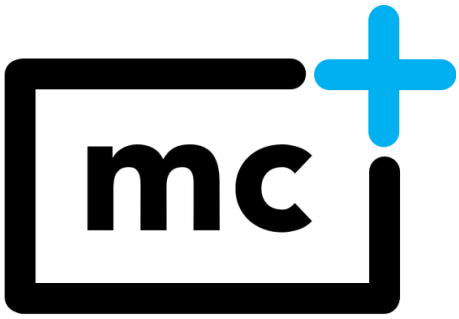

Access control policy

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. Access controls are put in place to protect information by controlling who has the right to use different information resources and by guarding against unauthorized use. Formal procedures must control how access to information is granted and how such access is changed. This policy also mandates a standard for the creation of strong passwords, their protection, and frequency of change.

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

Access control rules and procedures are required to regulate who can access the Company's information resources or systems and the associated access privileges. This policy applies at all times and all employees. Therefore, it should be adhered to whenever accessing the Company's information in any format, and on any device.

Passwords

Passwords are the first line of defense. A poorly chosen or misused password is a security risk and may impact the confidentiality, integrity, or availability of our computers and systems.

A weak password is one that is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers, and simple patterns of letters from a computer keyboard. A strong password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.Everyone must use strong passwords with a minimum standard of:

- At least seven characters.
- Contain a mix of alpha and numeric, with at least one digit
- More complex than a single word (such passwords are easier for hackers to crack).

Protecting Passwords

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all time.

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different systems.
- Do not use the same password for systems inside and outside of work.

Changing Passwords

All user-level passwords must be changed at a maximum of every 90 days, or whenever a system prompts you to change it. Default passwords must also be changed immediately. If you become aware or suspect, that your password has become known to someone else, you must change it immediately and report to your manager.

User Access Management

User access management consists of all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. All employees are required to keep their PC's is locked or logged out, leaving nothing on display that may contain access information such as login names and passwords. When an employee leaves the organization, their access to computer systems and data must be suspended at the close of business on the employee's last working day