WEIS CONTRACTORS

WEIS CONTRACTORS 2024

ACCESS CONTROL MANAGEMENT POLICY

POLICY STATEMENT

This company is committed to ensuring, so far as is reasonably practicable, the protection and security of company and client data stored on electronic data processing and storage systems owned and used by the company including remote storages and of our technology infrastructure. This policy applies to all of our employees, contractors, and others who have permanent or temporary access to our systems and hardware.

AIMS AND OBJECTIVES

We recognise the importance of protecting data from unauthorised access and corruption. To achieve this, we will restrict access to company systems and applications to only authorised users or processes and be based on the principle of strict need to know and least privilege.

RESPONSIBILITIES

Management will be responsible for the development and implementation of principles by which user access is granted that protect the company IT systems and applications.

Management and supervisors of the company must regularly review network and operating system accounts with regard to access levels, and ensure that only those persons who are current authorised users are given access to company systems and applications, and to take immediate action to terminate or review access levels where appropriate due to employee terminations, death, resignation or change of employment or role.

All account users are responsible for ensuring they comply with the company policies relating to access and security controls that protect the company IT systems and applications from unauthorised access.

IMPLEMENTATION

Access principles will be established to ensure protection of the company IT systems and applications managed by the company that store, process or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

Privileged access to systems, applications and data repositories will be validated when first requested and revalidated as specified in company procedures. Policy and/or technical controls will be used to prevent privileged users from unauthorised reading of emails, web browsing and obtaining files via online services.

AUTHORISED BY

Signed: _____ Date: _____