# Access Control Policy

## Policy

User access to Novus Altair information systems shall be granted on the basis of the need-to-know principle. Users shall be given access only at the appropriate level required to perform their job functions.

## Business Requirements for Access Control

**1.1** All employees shall be issued a Fob that will grant them access to the main entrance of the building. This shall be subject to an Alarm Fob holder unlocking the door initially to enable fob access.

**1.2** Alarm Fobs/Keys shall be restricted to managerial level.

**1.3** Upon loss of a key/fob this shall be reported to the Information Security Officer as soon as possible to enable it to be de-activated in a timely manner.

## User Access Management

User access management shall ensure authorised user access, and prevent unauthorised access to information and information systems. This is managed by the Information Owner.

**1.4** All user access control is managed through system privileges.

**1.5** The Information Owner maintains a User Access List to evidence clearly user access rights, this is archived as rights are changed to evidence user access history.

**1.6** Special attention is given to the control of privileged access rights.

**1.7** These access rights are reviewed at planned intervals by the senior management.

## User Responsibilities

Users shall take all measure to prevent compromise and/or theft of their access rights in accordance with the organisation's Password Policy. They shall be expected to do this through the following:

**1.8** Maintaining authentication security, particularly regarding password and key-fob safety

**1.9** Securing assets assigned to them (e.g. computer and other office equipment)

## Network Access Control

Users shall have direct access only to the services that they have been specifically authorised to use. Upon being granted specific authorisation, users may be allowed access to the following:

**1.10** Networks – Organisations LAN/WAN

**1.11** Network Services –File Services, E-mail & internet

## Operating System Access Control

Controls shall be implemented to restrict information system access to authorised users by requiring authentication of authorised users in accordance with the defined access control policy. Controls include:

**1.12** Providing mechanisms for authentication by knowledge-, Keys &/or Keypad methods as appropriate.
**1.13** Recording successful and failed system authentication attempts
**1.14** Recording the use of special system privileges and
**1.15** Issuing alarms when access security controls are breached.

## Information Access Control

Controls shall be established and implemented to prevent unauthorised access to information held in application systems.

## Mobile Computing

Controls shall be established and implemented to ensure information security when using mobile computing devices. Controls shall be implemented to commensurate with the:

**1.16** Type of user(s)
**1.17** Setting(s) of mobile use and
**1.18** Sensitivity of the applications and information being access from the mobile device.

Approved by Dr Adnan Niazi

Date 5/7/18
Last Reviewed On 05/07/24

Version 1