Australian Government

Creative Australia

# Guide to Developing a Cyber and Data Security Policy

**Like all businesses, arts and cultural organisations are reliant on technology to store, manage and process sensitive information. With the rise of cyber threats and privacy concerns, it is crucial that organisations prioritise cyber security and protect the privacy and security of their digital assets, intellectual property and collected information.**

**This factsheet and example policy provides guidance for arts and cultural organisations on how to manage cyber and data security risks effectively, and establish measures to safeguard valuable information from unauthorised access, use or disclosure.**

*This guide and template may assist boards and board members of all arts organisations to engage in better practice and meet their legal obligations. All organisations should check relevant state, territory and federal legislation for any specific legal requirements.*

Arts and cultural organisations may have responsibilities under the *Privacy Act 1988* and Australian Privacy Principles when collecting and handling personal information. This could include information collected about employees and/or volunteers, a database of member or donor contacts and financial details, or audience data that includes personal or sensitive information. Irrespective of the size or type of arts and cultural organisation or its activities or events, all organisations should prioritise the protection of personal information.

The scale and nature of the organisation, as well as the types of data collected through its activities will determine the complexity of its data and cyber security protocols. However, all organisations should consider how the data they collect is stored and protected and their responsibilities to the privacy of individuals who share their data with the organisation.

As with all policies, it is integral that cyber policies and procedures are regularly reviewed to ensure relevance and effectiveness, especially due to the constant evolution of the digital environment. The review of cyber policies should have mechanisms and measures in place to enable rapid updates in response to regulatory updates, emerging cyber threats, policy gaps and weaknesses, technological advancement and general changes to the organisation's digital activities.

## Who is involved in developing a cyber and data security policy?

The organisation's board and management should collaborate in the development and improvement of cyber policies and processes. Cyber security within arts and cultural organisations may not be something the board has considered. Having conversations about cyber security and building a healthy cyber governance culture involves prioritising cyber security as a strategic business issue, and raising awareness and responsibility throughout the organisation.

It is recommended, where possible, to seek legal advice or consult with cyber security professionals to tailor the policy effectively and ensure compliance with relevant laws and regulations.

In the event of a cyber threat, the board plays a crucial role in guiding an organisation's response, making informed decisions and allocating resources. This may require increasing the digital knowledge of board members and management, and ensuring regular review and adaptation of policies to emerging threats to maintain effective cyber security practices and conduct informed cyber crisis management.

# Steps to developing a cyber and data security policy

**Step: 1**

### Define the scope and purpose

- Clearly define the scope and purpose of the policy, outlining the objectives and goals it aims to achieve. This may include protecting sensitive data, maintaining system integrity, ensuring compliance with relevant regulations and promoting a culture of cybersecurity awareness.

**Step: 2**

### Ensure legal and regulatory compliance

- Consider applicable laws and regulations related to cyber security, data protection and privacy. Ensure the policy aligns with these legal requirements and incorporates necessary safeguards.

**Step: 3**

### Conduct a risk assessment

- Conduct a comprehensive risk assessment to identify potential cyber security threats, vulnerabilities and impacts specific to your organisation. This assessment will help in determining the appropriate controls and mitigation strategies to include in the policy. (See Creative Australia's *Guide to Risk Management Frameworks* for more information).

**Step: 4**

### Define roles and responsibilities

- Clearly define the roles and responsibilities of individuals involved in cyber security, such as the board, CEO, IT department and employees. Assign accountability for maintaining and enforcing the policy.

**Step: 5**

### Control access

- Establish guidelines for granting access to organisational resources based on job roles and responsibilities. Implement strong authentication mechanisms, password management practices and user access controls to ensure authorised access and minimise unauthorised access risks related to private or personal data.

**Step: 6**

### Define data protection procedures

- Define procedures for data classification, handling, storage and transmission.
- Include measures to protect sensitive and confidential information, such as encryption, data backup and secure disposal practices. See key terms below for further detail to these core aspects of data protection.

