WEIS CONTRACTORS 2024

USER AUTHENTICATION 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 extends to the authentication of
our employees, contractors, and others who have permanent or temporary access to our systems and data.

AIMS AND OBJECTIVES

We recognise the importance of protecting data from unauthorised access and corruption. To achieve this, we will develop and implement security measures and processes to minimise risks of unauthorised access to data and accounts by implementing appropriate user authentication of persons accessing our systems and data.

RESPONSIBILITIES

Management will be responsible for ensuring that authentication standards and guidelines are documented and for ensuring that all persons with access to company systems are aware of and comply with authentication procedures commensurate with their level of privilege or access.

All users are to ensure that they follow company guidelines forcreating, storing, updating andprotection of passwords and other multi-factor authentications and immediately report any actual or attempted unauthorised access to company systems and data.

IMPLEMENTATION

We will identify and implement user authentication appropriate to the level of security necessary for the particular access and will encourage the use of ‘strong’ passwords by persons requiring only single-factor authentication as a minimum level of security.

We will provide and implement standards and guidelines for the creation, protection and updating of strong passwords that are designed to minimise the risk of an unauthorised person gaining access to company systems through exploitation of user accounts and associated passwords.

We will encourage the use of multi-factor authentication for users of remote access solutions, and for all users who perform a privileged action or access an important (sensitive / high availability) data repository.

AUTHORISED BY

Signed: _____ Date: _____