Mining and Automotive Skills Alliance

Information Management Plan (including Cybersecurity)

Version 1.2

Contents

1. Purpose

This policy outlines the Mining and Automotive Skills Alliance Ltd (AUSMASA) guidelines and provisions for proactively managing and preserving the security of AUSMASA's data and technology infrastructure.

2. Overview

By increasingly relying on technology to collect, store and manage information, AUSMASA is exposing its data to increased risk of a security breach and is becoming increasingly vulnerable to the impacts of human error, sabotage (cyber-attack) and system malfunctions on the security, availability, and integrity of its data. Any event that compromises the security of AUSMASA's data has the potential to:

- cause a significant interruption to AUSMASA's activities
- constitute a breach of AUSMASA's confidentiality obligations under contract and at law
- jeopardise AUSMASA's business reputation
- cause AUSMASA to incur significant financial cost to restore its systems.

AUSMASA continues to implement data security measures through its IT services provider. This policy is intended to further mitigate data security risk by setting out the behaviours expected of Personnel when using AUSMASA's electronic equipment and responding to any security-related issues. In addition, the policy sets out AUSMASA's approach to accessing, retaining, processing or the destruction of AUSMASA's data.

3. Audience

This policy applies to AUSMASA's:

- Board
- Advisory Committees or Panels
- Sub-committees
- Employees
- Contractors and Sub-contractors
- anyone who has permanent or temporary access to AUSMASA's systems and electronic equipment.

4. Policy

4.1. Confidential Information and Data

Confidential information and data are secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas, or new technologies
- Customer lists (existing and prospective)

Employees must protect the data in AUSMASA's systems from security breaches so that it remains secure from unauthorised access, which can be achieved by following the instructions in this policy.

4.2. Protect Personal and Company Devices

Using digital devices to access company emails or accounts introduces a security risk to AUSMASA's data. All employees must keep their personal and company-issued computers and mobile phones secure, and must:

- keep all devices password protected
- not leave devices exposed or unattended
- log into company accounts and systems through secure and private networks only.

Employees must not access internal systems or accounts from other people's devices or lend their own devices to others. All employees, and particularly new starters, must follow any instructions issued to them to protect their devices and refer to AUSMASA's IT service provider if they have any questions.

4.3. Keep Emails Safe

Emails often host scams and malicious software. To avoid virus infection or data theft, employees must:

- avoid opening attachments and clicking on links when the content is not adequately explained (e.g., "watch this video, it's amazing")
- be suspicious of clickbait titles (e.g., offering prizes, advice)
- check email and names of people they received a message from to ensure they are legitimate
- Look for inconsistencies or other clues (e.g., grammar mistakes, capital letters, excessive punctuation).

If unsure whether an email is safe, employees must not click on any licks and should refer to AUSMASA's IT service provider for further guidance.

4.4. Password Management

Password leaks are dangerous as they can compromise AUSMASA's entire infrastructure. Not only should passwords be kept secure, but they must also remain confidential. For this reason, AUSMASA's employees must:

- choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g., birthdays)
- remember passwords instead of writing them down
- exchange credentials only when absolutely necessary, either in person or by telephone
- change passwords regularly or when instructed to do so by AUSMASA's IT service provider.

4.5. Transfer Data Securely

Transferring data introduces security risk. Employees must:

- avoid transferring sensitive data (e.g., client information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, employees must seek the assistance of AUSMASA's IT service provider
- share confidential data over the company network/system or private connection and not over public Wi-Fi

- ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies
- report scams, privacy breaches, and hacking attempts to AUSMASA's IT service provider.

All employees must report perceived attacks, suspicious emails, or phishing attempts as soon as possible to AUSMASA's IT service provider, who will investigate promptly, resolve the issue, and send a company-wide alert when necessary.

4.6. Data Retention

- Actively and continuously consider whether retention of data is necessary.
- Retain only the minimum data necessary. It is possible to have too much data. Over-collection of data is a significant risk. Only keep what is reasonably necessary for AUSMASA's business functions or to comply with our legal obligations.
- The industry best practice period to retain data (and relevant information record) is:
    I. for seven years for financial and governance records.
    II. for seven years if it is personal information about an adult
    III. for seven years after a child turns 18 if it is personal information about a child
    IV. until it is no longer necessary for the purpose for which it was collected (whichever is the longer).

