Office365 Multi-Factor Authentication (MFA) Policy

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	27/09/2018
V 0.2	Andrew Clarke	2.2 O365 MFA limitations documented i.e. on/off - no conditional access, remote wipe added	03/10/2018
V 0.3	Andrew Clarke	Approval from technical PWG and O365 Project Board	04/03/2019
V 1.0	Andrew Clarke	InfoSub Committee Approval	10/04/2019

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

This document requires the approval from BUL as defined in the ISMS Compliance document.

Document Owner: Andrew Clarke	Document Approver: Mick Jenkins
Cyber & Information Security Manager	Chief Information Security Officer

Document Distribution

Name	Title	Version	Date of Issue

Contents

1. About this document

1.1 Purpose of Document

This Policy establishes the area within Brunel University London covering Microsoft Office365 that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
All staff, affiliates and students	Are responsible for maintaining actions and activity compliant with this policy
Head of Infrastructure & Operations	Is responsible for ensuring that Office 365 network Authentication, Authorisation and Accounting (AAA) are in line with the security requirements of the ISMS.
Systems Manager	Is responsible for maintaining and managing Office 365 systems policies on IT systems and infrastructure and ensuring that Multi Factor Authentication systems comply with this policy.
Cyber & Information Security Manager	Is responsible for maintaining the Multi Factor Authentication policy best practice and ensuring compliance with legislative and regulatory requirements.
Cyber & Information Security Team	Responsible for investigating Office 365 authentication breaches and recommending remedial actions when breaches have occurred.
CISO / SIRO / CIO	Management of exceptions

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A9 – Access Control
ISO 27001:2013 Conformance Control	Information Classification Objective A.9.1.2 Access to networks and network services

1.4 Scope

The scope of this policy applies to:

- All Brunel employees, affiliates and students with a Brunel-owned or personally owned computer, workstation or mobile device used to connect to the Brunel Microsoft Office365 environment onsite and remotely

- Additional Brunel systems may be protected in the future by multi-factor authentication ("MFA") but may not use Microsoft Office365 MFA.
  This policy will apply to any University system that requires an additional layer of protection, as determined by the Chief Information Security Office (CISO) in collaboration with the Chief Information Officer (CIO), such as: CHIME, VPN, SITS and system administration tools & privileged accounts

1.4.1 Out of Scope

- Alumni accounts will be email only (no Office 365 Apps - OneDrive for Business, Skype, Teams, Yammer, Forms, Sway, Planner or Video) and are out of scope for Office365 MFA App resource use

1.5 References

- CESG Good Practice Guide (GPG) 10 - Remote Working v2.2
- Brunel University London Acceptable Use Policy
- Password Policy

1.6 Policy Objectives

The objectives of this policy with regard to the protection of information system resources against unauthorised access and compromised accounts are to:

- Minimise the threat of accidental, unauthorised or inappropriate access to electronic information owned by Brunel or temporarily entrusted to it and to limit damage including the loss of sensitive or University confidential data, intellectual property, damage to public image, damage to critical Brunel internal systems
- Minimise Brunel's network exposure, which may result in a compromise of network integrity, availability and confidentiality of information system resources
- Minimise reputation exposure, which may result in loss, disclosure or corruption of sensitive information and breach of confidentiality and
- Define standards for connecting to Brunel's network from any host. These standards are designed to minimise the potential exposure to Brunel from damages, which may result from unauthorised use of Brunel resources.

2.0 Office 365 Multi-Factor Authentication Policy

2.1 Policy Summary

The purpose of this policy is to protect the confidentiality, integrity and availability of Brunel's information by controlling access to University Information Services (IS) Office 365 systems by Brunel's personnel, temporary staff, contractors, students and service providers utilising Brunel's information system and to define standards for connecting to Brunel's network.

Brunel's Office 365 resources are assets important to Brunel's business and stakeholders and its dependency on these assets demands that appropriate levels of Information Security be instituted and maintained. It is Brunel's policy that appropriate onsite and remote access control measures are implemented to protect its Office 365 resources against accidental or malicious destruction, damage, modification or disclosure, and to maintain appropriate levels of confidentiality, integrity and availability of such Office 365 resources. Multi-factor authentication adds a layer of security which helps deter the use of compromised credentials.

2.2 User Requirements

User Requirements

- Register a device or alternative contact to provide a secure method for Brunel to contact you during the authentication (logon) process, such as a SmartPhone App, mobile phone that can receive texts or a landline phone.

  If you do not register, you will not be able to use MFA - MFA is a condition of use for the University Office 365 environment and you will not be able to use the Office 365 resources (including but not limited to email, OneDrive for Business, Skype, Teams, Yammer, Forms, Sway, Planner or Video).

- Any identified compromised account will have MFA enabled immediately to continue to use University Office 365 resources.
- Without MFA using a Smartphone App (Google Authenticator, Microsoft Authenticator or app that emulate these), SMS based authentication or a landline number, Office 365 tools (including but not limited to email, OneDrive for Business, Skype, Teams, Yammer, Forms, Sway, Planner or Video) will be unavailable.
- When you attempt to log into the Brunel Office 365 environment protected by MFA, the system will "challenge" you by either requesting a "permit/allow" response or a secret security code. This confirmation request or code will be provided through the secure method you selected during registration in the MFA application. If you enter the correct code, you will be allowed into the system. Failed attempts will be handled according to current IS policies on Network Account access.
- It is your responsibility to promptly report the theft, loss or unauthorised disclosure of proprietary or personally identifiable information (PII) to the IS Service Desk.

2.3 Registration

Users will use the MFA self-enrollment process to register their authentication device(s) and, when possible, install the Mobile MFA application.

Users can add multiple MFA mechanisms (specifying one as primary) to provide alternative methods of authentication. This provides the assurance that MFA authentication can be permitted for all eventualities (e.g. ring office phone) if the primary mechanism is unavailable (e.g. they have left their mobile phone at home).

2.4 Frequency of user challenges

Once a user has authenticated through the MFA process on a specific device **for a specific app** (e.g. each of these require separate MFA; logging in to Skype, logging in to OneDrive, logging in to Outlook, using webmail using Internet Explorer, using webmail using Chrome etc.) that user will not need to use the multi-factor authentication process again for a set number of days. Also only if the user selects “don’t ask me again” otherwise it will prompt for MFA every time.

2.5 Lost or stolen devices

If you have had a device or data stolen, have lost data, or believe that an individual has broken into your computer, regardless whether University owned or personal, please contact the IS Service Desk IMMEDIATELY.

For lost or stolen devices, users can perform full or selective wipes via office 365 of their device. Brunel owned devices will be managed by Mobile Device Management (MDM) to remotely wipe Brunel information from the device when lost.

Users can remove their MFA mechanisms themselves (e.g. before they sell a phone etc.)

3.0 Exceptions

3.1 Request

There may be situations in which a User has a legitimate need to utilise Brunel Office 365 resources outside the scope of this policy. The Chief Information Security Officer (CISO) may approve, in advance, exception requests based on balancing the benefit versus the risk to the University. Exception requests should be made through IS Service Desk.

Include a brief description of the type of data you need to access. Please be certain to indicate if you handle Personally Identifiable Information (PII) or other University Confidential information, such as financial data, student academic records (e.g. grades or test scores), HR records.

3.2 Periodic Review and Recertification

Due to the evolving nature of technology, cyber threats and the changing roles of users at the University, all exemptions will be reviewed periodically and at the discretion of CISO in collaboration with Information Asset Owners (IAOs). This review will verify that the need stated in the request is still valid and/or that the employee still requires the approved MFA exempted access.