Manufacturing Industry Skills Alliance

INFORMATION MANAGEMENT PLAN

Purpose

The *Information Management Plan* sets out the approach to securely storing, sharing, protecting, tracking and managing files, documents, project records and other information or documentation (information assets) as it relates to the Manufacturing Industry Skills Alliance (the Manufacturing Alliance).

Scope

This Plan applies to information assets in any format, created or received, to support the Manufacturing Alliance's business activities. It covers information created, managed, and stored in-house and off-site, including in cloud-based platforms, and outlines protection of systems.

Who needs to comply

Management of information assets is the responsibility of all users. All employees, contractors and sub-contractors should be aware of the Manufacturing Alliance's information management expectations, obligations, and controls. Board Directors, Strategic Industry Taskforce and sub-committee members should also be broadly aware of the organisation's approach to information management and are required to discharge their responsibilities in accordance with relevant governance documents including charters, the *Manufacturing Industry Skills Alliance Constitution*, the *Jobs and Skills Councils Integrity Framework*, and specific legislative responsibilities.

What data is captured

In delivering the Jobs and Skills Councils (JSC) program, the Manufacturing Alliance expects to collect and store the following types of data:

- *Financial data*: information related to the financial health of the organisation such as financial records and banking statements.
- *Stakeholder data:* information gathered from interactions with Manufacturing Alliance stakeholders and may include personal or business information.
- *Personal data*: personal information about persons doing work for the Manufacturing Alliance including (but not limited to) employees, Board and committee members, and may include payroll details and other sensitive information.
- *Supplier data*: e.g., business information, banking details.
- *Contractual-related information*: documentation associated with the development of contractual deliverables; ranging from a Workforce Plan, Strategic Plan, Annual Workplan, etc., reporting information; pricing and funding information; statistical data, business records, through to emails and documents developed by employees to support the core business of the Manufacturing Alliance; any other data identified through the *Grant Agreement* as being owned by the Department of Employment and Workplace Relations (DEWR).
- *Compliance data*: records maintained for the purposes of satisfying the organisation's compliance requirements under the Grant Agreement, the JSC Integrity Framework, and any other record-keeping required under legislative and regulatory obligations

How we store and protect data

The Manufacturing Alliance requires that company and client information is stored securely and systematically and is kept confidential (refer Privacy Policy).

Data access

All users will access data via web browsers, and authentication will be by their email addresses and passwords reinforced by Multi Factor Authentication.

Data control

Data control will be enforced by granting permissions to users on a need's basis. Regarding Microsoft SharePoint, policies will be put in place by using best practice data governance and data loss policies, designed in consultation with internal stakeholders. User access to Manufacturing Alliance data will be controlled by Azure AD and Intune policies to restrict access to trusted devices. USB device controls will be put in place to avoid data exfiltration.

Data storage

In line with legislation, the majority of documents must be kept for a minimum of seven (7) years. As part of normal operational practice, electronic records no longer required may be archived prior to the minimum document retention period. The disposal of any information assets must be authorized by the appropriate manager.

A tailored IT Disaster Recovery Plan (ITDRP) is in place for the organisation, underpinned by the following limitations:

- Where cloud-based storage solutions are in place, the Manufacturing Alliance will have limited control over the service provider's response to an outage i.e., Microsoft, Xero.
- The Manufacturing Alliance will have limited control over disruptions affecting external digital communication infrastructures such as the Internet, NBN, telephone networks, and other communication channels managed by third-party service providers.

Offline data

The Manufacturing Alliance promotes the online storage of all data, however where required, hard copy documents are stored securely on and off-site. Senior personnel that require access to material of a highly sensitive nature (e.g., HR or Corporate Governance material) are provided with secure storage facilities. A confidential secure bin is provided on premises to ensure that physical records are destroyed securely and in such a way that the information is unreadable.

Cyber Security

The Manufacturing Alliance has in place a Information Technology and Data Security Policy that address our systems environment including hardware and network infrastructure, and software applications including those installed locally and those provided as a software as a service (Cloud services).

These policies set out provisions with respect to Network Security Management including email access and security, password management and security, and procedures for preparing for and responding to any cyber incident risks.

Compliance requirements

In delivering the JSC Program, the Manufacturing Alliance will comply with the information security requirements set out in the Grant Agreement (refer 9.15 Information Security) and in relevant legislation, including (but not limited to) the requirements under the *Privacy Act 1988* (Cth) regarding the protection of personal information it holds. Further information about the organisation's obligations and controls are set out in the Privacy Policy.

Review of controls

The *Information Management Plan* will be treated as a 'living document' and will be reviewed and revised on an as-needs basis.

Related policies and plans

- Confidentiality Policy
- Privacy Policy
- IT and Data Security Policy
- IT Disaster Recovery Plan (ITDRP)
- Business Continuity Plan (BCP)