

Third Party Application Access 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	First Draft	10/08/2018
V 0.2	Andrew Clarke	Comments from Stephen Middlehurst (CBASS College IT)	22/08/2018
V 0.3	Andrew Clarke	IS System Comments – AD logs cannot be encrypted, automating staff account creation with IAM, affiliate accounts, generic account clarification	23/08/2018
V 0.4	Andrew Clarke	IS Systems comments – Student Leavers IAM process	24/08/2018
V 0.5	Andrew Clarke	Amendments / Comments Peter Hart (PWG)	29/08/2018
V 0.6	Andrew Clarke	External & Cloud systems included in the policy. PH. Amendments to define trusted and untrusted conditional based access on certainty factors such as user, device, time/date, location. PP. 2.2.1.6 Phone Home systems MFA Appendix - Any compromised account must have MFA enabled to continue to use University network resources.	07/09/2018
V 0.7	Andrew Clarke	4.0 Privileged Access Management (PAM)	15/05/2019
V 0.8	Andrew Clarke	3.0 App Control	12/07/2019
V 0.9	Andrew Clarke	Amendments - Peter Hart	30/07/2019
V 1.0	Andrew Clarke	PWG Approval – make separate policy from Network Access	06/09/2019
V 1.1	Andrew Clarke	DSB Approval	30/11/2019
V 1.1	Andrew Clarke	Annual Review	01/09/2020

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.

Owner: Michael Jenkins	Chief Information Security Officer
Signature: <i>MGJ</i>	Date: 30 Nov 2019
Approver: Pekka Kahkipuro	Chief Information Officer
Signature: <i>PK</i>	Date: 30 Nov 2019
Distribution:	

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

Contents

1.0 About this document	4
1.1 Purpose	4
1.2 Responsibilities	4
1.3 ISO27001 Conformance	5
1.4 Scope	5
1.5 References	5
1.6 Definitions	6
1.7 Objectives	6
1.8 Exceptions	7
1.9 Review	7
2.0 App Control (BYOD)	8

1. About this document

1.1 Purpose of Document

This Policy establishes the area within Brunel University London covering Application user access by means of Brunel Azure authenticated email accounts on any computer, mobile device and communications system.

Please refer to Brunel University London ISMS Document [University-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 server and network Authentication, Authorisation and Accounting (AAA) are in line with the security requirements of the ISMS.
Systems Manager	Is responsible for maintaining and managing systems policies on IT systems and infrastructure and ensuring that Authentication, Authorisation and Accounting (AAA) systems (including Multi Factor Authentication mechanisms where applicable) comply with this policy.
Network Manager	Is responsible for maintaining and managing network policies on network systems and ensuring that Authentication, Authorisation and Accounting (AAA) systems comply with this policy.
Head of Development and Application Services	Is responsible for maintaining and managing password policies on application and web systems and ensuring that Authentication, Authorisation and Accounting (AAA) systems (including Multi Factor Authentication mechanisms where applicable) comply with this policy.
Cyber & Information Security Manager	Is responsible for writing and maintaining this policy and establishing access control principles with best practice and ensuring compliance with legislative and regulatory requirements.
Cyber & Information Security Team	Responsible for assessing Cloud Due Diligence responses are compliant with Network Access Policy Responsible for investigating breaches and recommending remedial actions when network access control policy breaches have occurred.
System Owners	Are responsibility for systems access (including designating access) upon which BUL data reside. This includes, but is not limited, to Finance, HR, Registry, Library, SITS.
Security And Emergency Planning	Responsible for: <ul style="list-style-type: none"> Physical security on campus Administration of door access control systems Security of comms rooms and onsite datacentre
Operations	Are responsible for cancelling BUL cards

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

All Brunel University staff, affiliates and students with either a Brunel University-owned or personally owned device used to connect to the Brunel University network onsite and remotely

External websites and cloud systems outside IS control should ensure compliance with the Brunel University London Network Access and Password Policies. [BUL-CSP01 Cloud Security Principles](#)

This policy applies to all Privileged Access information security analysts and system administrators responsible for the maintenance of accounts and password management systems on Brunel electronic information resources.

Privileged access to non-IS managed systems, resources and applications (e.g. CHLS Qualtrics, Asite) is the responsibility of the system, resource or application owner, *not* IS. The authorisation and auditing processes involved in granting access to these resources is the responsibility of the resource owners.

