Australian Government

Creative Australia

IT SECURITY POLICY

Issue no:	3.0
Date issued:	July 2018
Updated:	August 2023
Scheduled review date:	August 2024
Document status:	Final
Supersedes:	IT Security Policy 2.0
Prepared by:	Lassity Martin, Director IT
Approved by:	Executive

1. Purpose

The IT Security Policy sets out Creative Australia's information security direction and is the backbone of our IT Security Management Framework (ISMF). The purpose of the ISMF is to identify, mitigate, monitor, and manage information security vulnerabilities, threats, and risks to protect Creative Australia and its assets, information, and data proactively and actively.

The ISMF sets the intent and establishes the direction and principles for the protection of Creative Australia's IT assets. This is to enable continuous improvement of our security capability and resilience to emerging and evolving security threats.

The Creative Australia Executive Team demonstrates its commitment to IT security through the issue of this policy. The Executive Director, Corporate Resources is the owner of this policy and is responsible for the review and enforcing the controls provided within the policy. Key Security roles and responsibilities are described in Section 5.

2. Scope

This policy applies to all users or providers of Creative Australia IT resources – including (but not limited to) temporary, permanent, and casual employees; consultants and contractors; agency employees; third party suppliers, arts sector partners and visitors. This policy applies to all Creative Australia IT assets, devices connected to the Creative Australia network and Cloud-based systems containing Creative Australia data.

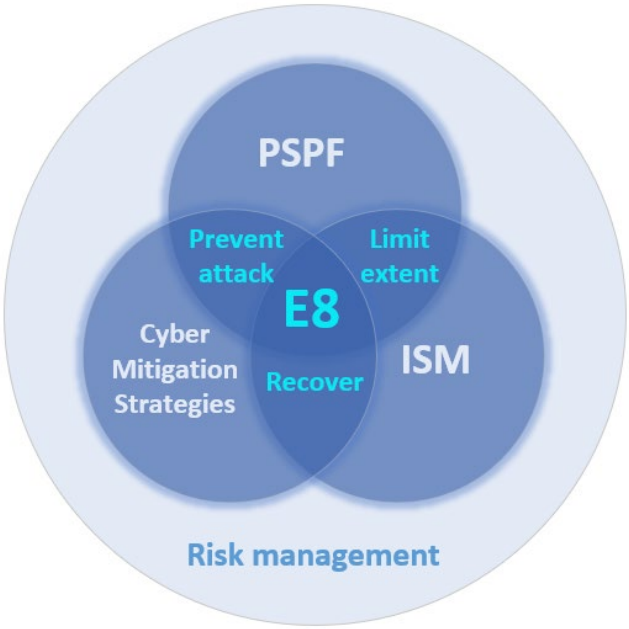
3. Policy statements

3.1 Risk-based approach to IT Security

Information security is a key part of Creative Australia's broader risk management process. Our approach to information security risk management is informed by the Protective Security Policy Framework (PSPF) published by the Attorney-General's Department and the Information Security Manual (ISM) including Essential Eight Strategies to Mitigate Cyber Security Incidents produced by the Australian Cyber Security Centre (ACSC). The PSPF (which is not mandatory for corporate commonwealth entities such as Creative Australia) represents better practice guidance with respect to IT security; the ISM provides strategic and practical advice about how to protect systems from cyber threats and the Essential Eight is a baseline set of mitigation strategies to help organisations prevent, limit the extent of and recover from cyber-attacks.

The Essential Eight Maturity model defines three levels for each mitigation strategy. These levels provide a high level indication of an organisation's cyber security maturity:

- Maturity Level One: Partly aligned with the intent of the mitigation strategy.
- Maturity Level Two: Mostly aligned with the intent of the mitigation strategy.
- Maturity Level Three: Fully aligned with the intent of the mitigation strategy.



ACSC "Essential Eight" alignment with other Australian government frameworks

Statement: IT suppliers and staff must take a risk-based approach to information security. Service providers and vendors must comply with Australian government protective security policies and procedures, as described in the PSPF including Policy 10: Safeguarding data from cyber threats, and adhere to any legislative or regulatory obligations under which Creative Australia operates.

Statement: Creative Australia aims to achieve a minimum of Maturity Level 2 across Essential Eight controls for internally managed systems. The ACSC has highlighted risk associated with third party suppliers as an emerging area of concern and advised that managed service providers are a popular target for cyber-crime. Accordingly, the security posture of third-party systems hosting Creative Australia data should (at minimum) align with Essential Eight Maturity Level 3.

