Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Cyber Security Principles (Initial Draft)

JANUARY 2019

Introduction

The purpose of this document is to articulate the foundational principles that must be applied by organisations to protect their information and systems from cyber threats. While there are other standards and guidelines designed to protect information and systems, the advice in this document is based on the experience of the Australian Cyber Security Centre (ACSC) and the Australian Signals Directorate (ASD).

The principles

- Cyber security leadership within organisations is provided by a Chief Information Security Officer (CISO).
- Cyber security risks are identified, managed and accepted before systems are used in production environments.
- Measures are implemented to detect and respond to cyber threats and cyber security incidents.
- Only trusted suppliers are used to deliver and support information and communications technology services.
- Unauthorised access to systems, supporting infrastructure and facilities is restricted.
- Only trusted and vetted personnel are granted access to systems.
- Personnel are educated and trained in cyber security matters.
- Sensitive information is removed from ICT equipment and media before disposal.
- Only trusted, and vendor-supported, applications are allowed to execute on systems.
- Applications and services are configured in a secure manner to reduce their attack surface.
- Personnel are granted the minimum access to information, applications and systems required for their duties.
- Multiple methods are used to identify and authenticate personnel to systems and important data repositories.
- Applications and systems are administrated in a secure and accountable manner.
- Security vulnerabilities in applications and systems are patched in a timely manner.
- Important information is backed up in a secure and resilient manner on a regular basis.
- Applications, services and systems are designed, developed and deployed using secure practices.
- Sensitive information is encrypted at rest and in transit between different systems.
- Information transferred between different systems is done so in a controlled and auditable manner.

Further information

These principles are supported by the cyber security guidelines within the ***Australian Government Information Security Manual*** (ISM). The ISM and supporting publications can be found at https://www.acsc.gov.au/infosec/ism/index.htm.