Microsoft Authenticator App Alternative Authentication Policy

Version	Date	Changes	Author	Approver
0.1 Draft	October 2023	New Policy	James Vincent (Cyber Security Manager)	
1.0 Approved	4th December 2024	Updated following review	James Vincent (Cyber Security Manager)	Greg McCloskey (Director of D&IS)

Introduction

This policy outlines the procedure for staff members who are unable to use the Microsoft Authenticator app for multi-factor authentication (MFA) and need to utilise alternative authentication methods. It specifies the processes for staff members to follow for the issuance of a FIDO key or an OATH Hardware token as a secondary authentication method.

Policy Objectives:

The objectives of this policy are to ensure the security of the organisation's systems and data while accommodating staff members who are unable to use the Microsoft Authenticator app. By providing alternative authentication methods, the organisation aims to maintain a secure and accessible MFA process for all staff.

Scope:

This policy applies to all staff members who require alternative authentication methods due to an inability to use the Microsoft Authenticator app.

Policy Guidelines:

Eligibility for alternative authentication:

a. Staff members who are unable to use the Microsoft Authenticator app due to technical limitations or personal preferences may be eligible for alternative authentication methods.

b. Eligibility for alternative authentication methods is subject to approval by a line manager, the Queen’s University Cyber Security Team, and the Digital & Information Services Cyber Security Program Board.

Request for Alternative Authentication:

a. Staff members who require an alternative authentication method should firstly inform their line manager.

b. Line managers are responsible for collecting and documenting requests from staff members.

c. Line managers should submit these requests using the online request form.

Review and Approval:

a. The Cyber Security Team will review requests for alternative authentication methods.

b. Requests will be approved based on the staff member's eligibility and the organisation's security requirements.

c. The Cyber Security Team will communicate the approval or denial of requests to line managers and staff members.

Issuance of FIDO Key or MFA Token:

a. Upon approval, the Cyber Security Team will arrange for the issuance of a FIDO key or MFA token to the staff member.

b. The FIDO key or MFA token will serve as the secondary authentication method for the staff member.

Training and Support:

Staff members receiving alternative authentication methods will be provided with appropriate training and guidance on their usage.

Reporting and Monitoring:

a. Queen’s University will maintain a record of staff members using alternative authentication methods.

b. Digital &Information Services will regularly review and monitor the effectiveness and security of these methods.

Compliance:

All staff members are expected to comply with this policy and use alternative authentication methods responsibly and securely.

Policy Review:

This policy will be reviewed bi-annually (as a minimum) to ensure that it remains current and effective in meeting the organisation's security and accessibility needs.

In future versions, consideration will be given to passkeys/passwordless options.

Note: The specifics of implementing alternative authentication methods, such as FIDO keys or MFA tokens, may vary depending on the organisation's IT infrastructure and security requirements. It is crucial to work with Digital & Information Services to ensure that the chosen alternative methods are both secure and compliant with organisational policies.