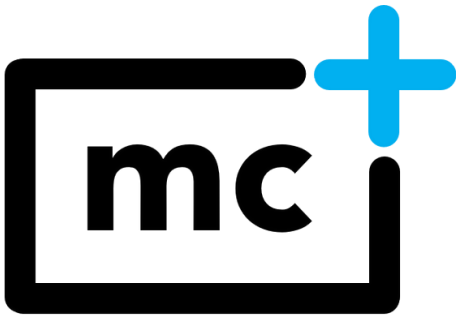

Email Policy

Context

Information security is the protection of information against accidental or malicious disclosure, modification, or destruction. Information is an important, valuable asset of the Company that must be managed with care. E-mail is to be used for business purposes and in a manner that is consistent with other forms of professional business communication. The transmission of a harmful attachment can not only cause damage to systems, but also harm the Company's reputation.

The Company

Economic Capital Solutions Limited, trading as Monte Carlo Plus ("the Company"), is an independent risk management software and consulting company. The Company develops risk management software and provides advisory services to well-known financial firms. All our clients are regulated by the FCA or the PRA.

Purpose

E-mail at the Company must be managed as valuable and mission critical resources. Thus, this policy is established to create prudent and acceptable practices regarding the use of information resources and educate employees with respect to their responsibilities.

Legal liability

Employees may be held liable for:

- Sending or forwarding e-mails with any libelous, defamatory, offensive, racist, or obscene remarks
- Sending or forwarding confidential information without permission

- Sending or forwarding copyrighted material without permission
- Knowingly sending or forwarding an attachment that contains a virus

Definitions

- Anti-Spoofing: A technique for identifying and dropping units of data, called packets, that have a false source address.
- Antivirus: Software used to prevent, detect, and remove malicious software.
- Electronic mail system: Any computer software application that allows electronic mail to be communicated from one computing system to another.
- Electronic mail (e-mail): Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.
- Email spoofing: The forgery of an email header so the message appears to have originated from someone other than the actual source. The goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation to provide sensitive data or perform an action such as processing a wire transfer.
- Inbound filters: A type of software based traffic filter allowing only designated traffic to flow towards a network.
- Quarantine: Suspicious email message may be identified by an antivirus filter and isolated from the normal mail inbox.
- SPAM: Unsolicited e-mail, usually from Internet sources. It is often referred to as junk e-mail.

Employee Responsibilities

E-mail is to be used for business purposes and in a manner that is consistent with other forms of professional business communication. Company e-mail is not private. Employees expressly waive any right of privacy in anything they create, store, send, or receive on the Company's systems. The Company can, but is not obliged to, monitor emails without prior notification.

Incoming email must be treated with the utmost care due to the inherent information security risks. Incoming emails must be scanned for malicious file attachments. An anti-virus application must be used to identify malicious code(s) or files. All email is subjected to inbound filtering of e-mail attachments to scan for viruses, malicious code, or spam. Introducing a virus or malicious code to the Company's systems could wreak havoc on the ability to conduct business. If the automatic scanning detects a security risk, it must be immediately notified.

All outgoing attachments must be automatically scanned for virus and malicious code. The transmission of a harmful attachment can not only cause damage to the recipient's system, but also harm the Company's reputation.

All confidential or sensitive material transmitted via e-mail must be encrypted. Passwords to decrypt the data should not be sent via email.

E-mail is not secure. Users must not e-mail passwords, social security numbers, account numbers, pin numbers, dates of birth, mother's maiden name, etc. without encrypting the data.

Employees must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the Company, unless appropriately authorized to do so.

Users must not send, forward, or receive confidential or sensitive } information through non-company email accounts. Examples of non-company e-mail accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and e- mail provided by other Internet Service Providers (ISP).

Prohibited Activities

- Sending e-mail that may be deemed intimidating, harassing, or offensive. This includes, but is not limited to: abusive language, sexually explicit remarks or pictures, profanities, defamatory or discriminatory remarks regarding race, creed, color, sex, age, religion, sexual orientation, national origin, or disability.
- Using e-mail for conducting personal business.
- Using e-mail for the purposes of sending SPAM or other unauthorized solicitations.
- Violating copyright laws by illegally distributing protected works.
- Sending e-mail using another person's e-mail account, except when authorized to send messages for another while serving in an administrative support role.
- Creating a false identity to bypass policy.
- Forging or attempting to forge e-mail messages.
- Knowingly disabling the automatic scanning of attachment.
- Knowingly circumventing e-mail security measures.
- Sending or forwarding joke e-mails, chain letters, or hoax letters.
- Sending unsolicited messages
- Sending excessively large messages or attachments.
- Knowingly sending or forwarding email with computer viruses.
- Setting up or responding on behalf of the Company without management approval.