3.2 Application Control

Application control is a mitigation strategy to prevent execution of unapproved/malicious programs. An application whitelisting solution must be used within standard operating environments to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an approved set.

Statement: Application control must be implemented on workstations and servers to ensure that all non-approved applications (including malicious code) are prevented from executing within standard user profiles and temporary folders used by the operating system, web browsers and email clients. Allowed and blocked executions on workstations and Internet-facing servers must be logged.

Statement: Internally managed systems should achieve Essential Eight Maturity Level 2 with respect to application control. Third-party systems should achieve Maturity Level 3.

3.3 Patch Applications

A patch is a piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other program deficiencies and improving the usability or performance of the software.

Application patching is an essential control to remediate security vulnerabilities that could be used to execute malicious code on systems.

Statement: The latest versions of applications should be used wherever possible, and applications or services that are no longer supported by vendors should be removed from Creative Australia's environment. Patches, updates, or vendor mitigations for security vulnerabilities in Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software and security products must be applied within two weeks of release, or within 48 hours if an exploit exists. Other security patches should be applied within a month following their release by vendors.

A vulnerability scanner should be used on a regular basis to identify missing patches or updates for security vulnerabilities as follows:

- Daily for Internet-facing services.
- Weekly for office productivity suites, web browsers and their extensions, email clients, PDF software and security products.
- Fortnightly for other applications.

Statement: Internally managed systems should achieve Essential Eight Maturity Level 2 with respect to application patching. Third-party systems should achieve Essential Eight Maturity Level 3.

3.4 Configure Microsoft Office Macro Settings

A macro is a series of commands and instructions that are grouped together as a single command to accomplish a task automatically. Microsoft Office macros are created using embedded code written in a programming language known as Visual Basic for Applications (VBA). Macros should be carefully controlled as they can be used to deliver and execute malicious code on systems.

Statement: Microsoft Office macros should be disabled for users that do not have a demonstrated business requirement. Macros in files originating from the Internet should be blocked. Antivirus scanning should be enabled for Microsoft Office macros, and they should be blocked from making Win32 API calls. Allowed and blocked Microsoft Office macro executions should be logged. Macro security settings must not be able to be changed by users.

Statement: Internally managed systems should achieve Essential Eight Maturity Level 2 with respect to Microsoft Office Macro Settings. Third-party systems should achieve Essential Eight Maturity Level 3.

3.5 User Application Hardening

Application hardening is an overall term for improving the security of a given application by removing functionality that is not required and ensuring that security functionality is set at an appropriate level rather than the default settings. An example of hardening is changing the default login on a home Internet router from ‘admin’ to something unique. This is particularly important for office productivity suites such as Microsoft Office, web browsers and Internet-facing systems that are likely to be targeted by an adversary: for Example, web advertisements and Java are popular ways to deliver and execute malicious code.

To assist in securely configuring their products, vendors may provide security guides: Microsoft provides Microsoft Office security guides as part of the Microsoft Security Compliance Manager tool.

Statement: Web browsers should not process Java or web advertisements from the Internet. Internet Explorer 11 should not process content from the Internet. Microsoft Office should be configured to prevent activation of OLE packages and blocked from creating child processes, creating executable content, and injecting code into other processes. PDF software must be blocked from creating child processes. ACSC or vendor hardening guidance for Microsoft Office and PDF software must be implemented.

Web browser, Microsoft Office and PDF security settings must not be able to be changed by users. Any security functionality in applications should be enabled and configured for maximum security. Any unrequired functionality in applications should be disabled. Vendor guidance should be followed to assist in securely configuring their products.

Statement: Internally managed systems should achieve Essential Eight Maturity Level 2 with respect to user application hardening. Third-party systems should achieve Essential Eight Maturity Level 3.

3.6 Restrict Administrative Privileges

Administrator accounts are the ‘keys to the kingdom’. Adversaries use these accounts to gain full access to information and systems.

Statement: Administrative privileges to operating systems and applications should be restricted based on user duties. The need for privileges should be regularly revalidated. Privileged accounts should not be used for reading email and web browsing.

Statement: Internally managed systems should achieve Essential Eight Maturity Level 2 with respect to restriction of administrative privileges. Third-party systems should achieve Essential Eight Maturity Level 3.

