Network 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 – remove PAM and App policies	06/09/2019
V 1.1	Andrew Clarke	Approved DSB 11/2019	30/11/2019
V 1.2	Andrew Clarke	Add NAC -1.1 Purpose; 1.6 Definition; 2.3 Endpoint Device	05/06/2020

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: MGJ	Date: 30 Nov 2019
Approver: Pekka Kahkipuro	Chief Information Officer
Signature: PK	Date: 30 Nov 2019
Distribution:	

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

Contents

1. About this document

1.1 Purpose of Document

This Policy establishes the area within Brunel University London covering who or what has authorised permission to access the University network and information.
This includes both users and endpoints and is a critical component of the zero-trust strategy in securing the University workplace.

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: • 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 endpoints* 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

1.6 Definitions

- NAC is Network Access Control, NAC intercepts the connection requests, which are then authenticated against a designated identity and access management system. Access is either accepted or denied based on a pre-determined set of parameters and policies that are programmed into the system.

- 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 it 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 Data or other University Confidential information, such as financial data, student academic records (e.g. grades or test scores), HR records.

1.9 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 Network Access Control Policy

2.1 User Access Principles

Brunel University will provide all staff, students and contracted third parties with on-site access to the information they need to carry out their responsibilities in as effective and efficient manner as possible.

2.1.1 Generic identities

Generic or group IDs shall not normally be permitted as means of access to Brunel University data and services but may be granted under exceptional circumstances if sufficient other controls on access are in place. Under all circumstances, users of accounts *must* be identifiable in order for Brunel University to meet the conditions of its Internet Service Provider, JISC (as laid out in the JISC Acceptable Use Policy).
Generic account identities, including shared mailboxes, will *never* be used to access University Confidential data or Personally Information unless an individual is identified as being responsible for the identity and takes ownership of the information. The account owner will be responsible for preventing:

- Inappropriate access to, or disclosure of, protectively marked or sensitive personal data by staff, contractors and outsiders, whether accidental or deliberate
- Inappropriate data sharing – too much or irrelevant data is shared internally i.e. a full list with all personal data is provided where only numbers of a specific category have been requested.
- Internal threat – staff acting in error or deliberately, or external parties getting your information illegally and exposing it/acting maliciously to defraud.

Generic identities will be named in such a way to ensure easy, visible and recognisable demarcation between these and individual accounts.

Shared Brunel-owned devices loaned out to “teams” generate a specific device account for that device (only) which can be accessed by the team. Each team is linked to an individual who is identified as being responsible for the identity and takes ownership of the information.

2.1.2 Privileged accounts / Least privilege

The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted, controlled and not provided by default. The University adopts the principle of least privilege.
Authorisation for the use of such accounts shall only be provided explicitly, upon written request from a senior manager (such as a head of department/division, or a departmental or centre manager), and will be documented by the system owner. Technical teams shall guard against issuing privilege rights to entire teams without the correct authorisation to prevent potential losses of confidentiality and / or integrity. (such as may happen via Ransomware attacks, which, typically, are able to encrypt user data after silently installing on a machine over which the user has admin privileges, or the creation of unauthorised user accounts)

2.1.3 Maintaining data security levels (Information Classification)

Every user should understand the classification of their data and treat them accordingly. Even if technical security mechanisms fail or are absent, every user should still attempt to maintain the security of data commensurate to their classification. The Information Classification Procedure enables users to classify data appropriately and gives guidance on how to store it, irrespective of security mechanisms that may or may not be in place.
Users electing to place information on non-IS-managed systems and databases, digital media, cloud storage, or removable storage devices are advised by IS only do so where

such an action is in accord with the information's security classification, or where other protective measures (such as the use of encryption) have been implemented. Users are consequently responsible in such situations for ensuring that appropriate access to the data are maintained in accord with the Information Security Policy and any other contractual obligations they may have to meet.
Users are obligated to report instances of non-compliance with this policy to the Cyber & information Security Team via the IT Service Desk.

