

Section: INFORMATION MANAGEMENT

Subject

**ACCEPTABLE USE OF
INFORMATION SYSTEMS**

Approved by: Board of Directors

GENERAL PURPOSE

The Acceptable Use of Information Systems Policy of Marathon Oil Company (the Company) is provided to assist employees in managing, communicating, creating, obtaining and storing Business Information (information maintained as evidence or reference to support ongoing business activities and/or to comply with legal or regulatory requirements).

This Policy outlines the requirements, responsibilities and behaviors necessary to ensure responsible and productive use of information systems.

POLICY STATEMENT

The Company expects its Authorized Users (employees and others performing services for the Company), to exercise good judgment and behavior in the use of all Company assets, including its information systems, which include but are not limited to:

- computers,
- telecommunication devices,
- the Internet and other internal and external electronic networks,
- voice mail, e-mail, fax machines,
- software applications, and
- electronic media storage devices.

The Company's information systems are intended to be used only for business purposes consistent with all Company policies and in conformity with any rights, limitations or obligations to which the Company or the user is subject with respect to information systems.

Personal Use

While Company information systems are intended for job-related activities, incidental and occasional brief personal use is permitted within reasonable limits.

However, inappropriate use of information systems is strictly prohibited at any time.

Such inappropriate use includes, but is not limited to:

- communicating, creating, obtaining, sending, or storing information which is offensive, discriminatory, defamatory, disparaging, harassing, obscene, intimidating, or constitutes racial, ethnic, or sexual slurs,
- accessing inappropriate Internet sites, such as those that contain sexually-explicit, racial, hate, or gambling content,
- creating or forwarding e-mail, blogging, social network participation or other communication activity that involves inappropriate content,
- spending excessive amounts of work time at non-business related sites, or
- using Company information systems for personal business ventures or personal political or religious causes.

Section: INFORMATION MANAGEMENT

Subject

**ACCEPTABLE USE OF
INFORMATION SYSTEMS**

Approved by: Board of Directors

Authorized Users are strongly advised against copying electronic information from an external source, such as the Internet, and intentionally saving it to Company information systems for purely personal use (e.g., software applications, music, pictures and video files).

Authorized Users shall not engage in any blogging or social network participation, regardless of whether during work or on their personal time, which may harm or tarnish the image, reputation, and/or goodwill of the Company or any of its employees, vendors, customers, business affiliates or partners. In addition, Authorized Users are prohibited from making any discriminatory, disparaging, defamatory or harassing comments or otherwise engaging in any conduct prohibited by the Company's Harassment Policy when blogging or participating in social networks, both internal and outside the company.

Employees should request guidance from their supervisor or Human Resources on any questions regarding the business or personal use of information systems.

Any information that is created, obtained, or stored on Company information systems is considered Company property. The Company reserves the right to manage, access, monitor, read, review, delete, and audit, without prior notification, all usage or content of its information systems. **THERE IS NO EXPECTATION OF PERSONAL PRIVACY OR CONFIDENTIALITY WITH RESPECT TO ANY USE OR CONTENT OF INFORMATION SYSTEMS.**

Passwords

Authorized Users should not disclose passwords or provide access authorizations to other persons. Users should not use unauthorized access authorizations or passwords to gain access to other users' files or communications, except as otherwise permitted by this Policy.

Intellectual and Confidential Property

Authorized Users must safeguard the Company's intellectual property. Information systems should never be used for the disclosure of proprietary, confidential, or privileged information to unauthorized parties. Accordingly, care and discretion must be exercised when transferring information to third parties.

Information not suitable for public disclosure, particularly proprietary, confidential, or privileged information, must never be created, maintained or stored on sites accessible by third parties outside the Company.

Authorized Users should take care when retrieving information from outside sources to ensure no proprietary third-party information is illegally or improperly transferred to the Company.

In addition, when using e-mail, Company confidential proprietary information must be appropriately labeled; e.g., "**CONFIDENTIAL – PROPERTY OF MARATHON OIL COMPANY.**"

Section: INFORMATION MANAGEMENT

Subject

**ACCEPTABLE USE OF
INFORMATION SYSTEMS**

Approved by: Board of Directors

Company Use of Personal Devices

Authorized Users are prohibited from forwarding or intentionally saving Business Information to their personal computers, personal e-mail accounts or other personal devices, except in times of emergency, implementation of business continuity plans, or as otherwise permitted by this Policy.

Any Business Information that is created, obtained, or stored on such personal computers, other personal devices, or personal e-mail accounts is subject to the provisions of this Policy, as well as all other Company policies dealing with the use and storage of Business Information.

In addition, Authorized Users must return to the Company and ensure deletion of all Business Information stored on their personal computers, other personal devices, or personal e-mail accounts upon termination of their employment or assignment with the Company. Authorized Users are hereby advised that **THERE IS NO EXPECTATION OF PERSONAL PRIVACY OR CONFIDENTIALITY WITH RESPECT TO ANY INFORMATION COMINGLED WITH BUSINESS INFORMATION ON THEIR PERSONAL COMPUTERS, OTHER PERSONAL DEVICES, AND PERSONAL E-MAIL ACCOUNTS.**

Policy Violations

Any violation of this Policy by an Authorized User or any failure or refusal to cooperate with efforts to audit or otherwise implement this Policy, may result in disciplinary action up to and including discharge for the first offense.

It is not intended that this Policy regulate or interfere with information systems maintenance or repair, whether constant, regular, intermittent, or on-demand, as such is normally provided by the Information Technology department or its designated contractors.

The Company does not waive any confidentiality or privilege it may have with respect to the use of information systems.

POLICY APPLICATION

This Policy applies to any Company operations and facilities, including any information systems provided by the Company, as well as any information systems used in furtherance of the Company's business, whether owned or leased by the Company, by an employee, or by another Authorized User, unless otherwise prohibited by local law.

The substance of this Policy, appropriately adapted for the conditions involved in each case, is recommended for adoption by Marathon's wholly or majority owned subsidiaries and, if permitted under applicable agreements, all Marathon-operated joint ventures and projects.

Section: INFORMATION MANAGEMENT

Subject

**ACCEPTABLE USE OF
INFORMATION SYSTEMS**

Approved by: Board of Directors

POLICY IMPLEMENTATION

The ECM Director has the responsibility and authority to oversee the application of and adherence to this Policy.

The ECM Director must be consulted whenever the review, monitoring or auditing of information systems is being considered within the scope of this Policy and when an organization is considering whether, and to what extent, to permit the non-business use of Company information systems or business use of personal information systems. The ECM Director will in turn consult with the Human Resources, Law, Internal Audit and Information Technology departments as necessary.

Line managers have the responsibility to communicate and implement this Policy within their respective organizations.

Adherence to this Policy is the responsibility of every Authorized User.

POLICY REVIEW

This Policy shall be reviewed at least once every five years, or more frequently as stipulated by the ECM Director, or when a significant change occurs, including changes in law that impact information management.

POLICY EXCEPTIONS

Modification, waiver, limitation or exception of this Policy requires the written approval of the ECM Director.

POLICY SUPERSEDES

- ADM 002 – Information Systems and Electronic and Voice Mail Policy
- ADM 005 – MOC/MAP Acceptable Use of the Internet and Electronic Mail Policy