Policy

Information Security and Artificial Intelligence Use

Brendan McKenna Earthmoving

Date Modified: 21/08/26 Next Revision Date: 21/08/28

Policy statement

MCK Group is committed to protecting business, worker, client and project information and to using artificial intelligence (AI) responsibly, securely and transparently. Information security and AI risks will be identified, assessed and controlled through the MCK Group Integrated Management System (IMS).

This policy forms part of the MCK Group IMS and supports the Corporate Risk Register, including CR-019 Information Security and CR-021 Artificial Intelligence Use.

Purpose

The purpose of this policy is to establish practical requirements for protecting information, maintaining access to business systems, responding to security incidents and ensuring AI-assisted work is checked and approved before use.

Scope

This policy applies to all MCK Group workers, contractors and other authorised users who access company devices, accounts, systems, records, applications or AI tools. It applies to information in electronic, paper, verbal and visual form, including personal, client, commercial, project and IMS information.

Responsibilities

Role	Responsibilities
Director	Approves this policy, approved systems and significant AI uses; ensures resources are available; oversees serious information-security or privacy incidents.
Operations Manager	Implements access, device, backup and AI-use controls; reviews risks; coordinates incident response and corrective actions.
Administration	Maintains authorised accounts and records, supports access changes and backups, and reports suspected incidents or unusual system activity.
Workers and contractors	Protect passwords and information, use only approved systems and AI tools, check AI-assisted work, and immediately report loss, disclosure, suspicious activity or errors.

Policy requirements

Approved systems and access

- Company information must be accessed only through approved devices, accounts, applications and storage locations.
- Users must have individual accounts, protect passwords, use multifactor authentication where available and never share login details. Access must be limited to the role and changed promptly when duties or employment end.

Secure handling of information

- Personal, client, commercial, project and IMS information must be collected, used, shared, stored and disposed of only for authorised business purposes.
- Users must check recipients and must not transfer company information to personal email, unapproved storage or unauthorised media. Confidential information must be protected from unauthorised access.

Devices, updates and backups

- Devices must have screen locks and current security updates. Lost, stolen, damaged or compromised devices must be reported immediately.
- Important records must be stored in approved backed-up locations, and recovery must be tested periodically. Suspicious links, attachments, credential requests or payment instructions must be verified before action.

Approved use of artificial intelligence

- AI tools may be used only for approved business purposes and where suitable for the task.

- Confidential, personal, client, commercially sensitive, security-related or legally privileged information must not be entered into AI unless the Managing Director approves the tool and specific use.
- AI must not independently make safety, employment, legal, environmental, financial or client decisions. Consultation, competency, management approval, copyright, privacy, contractual and client requirements still apply.

Human review and approval of AI outputs

- AI-generated information must be treated as a draft and checked by a competent person for accuracy, completeness, relevance, bias and appropriate source support.
- Controlled IMS documents, tenders, client communications, risk assessments and significant decisions require normal MCK Group review and approval. AI does not replace qualified professional, legal or technical advice.

Incident reporting, response and review

- Suspected unauthorised access, data loss, disclosure, malware, phishing, unusual account activity or inappropriate AI use must be reported immediately to the Operations Manager or Managing Director.
- MCK Group will contain and assess the incident, protect information, restore services, retain records and determine required notifications. Risks, access, backups and this policy will be reviewed after incidents or significant changes and at least annually.

Training and communication

Relevant workers will be informed of this policy through induction, toolbox communication or the MCK Group App. Additional instruction will be provided where a worker administers systems, handles sensitive information or uses AI for controlled documents or significant business activities.

Records and monitoring

MCK Group will retain appropriate records of access changes, backups, incidents, corrective actions, worker communication and approvals for significant AI use. Compliance will be monitored through workplace observations, document reviews, risk-register reviews, internal audits and management review.

Related information

- HS-RA-001 Risk Assessment Register - Corporate Risks CR-019 and CR-021
- IMS Document Control Procedure and Document Register
- HS-PR-005 Incident Investigation & Reporting Procedure and Incident Register
- MCK Group IMS Registers Master
- Privacy Act 1988 (Cth) and Notifiable Data Breaches Scheme, where applicable
- Australian Signals Directorate - Essential Eight and Artificial Intelligence for Small Business guidance

Approved by

Brendan McKenna
Managing Director
Brendan McKenna Earthmoving Pty Ltd

Controlled document: The current approved version of this policy is available through the MCK Group App. Printed or downloaded copies are uncontrolled unless specifically issued as controlled copies.