1.5 References

- CESG Good Practice Guide (GPG) 10 - Remote Working v2.2
- [Brunel University London Acceptable Use Policy](#)
- [Password Policy](#)
- [MFA Policy](#)
- BUL-POL-09.02 - Network Access Policy

1.6 Definitions

- Single sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials (e.g., name and password) to access multiple applications.
- “Central Authentication Service (CAS)” is a single sign-on protocol. Its purpose is to permit a user to access multiple applications while providing their credentials (such as user id and password) only once, such as logging on to the University network.
- “Universal Credential” is the same username and password for multiple systems that have their own individual sessions. e.g. MS Active Directory credentials used by numerous services.
- “University Affiliate” or “Contractor” is someone officially attached or connected to the University who is not a student or employee (e.g., contractors, vendors, interns, temporary staffing, volunteers)
- “Information Asset Owners” (IAO) - is a person responsible for the management and fitness of data elements (also known as critical data elements) - both the content and metadata.
- Cloud access security brokers (CASB) – A Third Party Software tool or service that sits between an organisation's cloud provider's infrastructure and an organisational user. A CASB acts as a gatekeeper, allowing the organisation to extend the reach of their security policies beyond their own infrastructure. This can include encryption, device management & profiling, multi-factor authentication and single-sign-on components.
- “Multi-Factor Authentication (MFA)” is a method of access control in which a user is granted access only after successfully presenting multiple separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know e.g. password), possession (something they have e.g. mobile phone, token etc), and inherence (something they are e.g. biometrics).
- “VPN” or Virtual Private Network is a method employing encryption to provide secure access to a remote computer over the Internet.

1.7 Policy Objectives

Brunel University London information system resources are important business assets that are vulnerable to access by unauthorised individuals, compromised accounts or unauthorised remote electronic processes. Sufficient precautions are required to prevent and detect unwanted access and to protect its IS resources against accidental or malicious destruction, damage, modification or disclosure from unauthorised users in remote locations. Users should be made aware of the dangers of unauthorised access, and managers should, where appropriate, introduce special controls to detect or prevent such access.

The purpose of this policy is to protect the confidentiality, integrity and availability of Brunel University London's information by controlling access to University IS systems by Brunel University London's personnel, temporary staff, contractors, students and

service providers utilising Brunel University London's information system and to define standards for connecting to Brunel University London's network.

Brunel University London's dependency on these assets demands that appropriate levels of Information Security be instituted and maintained.

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 University London 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 University internal systems
- Minimise Brunel University London'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 University's network from any host. These standards are designed to minimise the potential exposure to Brunel University from damages, which may result from unauthorised use of Brunel University resources.

1.8 Exceptions

There may be situations in which a User has a legitimate need to utilise Brunel University technology resources outside the scope of this policy. The Chief Information Security Office 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.

When submitting an exception request, 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.

1.8.1 Periodic Review and Recertification

Due to the evolving nature of technology, cyber threats and the changing roles of users at the University all approved user 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 exempted access.

2.0 App Control (BYOD)

3.1 Apps using Azure authentication

There are risks that mobile apps pose in a bring your own device (BYOD) environment when registered (and authenticating) using the Brunel University provided login (Microsoft Azure) – example john.smith@brunel.ac.uk

Staff and students can expect to be able to install personal Apps on both their own personal smartphones and tablets and University provided smartphones and tablets. (both should be viewed from a policy perspective as BYOD)

When accessing Brunel information on a BYOD, all staff and students must remain compliant with the Brunel Acceptable Use Policy.

The University reserves the right to manage and control Apps that are registered, downloaded and installed using the Brunel University provided login that are installed on BYODs.

This management includes the option of blocking suspect or bad Apps.

The University will maintain a blacklist of Apps that users should avoid because of security concerns or other reasons,

Suspect Apps include those that:

- contain malware
- consume too much wireless network bandwidth
- do not comply with GDPR
- exfiltrate data
- attempt to harvest Brunel contacts and authentication details (usernames and passwords)
- download and embed other Apps
- hosts data in suspect geographic locations

University provided smartphones and tablets will be subject to University managed Mobile Device management (MDM) which will manage and control a combination of on-device applications and configurations, corporate policies and certificates, and backend infrastructure, for the purpose of simplifying and enhancing the IT management of end user devices.