3.7 Patch Operating Systems

Security vulnerabilities in operating systems can be used to further the compromise of systems. Timely patching of operating systems is an essential strategy for limiting the extent of cyber security incidents.

Statement: The latest versions of operating systems should be used wherever possible. Unsupported versions should not be used. A patch management strategy must be defined covering the patching of security vulnerabilities in operating systems, applications, drivers, and hardware devices. Systems with 'extreme risk' vulnerabilities should be patched within 48 hours.

Statement: Internally managed systems should achieve Essential Eight Maturity Level 2 with respect to patching of operating systems. Third-party systems should achieve Essential Eight Maturity Level 3.

3.8 Multi-factor Authentication

Stronger user authentication makes it harder for adversaries to access sensitive information and systems.

Statement: Legacy authentication must not be used. Multi-factor authentication must be used to control access to Creative Australia systems and data, including for VPNs, RDP, SSH and other remote access, and when users perform a privileged action or access important (sensitive/high availability) data repositories.

Statement: Internally managed systems should achieve Essential Eight Maturity Level 2 with respect to multi-factor authentication. Third-party systems should achieve Essential Eight Maturity Level 3.

3.9 Regular Backups

Backups are primarily a preventative measure to protect against loss of data resulting from system failure (disaster or other), virus/malware attack, system, or human error.

Backups are an essential control and safeguard to ensure availability of Creative Australia information being stored, processed, or transmitted via IT systems, and to ensure information can be accessed again in case of a successful ransomware incident or other cyber-attack.

Statement: Data must be backed up on a regular basis, protected from unauthorised access or modification during storage, and available to be recovered in a timely manner in the event of incident or disaster. Important new/changed data, software and configuration settings should be backed up daily, stored disconnected and retained for at least three months. Test restoration of backups should be performed initially, annually, and when IT infrastructure changes.

Statement: Internally managed systems should achieve Essential Eight Maturity Level 2 with respect to regular backups. Third-party systems should achieve Essential Eight Maturity Level 3.

3.10 Security Incident Management

Provide preventive, corrective, and detective measures, ensuring a consistent and effective approach to the management of information security incidents, including communication of events and weaknesses, such as breach of access.

Well designed, understood tools and processes will help contain, preserve (legal / forensic purposes), and limit any damage resulting from a security incident.

Statement: Intrusion detection, prevention and response systems based on industry best practice must be in place for all systems containing Creative Australia data. Identified security incidents must be handled appropriately in accordance with Creative Australia Security Incident Response Plans. Service providers and employees must report cyber security incidents to the Creative Australia CISO as soon as possible after they occur or are discovered.

3.11 User Access Management

Unauthorised access to systems could enable a malicious or accidental security breach, potentially resulting in productivity, reputational or financial loss.

Only authorised users should be granted access to Creative Australia systems. Access to systems and the information they process, store, or communicate is controlled through strong user identification, authentication, and authorisation practices.

Statement: All user access related requests (e.g., adding new users, updating access privileges, and revoking user access rights) must be logged, assessed, and approved in accordance with the Creative Australia User Access Management Process.

Statement: Users must be uniquely identifiable, and use of shared non-user specific accounts should be avoided. Multi-factor authentication must be used to confirm the claimed identity of a user. Passwords must comply with standards defined in the IT Acceptable Use Policy.

Statement: All users must agree to comply with Creative Australia's IT Security Policy and IT Acceptable Use Policies before being granted access to Creative Australia systems and data.

3.12 Logging and Monitoring

Security devices such as firewall, Intrusion detection / prevention, security event incident management, mail content filters and anti-virus all generate log data. The timely detection of information security incidents relies on comprehensive security log data being available from IT systems.

Statement: Key security-related events such as user privilege changes must be recorded in logs, protected against unauthorised changes, and analysed on a regular basis to identify potential unauthorised activities and facilitate appropriate follow up action.

3.13 Cloud Security

Creative Australia is increasingly utilising Cloud solutions to deliver business solutions and functionality. This Policy explains what we expect of "Cloud Service Providers" to ensure all Creative Australia information and system controls, and service expectations are met.