**Step: 7**

### Develop an incident response plan

- Develop an incident response plan that outlines steps to be taken in the event of a cyber security incident. Include protocols for reporting incidents, assessing impact, containing threats and restoring normal operations. Assign incident response roles and establish communication channels.
- Note: Established organisations may have incident reporting standards and procedures that require documentation of breaches or misconduct. Cyber security reporting may simply involve having a line or multiple lines of reporting. For example, staff can verbally report breaches to management, including safeguarding mechanisms where there are alternative leaders or board members that reporting can be directed to.

**Step: 8**

### Increase employee awareness and provide training

- Emphasise the importance of cyber security awareness among employees and provide training programs to educate them about best practices, potential risks and their responsibilities in safeguarding organisational assets.

**Step: 9**

### Monitor and audit

- Define procedures for ongoing monitoring, auditing and assessment of cyber security controls to detect and respond to potential threats. This may include network monitoring, log analysis, vulnerability assessments or penetration testing, where an authorised simulated cyberattack is performed on a system to evaluate security.

**Step: 10**

### Review and update the policy

- Establish a regular review cycle to ensure the policy remains up to date with evolving cyber threats, technologies and regulatory changes. Encourage feedback from stakeholders and incorporate lessons learned from security incidents or audits.

## Key cyber security and data management terms

- **Data classification:** Identification and classification of different types of data based on their sensitivity and importance. This involves categorising data into levels, such as public, internal, confidential or highly confidential. Clearly defining access rights and permissions based on data classification can help ensure that only authorised personnel can access specific types of data.
- **Data handling:** Implementation of a 'need-to-know' principle, meaning employees should only have access to data necessary for their roles. It can also entail avoiding use of personal or sensitive data and/or encouraging de-identifying data where possible. Data handling may require specific training for employees on proper data handling procedures and security protocols to prevent data breaches and unauthorised access.
- **Data storage:** This refers to the either using secure servers or cloud services with encryption to store sensitive data. Organisations should regularly review and/or update security systems to prevent vulnerabilities. Cloud providers invest in security, using encryption, firewalls and compliance frameworks, whereas on-site servers offer more control but require extensive expertise for security maintenance.
- **Encryption:** This refers to process of making data accessible to intended parties only (for example, encrypted by key or password). Implement strong encryption protocols for both stored data and transmitted data. Use industry-standard encryption algorithms to safeguard sensitive information.
- **Data backup:** The process of creating duplicate copies of digital data and storing them in a separate location to ensure data integrity and availability in the event of data loss, system failure or cyber incidents such as ransomware attacks or accidental data deletion.
- **Secure disposal practices:** Organisations might develop a data retention policy to determine how long data should be stored and when it should be securely disposed of. For example, data wiping for devices and media containing sensitive information.

**Access controls and authentication:** The mechanisms and processes for verifying the identity of a user attempting to access a system or resource. It involves validating credentials, such as usernames, passwords or multi-factor authentication, to confirm that the person or device is genuinely who or what it claims to be. Organisations should regularly review and update access permissions to ensure that only current employees have appropriate access.

**Data breach:** Unauthorised access, acquisition or disclosure of sensitive or confidential information. It occurs when an individual, group or organisation gains unauthorised access to digital systems, databases or networks and retrieves or exposes sensitive data, potentially leading to its misuse, exposure or malicious activity. Data breaches can result in significant financial, legal and reputational consequences for the affected organisation and stakeholders.

## Example: Cyber and data security policy

The following is an example cyber and data security policy.

Author:
Date published:
Review period:
Next review:

### Introduction

This cyber and data security policy aims to establish guidelines and practices to safeguard [Organisation name]'s computer equipment, software, data and network accounts from exploitation or misuse.

