

# Modini identity and access management policy

Version: 1.0

Date: 24 Jan 2023

Author: Owen Candy

---

## Contents

1. Introduction
  2. Onboarding, amendments and offboarding
  3. Access
- 

### 1. Introduction

- 1.1 All authorised Modini staff and direct contractors (Staff) have an Azure Active Directory account (AD).
  - 1.1.1. Staff are given an AD account on joining Modini.
  - 1.1.2. AD accounts include a Modini.co.uk email address.
  - 1.1.3. Staff are disabled in AD when they cease to work for Modini or are on compliance leave.
  - 1.1.4. Staff with valid AD accounts may request access to an installation of Modini hosted in the Modini Cloud or a managed Modini instance from a Modini director – they must include a reasonable justification.
  - 1.1.5. Reasons must be compatible with specific contractual obligations.
  - 1.1.6. Temporary access may be exceptionally granted for break-fix situations.
- 1.2 A review of all access is conducted on a quarterly basis outside of the join/leave process to assert that users still have valid reasons for access.

### 2. Onboarding, amendments and offboarding

- 2.1 **Onboarding**
  - 2.1.1 All new users are approved and created by a Company Director. Once the requirement for a new user has been agreed, the user is required to read and agree to the user Acceptable Use Policy after which the Operations Director will distribute the new user account.
  - 2.1.2 Access to systems and applications will be aligned to the roles performed and approved by the Business Manager.
- 2.2 **Amendments**
  - 2.2.1 Changes to access provisions will be via request to the Operations Director and approved changes will be provided by the Operations Director.
- 2.3 **Offboarding**
  - 2.3.1 All leavers are processed by the Operations Director who, as part of the end user process, removes accounts.

### 3. Access

- 3.1 **Access levels**
    - 3.1.1 Access to laptops, computers and servers of the organisation (and the applications they contain) is only by unique user name and strong password.
- 



- 3.1.2 Only the Operations Director and MSA365 has “administrator” level access or that staff with specific roles are to be provided with “administrator” level. Administrator access is documented in the administrators log.
- 3.1.3 “Administrators” of the corporate network will be provided with a separate administrative login in addition to a “user” level login. The latter will be used for all non-administrative actions such as web browsing and email.
- 3.1.4 Wherever available administrator access will be via Multi Factor Authentication.

### 3.2 Periodic review and controls

- 3.2.1 The Operations Director will perform a quarterly review of systems and applications access to ensure that only appropriate access is in place for Modini covering systems, applications, SaaS and the level of access to each.

# Document control

## Version history

Version	Date	Approved by	Notes
V1.0	24/01/2023	Board	Initial version

