Cyber security culture principles

by the NCSC-UK

16.10.2025

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.

Source: NCSC-UK
https://www.ncsc.gov.uk/collection/cyber-security-culture-principles

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.*

The Principles

1. Frame cyber security as an enabler, supporting the organisation to achieve its goals
2. Build the safety, trust and processes to encourage openness around security
3. Embrace change to manage new threats and use new opportunities to improve resilience
4. The organisation's social norms promote secure behaviours
5. Leaders take responsibility for the impact they have on security culture
6. Provide well-maintained cyber security rules and guidelines, which are accessible and easy to understand

Principle 1. Frame cyber security as an enabler, supporting the organisation to achieve its goals

What good looks like

- People in the organisation know the important role cyber security plays in keeping their vital technology functioning, and their important information confidential and available.
- People know how their own secure behaviours contribute to achieving the shared purpose.
- People don't see your cyber security policies and processes as barriers to doing their jobs.
- The people who design and implement cyber security controls are fully aware of how they impact on people's ways of working, and proactively engage to reduce any negative impact.

Suggestions for implementation

- Create and define a clearly articulated and well-understood shared purpose.
- Describe in internal communications how cyber security activities help to achieve the shared purpose.
- Demonstrate that your senior leaders are firm advocates for the cyber security activities which help achieve the shared purpose.
- Ensure that your formal and informal reward mechanisms align with the shared purpose.

Principle 2. Build the safety, trust and processes to encourage openness around security

What good looks like

- The organisation is committed to building a psychologically safe environment where people feel willing, able and supported to speak openly about cyber security.
- There are quick, easy and accessible routes for people to ask questions or report security issues.
- Incidents are investigated with a view to learn and improve, not to blame.
- People involved in an incident are treated fairly, with no punishment for innocent mistakes.

Suggestions for implementation

- Review and enhance your mechanisms for reporting cyber security issues and incidents, to encourage engagement.
- Follow up with reporters to thank them and provide feedback on any action taken.
- Review and improve mechanisms for providing timely cyber security help and support.
- Ensure incident investigations are conducted in a transparent and fair manner, focusing on what went wrong and avoiding blame.
- Share information about the lessons learned and resulting improvements made.

Principle 3. Embrace change to manage new threats and use new opportunities to improve resilience

What good looks like

- The organisation's culture is positive about change, seeing it as a route to improve organisational outcomes – including security resilience.
- Decisions about change are well-considered and only implemented when necessary, to reduce change fatigue and disruption.
- People feel supported to cope with change and confident that responsibility for new risks goes to those best equipped to manage it.

Suggestions for implementation

- Put routine mechanisms in place to identify emerging risks and opportunities for improvement to organisational resilience.
- Bring together all stakeholders to discuss options and agree appropriate change and approaches.
- Enable decisions about risks to be made quickly and to be managed at the appropriate level by the most appropriate people.

Principle 4. The organisation's social norms promote secure behaviours

What good looks like

- You have identified the social norms (desirable and undesirable) associated with cyber security in your organisation.
- You have worked out how to ensure the social norms work in tandem with your security policies.

Suggestions for implementation

- Be open and proactive in engaging with people and data to understand which cyber security policies and practices don't work for the organisation – and the reasons behind this.
- Where non-adherence to security stems from desirable social norms (such as politeness or efficiency) then consider implementing alternative security controls that don't conflict with the norm.
- If undesirable social norms are resulting in people ignoring security rules then focus on ways to disrupt the underlying drivers. This could be achieved through rewards and incentives or by influencing key role models.

Principle 5. Leaders take responsibility for the impact they have on security culture

What good looks like

The organisation's leaders:

- role model secure behaviours
- understand how cyber security enables their particular business area and communicate this to their staff
- promote psychological safety and a learning culture through their actions and words
- use rewards and other incentives to positively encourage secure behaviours and remove incentives that drive poor security behaviours

Suggestions for implementation

- Ensure that leaders have up to date knowledge about security policies and can help their teams find the information they need.
- Support leaders in 'going first' with sharing experiences of past security mistakes or challenges, and how they went about rectifying them, before working with their teams to identify ways they can collectively improve security in their area.

Principle 6. Provide well-maintained cyber security rules and guidelines, which are accessible and easy to understand

What good looks like

- You have tested every cyber security rule to ensure it makes a meaningful contribution to the security of the organisation, is usable and accessible by everyone, and aligns with the shared purpose.
- Your cyber security rules and guidelines are designed for inclusivity, are easy to find and access, and are included in onboarding materials.
- People understand the difference between the rules that must be followed and the guidelines that provide advice.
- You invite and use people’s feedback to continue to refine and improve your security rules.
- You widely communicate any changes to rules and ensure out of date material is archived to avoid confusion.

Suggestions for implementation

- Review all existing security rules and establish a process to ensure all new rules contribute meaningfully to the organisation and align with its shared purpose.
- Form a stakeholder engagement group that represents the entire organisation to assist in developing cyber security rules, ensuring people understand them, and evaluating their impact on various teams' workflows.
- Implement feedback mechanisms as part of a continuous learning strategy.
- Ensure there is a robust process to update rules and guidelines, archive old versions, and effectively communicate the updates to everyone they impact.

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.

https://www.ncsc.gov.uk/collection/cyber-security-culture-principles


CYBER SECURITY
CULTURE PRINCIPLES