Secure by Default

# Secure by Default

We believe that technology should be Secure by Default. This means embedding security from inception, so that it is intrinsic and as transparent as possible.

h/t <https://www.ncsc.gov.uk/articles/secure-default>

## Good technical design is security design

Secure by Default takes a holistic approach to solving security problems. Security is treated as a core fundamental rather than a followup activity.

Embedding security within a design is directly comparable to good modern technical designs and fundementally ensuring the 'thing' actually works.

## Secure by Default

The [National Cyber Security Centre (NCSC)](https://www.ncsc.gov.uk) describe the Secure by Default principles as:

* security should be built into products from the beginning, it can't be added in later;
* security should be added to treat the root cause of a problem, not its symptoms;
* security is never a goal in and of itself, it is a process - and it must continue throughout the lifetime of the product;
* security should never compromise usability - products need to be secure enough, then maximise usability;
* security should not require extensive configuration to work, and should just work reliably where implemented;
* security should constantly evolve to meet and defeat the latest threats - new security features should take longer to defeat than they take to build;
* security through obscurity should be avoided;
* security should not require specific technical understanding or non-obvious behaviour from the user.

### Context is important

The principles above can generally be applied in most scenarios however interpretation and applicability in context can vary - the Ministry of Justice (MoJ) Cybersecurity team are here to help and advise.

NCSC also have a set of whitepapers which help explain some approaches to building products which align with these principles (and they add to them over time):

* [Building a secure feature-rich computing platform](https://www.ncsc.gov.uk/articles/secure-default-platforms), such as a smartphone.
* [Storing sensitive data on consumer platforms](https://www.ncsc.gov.uk/articles/sensitive-data-consumer-platforms)