Information Security Policy

Overview

FP McCann's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to FP McCann's established culture of openness, trust and integrity. FP McCann is committed to protecting FP McCann's employees, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP (File Transfer Protocol), are the property of FP McCann. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations

Effective security is a team effort involving the participation and support of every FP McCann employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at FP McCann. These rules are in place to protect the employee and FP McCann. Inappropriate use exposes the Company to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct FP McCann business or interact with internal networks and business systems, whether owned or leased by FP McCann, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at FP McCann and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with FP McCann policies and standards, and local laws and regulation.

This policy applies to employees, contractors, consultants, temporaries, and other workers at FP McCann, including all personnel affiliated with third parties, and irrespective of their length of service, status or number of hours worked. This policy applies to all equipment that is owned or leased by FP McCann.

This policy and procedure does not form part of the contract of employment and will be amended from time to time.

Policy

General Use and Ownership

FP McCann proprietary information stored on electronic and computing devices whether owned or leased by FP McCann, the employee or a third party, remains the sole property of FP McCann. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*

You have a responsibility to promptly report the theft, loss or unauthorised disclosure of FP McCann proprietary information.

You may access, use or share FP McCann proprietary information only to the extent it is authorized and necessary to fulfil your assigned job duties.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their supervisor or manager.

For security and network maintenance purposes, authorised individuals within FP McCann may monitor equipment, systems and network traffic at any time, per FP McCann's *Internet & Email Policy*.

FP McCann reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Policy*.
System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited. Breaches will be dealt with through the Company's Disciplinary Procedure.
All mobile computing devices must be secured with a password or passcode in accordance with the Company's password complexity requirements with the automatic activation feature set to 10 minutes or less. The IT Department has configured policy to ensure that your device will require a password after a period of inactivity usually 10 minutes or less. You must lock the screen or log off when the device is unattended.
Postings by employees from an FP McCann email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of FP McCann, unless posting is in the course of business duties.
Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware. If you are unsure of the source or sender of the email, then just delete the email.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
Under no circumstances is an employee of FP McCann authorised to engage in any activity that is illegal under local, state or international law while utilising FP McCann-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by FP McCann.
- Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which FP McCann or the end user does not have an active license is strictly prohibited.
- Accessing data, a server or an account for any purpose other than conducting FP McCann business, even if you have authorised access, is prohibited.

- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using an FP McCann computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any FP McCann account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to FP McCann is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Introducing honeypots, honeynets, or similar technology on the FP McCann network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, FP McCann employees to parties outside FP McCann.

Email and Communication Activities

When using company resources to access and use the Internet, users must realise they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorised use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within FP McCann's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by FP McCann or connected via FP McCann's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- The company will randomly audit user mailbox content to ensure compliance.

Social Media & Blogging

Blogging by employees, whether using FP McCann's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of FP McCann's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate FP McCann's policy, is not detrimental to FP McCann's best interests, and does not interfere with an employee's regular work duties. Blogging from FP McCann's systems is also subject to monitoring.

FP McCann's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material that could be considered Confidential Information policy when engaged in blogging.

Employees shall not engage in any social media that may harm or tarnish the image, reputation and/or goodwill of FP McCann and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments and should always use best judgment when posting. Indicated social media includes the posting of text, images, audio and/or video as well as reposting and forwarding etc.

Employees should be aware the effect their actions may have on their images, as well as FP McCann's image. The information that employees post or publish may be public information for a long time.

Employees are not to publish, post or release any information that is considered confidential or not public. If there are questions about what is considered confidential, employees should check with the human resources department and or management.

Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refrain from any response and refer the approach to a Company director.

Social media use and building an online profile carries with it a responsibility not to negatively impact the company or colleagues or customers or suppliers reputations either expressly or by implication.

Employees may also not attribute personal statements, opinions or beliefs to FP McCann when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of FP McCann. Employees assume any and all risk associated with blogging.

It is expected that employees exercise best judgement when interacting on social media with other employees and stakeholders recognising the distinction between online relationships and a normal business relationship. Any

potential conflict of interest arising from a social media profile should be disclosed to HR department as soon as it becomes apparent.

Employees should be aware that their online profile and digital footprint could be used by malicious sources as part of social engineering methods and they should not post details that are likely to assist in a social engineering effort.

Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, FP McCann's trademarks, logos and any other FP McCann intellectual property may also not be used in connection with any blogging activity.

If employees encounter a situation while using social media that threatens to become hostile or implicate the company, they should disengage from the discussion and seek the advice of their line manager

Subject to applicable lay, after-hours online activity that violates FP McCann's Code of Conduct or any other company policy may subject an employee to disciplinary action up to and including dismissal.

Policy Compliance

Compliance Measurement

The FP McCann team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the FP McCann team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Review

The Senior Management Team will monitor and review this policy regularly.

Signed: _____

Hugh McCann
Managing Director

Reviewed: **12 January 2026**
Last Reviewed: **11 January 2025**
Next Review: **January 2027**