2.1.4 Access Control and Authentication

2.1.4.1 User accounts

Access to Brunel University IT resources and services will be given through the provision of a unique user account and complex password. Network Account Policy

- **Staff User Accounts**
  Staff user accounts can be automatically created (IAM[1]) to improve security, ensuring that the right staff have access to the right data at the right time. This involves automatic HR data import for new staff accounts from CHIME and ensures the accurate user lifecycle support (staff entries, terminations and relocations) along with authorisation control based on roles and internal IT security policies. It is critical that HR maintain staff account details in CHIME and are kept up to date and accurate.

  Staff user accounts can also be manually created by a request in writing, and by using the appropriate forms, by departmental managers.

  No access to any Brunel University staffs IT resources and services will be provided without prior authentication and authorisation of a user's Brunel University account.

  By default, staff are provided with access to an H: space (with access denied to all other users), and an Office 365 email account.
  They have access to a standard suite of software applications.
  By default, staff accounts will expire upon termination of contract, unless a request for an extension is received from the relevant positions above the departmental manager or from relevant College Services management.

- **Affiliates of the University Access**
  Affiliate accounts (Agency, Sponsored International Researcher, Council or Senate appointment, Union of Brunel Students, LBIC - London Brunel International College, Chaplaincy, Recognised external teachers and supervisors for PGR students, Erasmus Students at other universities, Trade Union Representative and Work experience students) who are working for, on behalf of, or collaborating with the University on university business, are entitled to a network account provided that they have a written contract with the College, Department, Institute or Service that they are visiting and compliance is met.
  A Sponsor must be a current employee who can vouch for the affiliate, can request a restricted account for them in order to facilitate their work with the University. The issuing of an affiliate account will require that the sponsor accepts responsibility for the user-level management of the account, all compliance issues and data management. In order to request an account, the request must be in writing and signed by the hosting College Dean/Head of Department, a College Vice-

[1] Identity and access management (IAM) is a framework for University processes that facilitates the automatic management of electronic or digital identities. The framework includes the University policies for managing digital identity as well as the technologies needed to support identity management.

Dean/Deputy Head of Department, or the College/Department/Research Institutes Manager.
The affiliate account will have stringent restrictions placed upon it to ensure compliance with legislation and records management practice.

Affiliate user accounts can be automatically created (IAM) to improve security, ensuring that the right Affiliate has access to the right data at the right time. This involves automatic HR data import for new Affiliate accounts from CHIME if the correct affiliate details are within CHIME and ensures the accurate user lifecycle support (Affiliate entries, terminations and relocations) along with authorisation control based on roles and internal IT security policies. It is critical that HR maintain Affiliate account details in CHIME and are kept up to date and accurate.

Affiliate user accounts can also be manually created by a request in writing, and by using the appropriate forms, by departmental managers.

- **Taught Postgraduate and Undergraduate Student User Accounts**
  Taught postgraduate and undergraduate student accounts are automatically created (IAM), ensuring that the right students have access to the right data at the right time. This involves automatic SITS student record data import for new student accounts from SITS and ensures the accurate user lifecycle support (student enrolments, graduations/withdrawals and course changes) along with authorisation control based on roles and internal IT security policies. It is critical that Student Services maintain staff account details in SITS and are kept up to date and accurate.
  By default, taught postgraduate and undergraduate students are provided with access to H: space (with access denied to all other users), and an Office365 email account.
  They have access to a standard suite of software applications on Brunel owned PCs.
  The student leavers process is initiated automatically depending on the student status code within SITS[2]. Once a student transitions into one of these status codes they will be classed as either an Alumni or a Non-Graduate depending on the "reason for transfer" code (also within SITS).

  For an alumni status, an email is sent giving details about the new @alumni.brunel.ac.uk mailbox address and given two weeks' notice to transfer data to it (we do not transfer any data automatically).
  For non-Graduate, an email is sent giving details for the notice period but no alumni account.

  At the end of the notice period (two weeks), Alumni accounts will be prevented from logging on to University network PCs and Office365 apps (alumni email aside) but will retain access to Brunel Connect Services[3] for a period of time (6 months). This is to permit access in halls of residence for a number of months after completion of studies. After the 6 months the account is fully disabled and deleted 6 months later.
  For non-Graduate, the account is disabled after the 2 weeks grace period and deleted one year later.

- **Research Postgraduate Student User Accounts**
  Research postgraduate student accounts are automatically created (IAM), ensuring that the right students have access to the right data at the right time. This involves

[2] The student 'leave' status within SITS is updated by the exam boards but each college processes it differently.