NOTE: This is in conjunction with the Privacy Policy and the Privacy Act 1988. Link Here: https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act

- Record data in the most appropriate format and minimise paper records.
- Email inboxes and mailbox folders should not be the primary source of storing records and data, particularly data that consists of personal information or sensitive information.
- Data should be stored securely and in a manner that is appropriate to the value and sensitivity of the data and the physical properties (if applicable) of the record (for example, paper records should be stored in a cool, dry place outside of direct sunlight to avoid degradation).
- Take steps to secure records and data and minimise the risk of corruption of data or accidental loss. Ensure that important data is securely backed-up and archive records when they are not actively being used (but which are not ready to be destroyed).

4.7. Data Destruction

- Do not destroy records and data that are necessary for AUSMASA's business functions or legally required to be kept.
- Do not destroy records and data that may be relevant to ongoing or anticipated disputes, litigation or regulatory investigations. If you have doubts about whether certain records or data should be retained for their evidentiary value.
- Consider whether AUSMASA has contractual obligations to destroy certain records and data after the expiration of a contractual relationship.
- Ensure paper records are securely destroyed if appropriate. Use shredders or security bins to destroy paper records.
- There may be occasions where it is not possible or practicable to destroy data irretrievably (because, for example, the system on which the data is stored does not allow data to be deleted or where the data is part of a larger dataset). These circumstances should be avoided, if possible, but if they arise, you should take reasonable steps to:

(a) put the data beyond use. The Office of the Australian Information Commissioner (OAIC) defines this to mean:
    i. is not able (and will not attempt) to use or disclose that data, and
    ii. cannot give any other entity access to that data, and
    iii. surrounds the data with appropriate technical, physical and organisational security. This should include, at a minimum, access controls, including logs and audit trails, and
    iv. commits to take reasonable steps to destroy the data if, or when irretrievably, this becomes possible; or
(b) De-identify the data: If the data contains personal information or sensitive information, consider whether it is possible and practicable to de-identify the data. This means taking steps to remove information that could reasonably identify an individual (for example, by redacting scanned documents).

- There may be certain circumstances in which the data should be de-identified immediately (such as where it is being used for analytics or research purposes, which does not require individuals to be personally identifiable.

4.8. Remote Access

This policy applies equally to AUSMASA employees when they are working remotely. Employees must ensure that their private network is secure.

4.9. Additional Measures

To reduce the likelihood of security breaches, AUSMASA's employees must:

- lock devices when leaving desks in public settings
- report stolen or damaged equipment as soon as possible to their direct line manager or General Manager
- change all account passwords immediately if a device is lost or stolen
- report a perceived threat or possible security weakness in company systems
- avoid downloading suspicious, unauthorised, or illegal software on any equipment owned by AUSMASA
- avoid accessing suspicious websites.

AUSMASA's employees must also comply with any other policy regarding digital or electronic media, data, or the use of electronic equipment owned by AUSMASA.

AUSMASA will:

- install firewalls, anti-malware software and access authentication systems
- provide data security training to all employees as required
- inform employees regularly about new scam emails or viruses and ways to combat them
- investigate security breaches thoroughly.

4.10. Disciplinary Action

Any employee who causes a data security breach may face disciplinary action:

- First-time, unintentional, small-scale security breach: A verbal warning and training about data security
- Intentional, repeated, or large-scale breaches that cause severe financial or other damage to AUSMASA: Proportionate consequences, including potential termination of employment.

Additionally, we may take progressive disciplinary action against any employee observed disregarding AUSMASA's security instructions or this Policy, even if their behaviour has not or does not result in a security breach.

5. Definitions

CYBER-ATTACK is an attempt by hackers to damage or destroy a computer network or system.

DATA SECURITY refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, mobile phones, databases, and websites. Data security also protects data from corruption.

MALICIOUS SOFTWARE refers to any malicious program that causes harm to a computer system or network. Malicious 'Malware' software attacks a computer or network in the form of viruses, worms, trojans, spyware, adware or rootkits.

CLICKBAIT refers to something designed to make a reader want to click on a hyperlink, especially when the link leads to content of dubious value or interest.

FIREWALL refers to security that protects a network or system from unauthorised access.

PERSONNEL means Board members, Advisory Committee members, Sub-committee members, employees, contractors, subcontractors, suppliers and agents of AUSMASA or all of them as a group, as the context requires.

6. Document History and Contact Details

Version

Number	1
Version	1.2
Implementation date	28 June 2022
Review date(s)	30 June 2023
Next Review date	30 June 2024

Revision History

Revision date	Summary of amendments	Prepared by	Version
10 May 2023	Branding update Audience amendment	CEO	1.1
18 May 2023	Document Name updated in line with JSC requirements. Sections 4.6 Data Retention and 4.7 Data Destruction added.		1.2

Contact details

Owner	AUSMASA Board / AUSMASA CEO
Contact officer	Company Secretary, board@ausmasa.org.au or Gavin Lind, gavin.lind@ausmasa.org.au