Password Management Policy

Purpose: To ensure the secure management of user credentials within the Security Awareness Web Application.

Scope: Applicable to all IT staff members accessing the web application.

Policy:

- Passwords must meet minimum complexity requirements (ex: 8 characters, including upper and lower case letters, numbers, and symbols).
- Passwords should be changed every 90 days.
- Multi-factor authentication (MFA) should be implemented to enhance the security of user logins.
- Failed login attempts should be monitored and logged, and accounts should be locked after five failed attempts to mitigate unauthorized access.

Compliance: Users must adhere to these rules to maintain their access to the system, and violations will result in account suspension until the issue is resolved.