[3] ResNet and Wi-Fi

automatic SITS student record data import for new student accounts from SITS and ensures the accurate user lifecycle support (student enrolments, graduations/withdrawals and course changes) along with authorisation control based on roles and internal IT security policies. It is critical that Student Services maintain staff account details in SITS and are kept up to date and accurate.
By default, research postgraduate students are provided with access to H: space (with access denied to all other users), and an Office365 email account.
They have access to a standard suite of software on Brunel owned PCs.
By default, research postgraduate students accounts will expire at the end of the term following a successful viva but will retain access to Brunel Connect Services[3] for a period of time (6 months) code (also within SITS). This is to permit access in halls of residence for a number of months after completion of research. After the 6 months the account is fully disabled and deleted 6 months later.

- **Contractors Access**
  Contractors requiring the creation of an onsite Brunel University account will have an affiliate account created. Those contractors requiring remote access have a VPN access account created in the Connect Portal at the discretion of the Chief Information Officer, and will require the support of the senior officer of the appropriate unit within the University, who will be the sponsor of the account.
  The collaborator should attend (with the letter of collaborative agreement or analogous credentials) Information Services to be registered as an account-holder for an agreed period.

- **Third parties**
  Third parties are provided with accounts that solely provide access to the systems and / or data they are contracted to handle, in accordance with least privilege and need to know principles and they must comply and sign the Third Party Remote Access Policy
  The accounts will be removed at the end of the contract or when no longer required. Unless operationally necessary (and explicitly recorded in the system documentation as such) third party accounts will be disabled when not in use.
  Exceptions to this are for some Systems infrastructure, such as storage systems, where a phone home system that allow for controlled remote access is configured. These are not embodied in accounts in IAM or AD, but in the system itself.

2.1.5 Single Sign-on (SSO)

Once authenticated to the network some network services may be accessed via an SSO mechanism

The University controls access to information on the basis of business and security requirements

The security requirements of each business application are determined by a risk assessment that identifies the information related to the application and the risks to that information

The access rights to each application take into account:

- The classification levels of information processed within that application and ensure that there is consistency between the classification levels and access control requirements
- Data protection and privacy legislation regarding access to data or services

- The “need to know” principle (i.e. access is granted at the minimum level necessary for the role)
- Everything is forbidden unless expressly permitted (Zero-Trust)
- Prohibit user-initiated changes to user privilege permissions by requiring these to be done by Administrators or authorised by the Chief Information Officer
- Any privileges that users actually need to perform their roles, subject to it being on a need-to-use and event-by-event basis
- Management of access rights is in line with the principle of least privilege

User access requests are subject to formal authorisation from the IS department

2.2 Passwords

Password issuing will be managed by the IS Service Desk. Password length, complexity and expiration times for network and Central Authentication Service accounts (ref. 1.6) will be controlled through Windows Active Directory Group Policy Objects. Systems not utilising the Windows Active Directory user account or LDAP will have their own password policies but must remain compliant with the University Password Policy.
The criteria for both staff and student passwords are:
Summary:

- Passwords must be kept secure; they should never be divulged to anyone not authorised to know them.
- Passwords should be changed at regular intervals.
- Passwords must be protected in use; in particular they should never be passed over networks in clear text and encryption (whether synchronous or asynchronous) should be used (ref BUL-POL-10.1 - Cryptographic Policy) A secured network either requires you to enter a password/encryption key to use it OR the network has a list of machines allowed to get on, and *only* those machines can use the network. *Examples, Brunel Wi-Fi University network is secured, signup4wifi is unsecure, the Wireless network provided at coffee shops is unsecured*.
- The user’s identity must be clearly established before a password is issued to a user. For example, photo identification should be checked.
- Passwords should not be overused.
  - Brunel University London usernames and passwords should not be used with non-Brunel University London systems.
  - Separate usernames and password combinations should be used for trusted and un-trusted systems. (e.g. different username/passwords for internet mail (Gmail, Hotmail, yahoo) to University network or SITS)
- Password should be complex and obscure, such that they are not easily guessed by people or computer systems (ref. Password Policy).

