**Purpose and scope of this policy**

This policy aims to enhance the security of our systems from unauthorized access and misuse by ensuring the use of strong passwords and authentication. This policy relates to all forms of access to our systems and aims to provide a uniform method of access to all services.

As such, this policy relates to all users attempting to access our services.

**Roles and responsibilities**

Every user granted access to our services is responsible for the security and prevention of misuse of their password. This policy gives guidelines, that if they are followed should mitigate these risks. Not following them will result in consequences for the offending parties.

**Password Requirements**

* **Length:**
  + Password is between 14-32 characters long.
* **Complexity:**
  + No specific complexity requirements (e.g., uppercase, lowercase, numbers, symbols).
* **Use of Passphrases:**
  + The use of passphrases is encouraged (a sequence of words or a sentence) to improve memorability and security of your password.
* **Avoid Common Patterns:**
  + Avoid using easily guessable information, such as common words, sequences (e.g., "12345…"), or personal information.
* **Changing passwords:**
  + Passwords must be changed at latest every 180 days. If an issue arises please contact the IT department.
* **2FA Authentication:**
  + All users are required to use an authenticator to support 2FA of their logins.

**Password Management**

* **Storage:**
  + Passwords must not be written down or stored in plain text.
* **Sharing:**
  + Passwords must not be shared with anyone. Each individual must use their own unique password.

**Reporting and Response**

* Report any suspected or confirmed password compromise or misuse to the IT department immediately.
* Change passwords as soon as possible if a compromise is suspected.

**Points of contact**

In the case of any question regarding to the policy, please contact the IT department.