Cloud services must maintain an appropriate level of security to ensure the confidentiality, integrity, and availability of Creative Australia data. Cloud services must demonstrate a robust security posture including compliance with the ASD 'Essential Eight Strategies for Mitigating Cyber Security Incidents' at maturity level 3 or equivalent using alternative industry standards such as ISO 27001 or NIST.

Statement: When planning new business projects, Business System owners must carry out a risk assessment using Creative Australia's Third-Party Risk Management framework to

determine the impact if a system were to be compromised and consult with IT to determine appropriate security controls. Creative Australia's security requirements must be captured in contracts.

Statement: During the contract term of any Cloud service, Business System owners must:

- Ensure that agreed security controls have been implemented correctly and are operating as intended.
- Report at least annually to the CISO on the security status of their systems.
- Ensure the CISO is immediately advised of any cyber security incidents and that these are managed in accordance with the Creative Australia Cyber Security Incident Response Plan.

3.14 IT Asset Management and Configuration Control

Asset / Inventory management and configuration control is key to prudent security and management practices, providing context for all IT Security Policy statements.

Without an accurate inventory, processes such as vulnerability management are difficult to implement. For example, assessment of in scope devices when responding to critical vulnerabilities, may not be captured, hence devices will remain unpatched and therefore exposed to malicious exploit.

In the context of this policy, an IT asset is any Creative Australia-owned or managed device or service that connects to or is used by Creative Australia in its business activities such as data link, physical device, application (including firmware), database and middleware.

Statement: An accurate inventory must be maintained that documents the configuration of all IT assets, including Cloud-based services that are used by Creative Australia in its business activities.

3.15 Change Management

The Creative Australia IT Change Management process ensures stability and availability of related information technology communication systems across the organisation. It is important to maintain the security of systems when implementing changes.

Statement: Any change to production information systems must be logged and assessed for security and risk impact as documented in the IT Change Management Process. The requirements, risk and impact of each request must be evaluated, and the proposed risk mitigation solution must be documented and approved.

3.16 IT System Acquisition & Development

IT systems (applications, databases & middleware) are susceptible to attack and therefore security controls must be embedded throughout the whole acquisition and development lifecycle.

Statement: Appropriate security measures must be in place during all stages of IT system development, when new IT systems are implemented into the operational environment and be maintained until systems are retired.

3.17 End User Protection

End User devices are the primary gateway to Creative Australia data and business applications. Implementation of appropriate information security controls is necessary to mitigate the risk of inappropriate access to data and IT systems such as malware, information disclosure or loss.

Consequently, End User protection is critical to ensuring a robust, reliable, and secure IT environment. Failing to maintain adequate controls can result in an information security incident, causing financial and/or reputational loss.

Statement: End User desktop computers, mobile computers (such as laptops and tablets) must be protected with adequate security mechanisms to prevent the unauthorised disclosure and/or modification of Creative Australia data. Portable computing devices (e.g., portable hard drives, USB memory sticks etc.) should not be used unless they are encrypted.

3.18 Network Security

Network infrastructure and associated data links provide essential connectivity between internal and external systems. To provide mitigation against malicious activity, secure boundaries and connections need to be defined and managed in line with current security practices.

Statement: Creative Australia's network architecture must be commensurate with current and future business requirements as well as with emerging security threats. Appropriate controls must be established to ensure security of our data in private and public networks, and the protection of IT services from unauthorised access.

3.19 IT Recovery

Service availability is critical for Creative Australia IT communications, infrastructure, systems, and applications. This Policy ensures that processes are in place to ensure the ability to recover from system and environmental failures, and regular testing of these processes is afforded.

Statement: An IT Recovery Plan and associated process must be in place to enable the recovery of business-critical services in a timely manner, to minimise the effect of IT disruptions and to maintain resilience before, during, and after a disruption.

4. Definitions

ACSC – the Australian Cyber Security Centre within ASD leads the Australian Government's efforts on national cyber security.

ASD – the Australian Signals Directorate is the Australian government agency responsible for foreign signals intelligence, support to military operations, cyber warfare, and information security.

Cloud - In the simplest terms, Cloud computing means storing and accessing data and programs over the Internet instead of from your computer's hard drive or on-premise server. The Cloud is a metaphor for the Internet.

End User – An End User is the person who is intended to use a computer system or device after it has been fully developed and configured. In an enterprise setting, the End User is the individual employee who uses the technology.

Essential Eight - The ACSC has developed prioritised mitigation strategies to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are the Essential Eight.

