Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Essential Eight Explained

First published: February 2017
Last updated: May 2023

Introduction

The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies, in the form of the *Strategies to Mitigate Cyber Security Incidents*, to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are the Essential Eight.

The Essential Eight has been designed to protect Microsoft Windows-based internet-connected networks. While the principles behind the Essential Eight may be applied to cloud services and enterprise mobility, or other operating systems, it was not primarily designed for such purposes and alternative mitigation strategies may be more appropriate to mitigate unique cyber threats to these environments.

The Essential Eight

The mitigation strategies that constitute the Essential Eight are:

- application control
- patch applications
- configure Microsoft Office macro settings
- user application hardening
- restrict administrative privileges
- patch operating systems
- multi-factor authentication
- regular backups.

Implementing the Essential Eight

The *Essential Eight Maturity Model* articulates requirements for the implementation of the Essential Eight.

Assessing implementations of the Essential Eight

Assessments against the Essential Eight should be conducted using the *Essential Eight Assessment Process Guide*.

Further information

Further information on the *Essential Eight Maturity Model* and its implementation is available in the *Essential Eight Maturity Model FAQ* publication.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).