Cyber security culture principles

How to create the right cultural conditions in an organisation that support and encourage people to carry out the desired cyber security behaviours.

Context to this guidance

Research shows that any efforts to improve the cyber security of an organisation will only ever be effective if they are supported by a culture that encourages and enables this improvement. An organisation's culture influences how cyber security is approached, for example how decisions are made, how incidents are managed and people's attitudes towards it.

The organisation's leaders have a vital role to play in setting the tone for their organisation's culture. While some goals can be achieved by the cyber security team, significant and sustained impact needs leadership buy-in and advocacy

Who is it for?

These principles are designed to support both an organisation's leaders and cyber security specialists in creating the right cultural conditions to enable their people to carry out the right security behaviours.

What do we mean by cyber security culture?

While there are many definitions of cyber security culture, we are using the following for this guidance:

> *Cyber security culture is the collective understanding of what is normal and valued in the workplace with respect to cyber security. It sets expectations on behaviour and relationships, influencing people's ability for collaboration, trust, and learning.*

How to use these principles

Applying the following principles will help you create the best conditions for an organisation's cyber security by developing a culture where secure behaviours are valued and people feel safe to engage with it. This will help you build a workforce that is **both** high-performing and cyber secure.

But note, every organisation is unique and its journey to a healthy cyber security culture will also be unique. There is no one-size-fits-all approach to developing a good cyber security culture. These principles describe the desirable end-states found in healthy cultures rather than offer a prescriptive 'how-to' guide to getting there.

If your organisation already has a security culture programme in place, these principles will help you identify any cultural barriers that might be reducing its effectiveness, as well as suggesting new opportunities for intervention.

If you are looking for external tools and consultants to help you develop your cyber security culture, these principles can help you frame your requirements.

As you consult these principles, we recommend you also consider using the National Protective Security Authority's (NPSA) free Security Culture Tool to help you assess and better understand the current shape of your organisation's security culture, and identify how you might improve it.

Each principle is accompanied by:

- a brief description of the principle
- descriptions of what good looks like, helping you determine the best way to apply the principle within your organisation

- some suggestions for how you could implement the principle

In the 'Principles in practice' section is a set of scenarios designed to show how poor security outcomes can arise from certain kinds of work culture, and how applying the principles can help prevent this.

Finally, in 'The cyber security culture iceberg' section you will find an infographic which provides a handy visual aid demonstrating how applying the 6 principles promotes the behaviours seen in a healthy cyber security culture.

PUBLISHED

4 June 2025

REVIEWED

4 June 2025

VERSION

1.0

WRITTEN FOR

Large organisations

Cyber security professionals

Public sector

Small & medium sized organisations