Cyber Security Policy

1. INTRODUCTION

1.1 Background

Cyber security is one of the largest threats to organisations globally. While organisations cannot control cyber threats, they can control the work they do to protect their systems from infiltration. The Australian Cyber Security Centre (ACSC) within the Australian Signals Directorate (ASD) has developed prioritised strategies to mitigate cyber security incidents. While no single mitigation is guaranteed to prevent cyber security incidents, organisations can implement the Essential Eight to make it harder for adversaries to their compromise systems.

The Australian Government through the Australian Signals Directorate (ASD) invests significant resources developing and keeping up to date the Essential Eight. EREA will adopt the Essential Eight acknowledging the greater resource and testing that the ASD provides.

1.2 Purpose

To provide a standard methodology to protect our systems from cyber threats, including:

- Targeted cyber intrusions and other external adversaries who steal data
- Ransomware and external adversaries who destroy data and prevent computers and networks from functioning
- Malicious insiders who steal data
- Malicious insiders who destroy data and prevent computers and networks from functioning

1.3 Scope

The adoption of the Essential Eight and Mitigation Strategies apply to EREA's IT systems including, but not limited to, Mainstream Colleges, Flexi Schools, ELC's and the Parent Entity systems.

2. Roles and Responsibilities

Role	Responsibilities
EREA Board	• Approving this policy • Ensuring this policy is reviewed and updated as needed • Reviewing compliance with this policy • Ensuring this policy and its implementation complies with relevant Catholic social teachings, and legal and ethical obligations.
EREA Executive Director delegates to the National Director of Stewardship	• Developing protocols to support migration to this policy and to explain its context within a school setting • Ensuring this policy is implemented

Role	Responsibilities
	• Ensuring annual self-assessment of each IT system • Monitoring compliance with this policy
Principals	• Implementing this policy in line with protocols • Developing an understanding of the components of the Essential Eight • Monitoring the school's compliance with this policy
Business Managers	• Ensuring a functional understanding of the Essential Eight • Working with their IT Leader to agree interpretations of protocols in the context of the school
Senior IT Leaders	• Interpret policy in line with protocols provided with advice from the Business Manager • Developing adherence program • Ensuring on-going adherence to the Essential Eight and Cyber Security Mitigation Strategies • Migrate to new protocols as they are developed • Compete an annual self-assessment of maturity

3. Policy guidelines

3.1 Adhere IT Systems Framework to include the Essential Eight security baseline:

1) Application control
2) Patch applications
3) Configure macro settings
4) User application hardening
5) Restrict administrative privileges
6) Patch operating systems
7) Multi-factor authentication and
8) Regular backups

3.2 Maturity Levels are ranked across each element of the Essential Eight and overall:

- Maturity Level Zero
- Maturity Level One
- Maturity Level Two
- Maturity Level Three

The 2017 version of the Essential Eight ranked the average of each maturity level. The 2021 revision ranks the lowest of the four levels as it denotes the lowest level of vulnerability.

EREA will track both the lowest maturity level to understand the greatest level of vulnerability and the average maturity level to assess progress across the eight dimensions.

3.3 Specific protocols for Essential Eight and Mitigation Strategies

EREA has developed specific protocols to consider the likely maturity level for each component of the Essential Eight, in line with the ASD recommendation to assess your environment and respond accordingly.

4. Policy Compliance

4.1 Breach of this policy

Schools who are in breach of having acceptable and appropriate maturity across the Essential Eight will have 6 months to improve.

The National Office will have 3 months to improve their maturity to appropriate levels as described in the protocols.

4.2 Policy review

The EREA Board is responsible for ensuring this policy is reviewed and updated as needed and endorsing this policy.

As the ASD updates the Essential Eight, EREA will adopt the current version within 6 months of official publication.

5. Related Policies, Procedures and Legislation

5.1 EREA policy linkage

This is the first EREA Policy in the emerging Digital Policy framework.
It links with the Privacy Policy.

5.2 Legislation

https://www.cyber.gov.au/acsc/view-all-content/essential-eight

https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model-FAQ

Appendix 1:

Essential Eight Maturity Model – July 2021

Appendix 2:

Self-Assessment of the Essential Eight Protocols - July 2021