Commission Delegated Regulation (EU) 2017/589 of 19 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying the organisational requirements of investment firms engaged in algorithmic trading (Text with EEA relevance)

CHAPTER II U.K.

RESILIENCE OF TRADING SYSTEMS

SECTION 3 U.K.

Means to ensure resilience

Article 18 *U.K.*

Security and limits to access(Article 17(1) of Directive 2014/65/EU)

1 An investment firm shall implement an IT strategy with defined objectives and measures which:

a is in compliance with the business and risk strategy of the investment firm and is adapted to its operational activities and the risks to which it is exposed;

b is based on a reliable IT organisation, including service, production, and development;

c complies with an effective IT security management.

2 An investment firm shall set up and maintain appropriate arrangements for physical and electronic security that minimise the risks of attacks against its information systems and that includes effective identity and access management. Those arrangements shall ensure the confidentiality, integrity, authenticity, and availability of data and the reliability and robustness of the investment firm's information systems.

3 An investment firm shall promptly inform the competent authority of any material breaches of its physical and electronic security measures. It shall provide an incident report to the competent authority, indicating the nature of the incident, the measures taken following the incident and the initiatives taken to avoid similar incidents from recurring.

4 An investment firm shall annually undertake penetration tests and vulnerability scans to simulate cyber-attacks.

5 An investment firm shall ensure that it is able to identify all persons who have critical user access rights to its IT systems. The investment firm shall restrict the number of such persons and shall monitor their access to IT systems to ensure traceability at all times.

Status:
Point in time view as at 31/12/2020.

Changes to legislation:
Commission Delegated Regulation (EU) 2017/589, Article 18 is up to date with all changes known to be in force on or before 18 August 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations.
EUR 2017 No. 589 may be subject to amendment by EU Exit Instruments made by both the Prudential Regulation Authority and the Financial Conduct Authority under powers set out in The Financial Regulators' Powers (Technical Standards etc.) (Amendment etc.) (EU Exit) Regulations 2018 (S.I. 2018/1115), regs. 2, 3, Sch. Pt. 4. These amendments are not currently available on legislation.gov.uk. Details of relevant amending instruments can be found on their website/s.