	DIGITAL MANUFACTURING IRELAND	
Document Title:	Mobile Device Policy Digital Manufacturing Ireland	
Document Approvers:	**Signature**	**Department**
	Tracey Mannion	Document Control
	Billy Donovan	Information Technology
Version Number:	V2.0	
Effective Date:	29Sep2023	

Contents

1 Purpose & Objectives

Digital Manufacturing Ireland (DMI) is committed to the correct and proper use of mobile devices to support employee productivity. The risks of remote working including the use of mobile devices must be considered and appropriate protection applied.

The purpose of this document is to protect information against the risks introduced by using user endpoint devices.

2 Scope

This policy applies to

- All DMI users (DMI staff, DMI subsidiaries, partners, contractors and joint venture companies) who are authorised to access DMI information, information systems, applications or computer networks; and
- All DMI information (physical and digital).

3 Policy

3.1 Mobile Device

Only devices issued by the DMI IT Team / managed service provider or other devices subject to an authorised service request by DMI can be used to process and store DMI Information. These devices have been securely configured to address key security concerns.

1. Restricted, confidential, and internal data may be handled and processed on endpoint devices for the purpose of transferring them to approved locations. Restricted and confidential data should not be stored on the endpoint without manager approval.
2. Controls must be in place to restrict the installation of software on endpoint devices.
3. Controls must be in place to protect against the deployment of malicious software.
4. Controls must be in place to manage removable storage devices.
5. Controls must be in place to avoid the unauthorised access to or disclosure of DMI information stored and processed by these devices, e.g., using encryption and enforcing use of secret authentication information such as passwords.
6. Users must be informed of their responsibilities when using mobile devices in public places, meeting rooms and other unprotected areas.
7. Controls must be in place to ensure that the currency of mobile device software is managed, and updates applied as required.
8. The capability to remotely disable, erase and lock mobile devices must be implemented.
9. Devices carrying important, confidential, or strictly confidential information must not be left unattended and, where possible physically locked away or special locks used to secure the devices.

3.2 Remote Working

- The types of devices permitted to connect remotely to internal networks must be specified with the least-controlled devices having minimal access to DMI resources.
    - Only laptops, tablets and mobile phones that have been provisioned by DMI may connect remotely to internal networks and infrastructure.
- The type of work and level of access each remote worker is granted must be approved by an appropriate line manager and managed by appropriate controls.
- Unauthorised access to information or resources from other persons in remote sites must be prohibited.

3.3 Bring Your Own Device (BYOD)

DMI staff will be permitted in exceptional circumstances to use a personal device. This device will require DMI InfoSec controls to be installed, and it can be remotely wiped in the event of loss or theft. The usage will also have to be approved by your department lead and ISMS Committee.

3.4 User responsibility

All DMI users should be made aware of security requirements and procedures for protecting user. endpoint devices, as well as their responsibilities for implementing such security measures. DMI staff are advised to:

- log-off active sessions and terminate services when no longer needed.
- protect user endpoint devices from unauthorised use with a physical control (e.g. key lock or special locks) and logical control (e.g. password access) when not in use;
- not leave devices carrying important, sensitive, or critical business information unattended.
- use devices with special care in public places, open offices, meeting places and other unprotected areas (e.g., avoid reading confidential information if people can read from the back, use privacy screen filters);
- physically protect user endpoint devices against theft (e.g., in cars and other forms of transport, hotel rooms, conference centres and meeting places).

A specific procedure considering legal, statutory, regulatory, contractual (including insurance) and other security requirements of the organisation should be established for cases of theft or loss of user endpoint devices.

3.5 Wireless Connections

- Configurations for wireless connections on devices should follow best practice e.g. disabling vulnerable protocols, requiring a password, etc.
- When connecting to a wireless / wired connection, the staff member should ensure that the appropriate level of bandwidth is available to support security functions e.g. backups, updates, etc.

4 Appendix

4.1 Appendix A - Reference Documents

Document Name
DMI - Logical Access Process
DMI - Acceptable Usage Policy

Revision History

No #	Revision Description	Date Approved
2.0	Section 3.3 updated to include mor detail for DMI employees	29Sep2023
1.0	New Document	31Jul2023