Australian Government
Australian Signals Directorate

Essential Eight Explained

First published: February 2017
Last updated: November 2023

Introduction

The Australian Signals Directorate (ASD) 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 organisations' internet-connected information technology networks. While the principles behind the Essential Eight may be applied to enterprise mobility and operational technology networks, it was not designed for such purposes and alternative mitigation strategies may be more appropriate to defend against unique cyber threats to these environments.

The *Essential Eight Maturity Model*, first published in June 2017 and updated regularly, supports the implementation of the Essential Eight. It is based on ASD's experience in producing cyber threat intelligence, responding to cyber security incidents, conducting penetration testing and assisting organisations to implement the Essential Eight.

The Essential Eight

The mitigation strategies that constitute the Essential Eight are:

- patch applications
- patch operating systems
- multi-factor authentication
- restrict administrative privileges
- application control
- restrict Microsoft Office macros
- user application hardening
- 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).