me which you feel is more personal and influencing;

"We expect that all our employees apply security controls as required by their role."

Or

"We expect you to apply these controls as required by your role."

The first is rather corporate and speaks to the many, while the second talks to me personally and is far more engaging.

GARY HIBBERD - The Professor of Communicating Cyber

2 Mind your language.

Write policies that sound like they came from you and write as you speak. One of my favourite compliments is when someone says that they can hear my voice as they read my words (depending on your views, this could be a blessing or curse!)

If you're part of a large organisation, then consider the culture. Are you heavily regulated or highly creative? What are your values? If you are fun, creative and outgoing, then write your policies in the same way.

You can reduce word count and make policies less formal by replacing terms such as "should not" with "shouldn't" and "cannot" with "can't". Again, this may not be in line with how you speak – if not, you shouldn't do it!

HOW TO WRITE A POLICY

ISO27001 POLICIES THAT WORK

3 Use simple words & sentence structure.

Continuing this theme, don't overcomplicate things.

Don't use acronyms and jargon – even if you think everyone should know what you're talking about. Write it as if a five-year-old needs to understand it.

Keep sentences and paragraphs down to a single principle or idea, but don't overdo it! You will begin to sound like a robot and distant from your readers.

Consider the point made above and write as you speak. Where you use short sentences, you can still link these sentences together by using 'but' and 'and' to connect ideas and concepts.

If the message is relatively complex, consider sub-headings, charts, or bullet lists to get your message across.

HOW TO WRITE A POLICY

ISO27001 POLICIES THAT WORK

4 Make every word count.

Every word must fight for its place on the page. This is not a time for fluff and 'padding'. It should not be challenging to have a PoaP – Policy on a Page. If your policy is more than a page, ask why and start editing mercilessly.

ISO27001 mandates that you have a policy. ISO27002 provides guidance on what you should consider, but it does not tell you what must be included. Importantly, it does not state how long that policy must be.

Remember that ISO27001 does not require your policies to be dull, boring, or bland!

Be creative and make them a thing of beauty! Use graphics, emojis, images, diagrams, infographics, quotes, sayings, and examples to bring your policies to life. Just don't overdo it and use ALL these things at once!😂

Be sensitive to your organisation's culture, but why not create something that people want and enjoy reading?

GARY HIBBERD - The Professor of Communicating Cyber

Did you know...

It's possible to get 9 policies into 3 pages.

(Don't believe me? See the example provided)

OUR INFORMATION SECURITY PRINCIPLES

WE CARE ABOUT PRIVACY AND DATA PROTECTION.

At [Your company name], we understand that Information Security and Data Protection are important, but can often be confusing. This is why we have written these policies to help you understand what we expect of you.

Depending on your role, you will come into contact with client, employee and shareholder data and information, and we all have a duty of care in protecting it appropriately. This is why we have established clear objectives around these topics;

- **Confidentiality**– We have put in place technical & operational controls to protect data
- **Integrity** – We ensure that we comply with legal and contractual requirements
- **Availability** – We will prevent data from accidental or deliberate loss or destruction

We know you are committed to protecting the rights and freedoms of data subjects, so please read these policies, rules and supporting principles carefully.

If you have any questions, please speak to your line manager.

Thank you, and I appreciate your commitment.

Signed: [HEAD OF THE ORG] – Top Management

OUR INFORMATION SECURITY PRINCIPLES

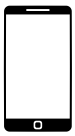
WE CARE ABOUT PRIVACY AND DATA PROTECTION.

Access control policy

To ensure you have access to the information you need, access to systems and locations is based on your role. Our user registration and de-registration process includes the provision of unique user names, password controls and multi-factor authentication. (MFA) If you require access to additional systems and services, then you must follow these processes

Information transfer policy

You should adhere to our Classification scheme and ensure appropriate controls are used when transferring information. You should always carefully consider; Why I am sending this data and how can I protect it?



Mobile device policy

We have implemented technical security controls to protect the mobile devices that we have provided to you. These include enabling encryption, anti-virus protection, and password controls. It is your responsibility to ensure devices are stored securely and device updates are implemented promptly.

Backup policy

To ensure Data is always available, our policy is to employ the '321' principle of backing up data; 3 copies of data, on two different mediums, with 1 held offsite. To safeguard Data, you must store all company-related data on drives provided, not on local drives, as these will not be included in the backup process. We will also periodically test our backup processes to ensure they are working correctly.

Supplier management policy (including Cloud services)

Where suppliers have technical or physical access to our data, we will ensure appropriate due diligence takes place. We will also ensure contracts containing Confidentiality and Non-Disclosure Agreements (NDAs) have been established and periodic monitoring and reviews of Contracts and the Suppliers are undertaken

.

OUR INFORMATION SECURITY PRINCIPLES

WE CARE ABOUT PRIVACY AND DATA PROTECTION.

Fair use policy (also known as 'Acceptable use')

We want to equip you with the right tools and environment so you can do a great job! Remember, you have a duty of care and responsibility for using physical assets like mobile devices and laptops to data and software (like the internet and email). We expect you to act professionally and diligently at all times in the use of the assets and systems we provide. Further guidance and procedures to enable this are available.

Clear desk & clear screen policy

Ensure that work areas are clear of confidential data when left for an extended period. Physical documents must be secured appropriately to reduce the risk of accidental disclosure, loss or destruction. Computers and mobile devices have been configured to 'auto-lock' after inactivity. Still, you are encouraged to get into locking your machine when left unattended.

Cryptographic & key management

We encrypt data using the latest cryptographic tools available for storage and transmission. Managing the electronic keys for cryptography rests with our IT team, and all cryptographic controls are used in line with national and international laws.

Management of our policies

We trust you to work in the best interests of our business and respect the data that you come into contact with. Where there are any violations of our policies these may be treated as a matter of misconduct.

All our policies are reviewed on an annual basis.

CONCLUSION

ISO27001 POLICIES THAT WORK

They say that the secret to making great food is to have fun while you do it. The same can be said for policies.

If you hate the process and struggle to put them together, it will come through on the page. If you find them painful to write, imagine what the person reading them feels!

Have fun with them and be creative. I genuinely enjoy writing policies and procedures.

My challenge to you is to ask you to do the same. If you can't, then get in touch, and I'll show you how!

Gary Hibberd - LinkedIn
0744 7911 742


Good luck!