Essential Eight Maturity Model – The Essential Eight Maturity Model provides advice on how to implement the Essential Eight to mitigate different levels of adversary tradecraft and targeting.

Internet - The Internet is a massive network. It connects millions of computers together globally, forming a network in which any computer can communicate with any other computer if they are both connected to the Internet.

ISM – Information Security Manual, published by the ACSC, provides strategic and practical guidance on how an organisation can protect their systems and data from cyber threats.

ISO/IEC 27001 – An international standard on how to manage information security, recognised as a best-practice framework.

IT – Information Technology

Malware - software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Multi-Factor Authentication – is an authentication method in which a computer user is granted access to a given IT system only after successfully presenting two or more pieces of evidence (known as ‘factors’) to an authentication mechanism, as follows:

- something the user knows (e.g., a personal identification number (PIN), password or response to a challenge)
- something the user has (e.g., a physical token, smartcard, or software certificate)
- something the user is (e.g., a biometric value such as fingerprint or iris scan).

NIST Cybersecurity Framework – is a set of guidelines for mitigating organizational cybersecurity risks, published by the US National Institute of Standards and Technology (NIST). NIST is used by several governments and a wide range of businesses and organizations.

PSPF – the Protective Security Policy Framework is published by the Australian Government Attorney-General’s Department. It sets out government protective security policy and supports entities to effectively implement the policy across areas including security governance, information security, personnel security, and physical security.

Remote Access - refers to the ability to access an IT resource, such as a home computer or an office network computer, from a remote location. This allows authorised users to work offsite, such as at home or in another location, while still having access to a distant computer or network, such as the office network.

User - A user is a person who utilises a computer, network service or other IT resource.

User account – is an established technique for connecting a user and an IT service. A user account is comprised of a username, password and any information related to the user. User accounts determine whether a user can connect to a computer, network, or other IT resource.

Wi-Fi – a facility allowing computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area.

5. Roles and responsibilities

Role	Responsibility
Chief Security Officer (CSO) Executive Director, Corporate Resources	• Provides strategic oversight of protective security across Creative Australia. • Makes security-related decisions and fosters a positive security- culture. • Appoints security advisors to support them to deliver protective security and perform specialist services. • Works with the CISO to ensure alignment between cyber security and business objectives.
Chief Information Security Officer (CISO) – Director, IT	• Provides cyber security leadership and guidance including about procurement and vendor management. • Oversees the cyber security program and ensures compliance with cyber security policy, standards, regulations, and legislation. • Implements cyber security measurement metrics and key performance indicators. • Oversees the response to cyber security incidents. • Coordinates security risk management activities between cyber security and business teams.
Business System Owner	• When planning new business projects, applies a risk management approach to determine the impact if a system were to be compromised. Consults with IT to assess the security posture of potential Cloud service providers and determine appropriate security controls. • Ensures that agreed security controls are captured in contracts and that compliance is regularly reported as part of contract management procedures. • Reports at least annually to the CISO on the security status of their systems. • Ensures the CISO is immediately advised of any cyber security incidents and that they are managed in accordance with Creative Australia's Cyber Security Incident Response Plan.
IT Service Providers and suppliers	• Responsible for compliance with this Policy. • Responsible for the day-to-day performance of security functions.
Executive	• Be aware of this policy, encourage and ensure adherence.

6. Interacting policies and information

This policy should be read in conjunction with the following related documents:

- IT Acceptable Use Policy
- Procurement of IT Services and Cloud Policy
- Out of the Office IT Access Policy
- BYOD Policy
- Code of Conduct
- Information Management Policy
- Privacy Policy
- IT Security Plan
- IT Change Management Process

The following external references are available for further information:

- Australian Government Information Security Manual (ISM) – ACSC
- Protective Security Policy Framework – Attorney-General's Department
- Essential Eight Maturity Model for Cyber Security - ACSC

7. Change history

Date	Change description	Reason for change	Author	Issue no:
07/2018	Creation		Lassity Martin	1.0
05/2022	Updated format. Updated definitions, roles, responsibilities. Amended policy statements.	Updates to the Essential Eight by the ACSC; audit recommendations for policy improvement	Lassity Martin	2.0
08/2023	Removed references to the Australia Council and replaced with Creative Australia	Legislation change	Lassity Martin	3.0

Attachment A: The Essential Eight

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