### Purpose

The purpose of this policy is to foster a culture of ethical conduct and trust between the board, executive, staff and all stakeholders of the organisation, while ensuring the protection of [Organisation name]'s systems against external threats. It provides guidelines for generating, implementing and maintaining cyber and data security practices to safeguard our organisation. This policy applies to employees, contractors, consultants and volunteers, as well as all equipment owned or leased by [Organisation name] and authorised for business purposes.

### Scope

#### Responsibilities

It is the responsibility of the [insert appropriate role, for example IT Manager] to induct and ensure whole-of-organisation awareness and comprehension of this policy. The [insert appropriate role, for example IT Manager] is to keep the CEO aware of any breaches or changes to this policy and ensure timely completion of incident reports. The CEO may submit updates and reports to the board.

#### Data ownership and confidentiality

All data created on the organisation's systems remains the exclusive property of the organisation.

[Organisation name] emphasises that the confidentiality of information stored on the organisation's network devices cannot be guaranteed and, therefore, periodic network audits will be conducted to ensure compliance and identify vulnerabilities.

*Example: Cyber and data security policy (continued)*

### Information classification and protection

[Organisation name] will implement a classification system [Note: Example of high level data classification categories below] for information based on its degree of confidentiality, ensuring that appropriate processes are in place to protect sensitive data. [Note: Depending on the nature of the data and scale of the organisation, this may include training employees, implementing access controls and/or data encryption].

Employees and volunteers are expected to adhere to necessary cyber security procedures, including, enabling two-factor authentication, secure computer access and the use of protective software.

### Access control

The [insert appropriate role, for example IT Manager] will determine the requirements for access for individuals to different organisational information and resources.

### Breaches and misconduct

In the event of a cyber security breach or any misconduct related to information security, it is the responsibility of all employees, contractors, consultants and volunteers to immediately report the incident to the organisation's [insert appropriate role, for example IT Manager]. Prompt reporting allows for swift action to mitigate the impact of the breach and ensure appropriate measures are taken to address the situation. The organisation will conduct thorough investigations into breaches and misconduct, and disciplinary actions will be taken in accordance with the severity of the incident and in compliance with organisational policies and applicable laws.

### Evaluation and review

Regular evaluation and review of this cyber security policy will be conducted to ensure its effectiveness and alignment with evolving threats, technologies and regulatory requirements. The policy will be reviewed by [insert appropriate role, for example IT Manager] and relevant stakeholders to identify areas for improvement and incorporate lessons learned from security incidents. Feedback from employees and volunteers will be sought and considered to enhance the policy's relevance and effectiveness. Any necessary updates or revisions will be made to maintain the highest level of cybersecurity standards within the organisation.

**Note: Example high level data classification categories**

- **High/extreme:** Highly sensitive data that may be demographic data, credit card information or banking details.
- **Medium:** Data that could be used for exploitation or information that has reputational or financial impacts, for example internal emails.
- **Low:** Publicly available data and information.

A detailed cyber security policy template can be downloaded from the **Institute of Community Directors: Cyber Security Policy**

## Resources

**Arts Law: Cyber Security: Know the basics**

A resource that provides practical guidelines, awareness of key privacy principles and steps to handle data breaches effectively.

**Community Door: Dealing with Cyber Security Threats**

Information on cyber security measures, including recent webinars, articles and training opportunities, for increasing understanding and addressing cyber risks.

**Institute of Community Directors: Data breach response plan Template**

This outlines a step-by-step data breach response plan, including the roles of the crisis management team, communication strategies and a template data breach response letter, providing a structured framework to address and manage data breaches effectively.

**Office of the Australian Information Commissioner: Australian Privacy Principles**

This outlines the Australian Privacy Principles which govern the collection, use and disclosure of personal information under the *Privacy Act 1988*.

**Office of the Australian Information Commissioner: Notifiable Data Breaches**

Note: Only relevant to organisations with annual turnover of over $3 million. This details the process and circumstances in which organisations must, under the *Privacy Act 1988*, notify affected individuals and the Office of the Australian Information Commissioner of data breaches.