2.2.1 Personal Passwords

- Personal passwords should not be shared; only in exceptional circumstances will passwords be issued to groups of users (for example in order to access a team mailbox).
- Personal passwords must be kept secure; they should never be divulged to anyone, not even support staff or someone acting on your behalf (personal assistant).

2.2.2 Device passwords

- All devices connected to Brunel University London networks will have a named person responsible for that device or will be centrally managed by Information Services.

- ‘Built in’ or default user accounts should not be used if possible. These accounts should be disabled, and personal user accounts used to administer the device using “admin” group membership.
  Where inbuilt accounts must be used, only those with a need to know should have access to the password.
- Passwords for devices must be held securely with access restricted to only those who have access specifically authorised.
  A record of who knows device passwords will be kept.
  Device passwords will be changed whenever anyone who knows them has authorisation to access them withdrawn. e.g. someone leaves.

2.2.3 Authentication Data Storage

- There is a need to process Authentication Data, classified as University Confidential (username and password or code) to manage user accounts and to allow Information Systems to be able to authenticate users. Typically, Authentication Data is held electronically in directories (e.g. Microsoft Active Directory) or in databases.
- The systems holding Authentication Data should be hardened to enhance their security and should not be used for any additional purpose that might compromise their security.
- All electronic copies of Authentication data must be encrypted when possible (Windows AD and event logs are exempt from this owing to the Windows Operating System keeping event log files open while the operating system is running and locking the files in such a way that they can only be written to by the event log process)
- Authentication Data must be protected from Brute Force Attacks. (e.g. password guessing).
- Access to Authentication Data should be restricted only to the authentication process in such a way that the data is non-reversable or one-way encryption of the authentication data (Hashing). Authentication data may be replicated to systems that share authentication details such as AD, IAM, Connect, Open LDAP, Azure AD and Cisco ISE.
  Particular care is required to restrict access to password files.
- Where Authentication Data is available in plain text (e.g. print outs) staff should be aware of its sensitivity, ensuring its protection and secure disposal. Ideally username and password should be transmitted and stored in different mediums / locations.

2.3 Endpoint device and Location Access Principles

2.3.1 Compliance checks of endpoint devices (NAC, ref 1.6 Definitions) and the respective geographic location will be conducted before permitting access to the University network with varying degrees of compliance dependent upon the level of risk and confidentiality associated with the areas of University network that access is sought.

These checks will be conducted on campus endpoints during the authentication stage and at ongoing times during the period the endpoint is connected to the network.

Offsite endpoints, such as Brunel managed laptops and Bring Your Own Devices (BYOD), such as Home PC’s, will require the installation of a University provided application that can facilitate these compliance checks (NAC).

When a NAC client runs on an endpoint, it will continually check and validate to ensure the appropriate software is installed, as well as confirming the devices have updated versions or patch management. If the endpoint fails any of these compliance checks, it will be denied access to the University network or VPN until appropriate updates are made.

2.3.2 Guest access: There will be times that the University needs to allow non-employees to access the network. An exception can be requested (Ref 1.8 Exceptions) to provide guests the ability to connect to the University network with restricted access.

2.3.3 Endpoint discovery and profiling: It is necessary that all users requiring remote VPN access register their respective endpoints.

2.3.4 Enforcement: There will be times when an unregistered or unauthorised endpoint or user attempts to connect to the network. When this happens, the NAC solution will automatically disconnect the endpoint.

2.3.5 Security analytics: Network access control is an important part of the Cyber security capability. Cyber Security reserve the right to monitor the behaviour of endpoints whilst connected to the University network, either on campus or remotely via VPN, by collecting logs, flows and packets,

2.3.6 Minimum Standards
Minimum security standards for endpoints attached to the BUL network are linked to this document Minimum Standards for Security of Brunel University London Campus Networked Endpoints). These standards change periodically. Endpoint device users should consult the above link to make sure they have the latest security standards before attaching their endpoints to the network or VPN.

2.4 Access Control Methods

Access to data is variously and appropriately controlled according to the information classification levels described in the Information Classification Policy.

A proper and proportional method of authentication must be used by all users and systems accessing Brunel University Information Systems or Networks. In most cases this will be a Brunel University issued **username** and **password/passphrase** and a **managed or registered** endpoint.

Brunel University systems may be protected by Multi-Factor Authentication (“MFA”). This policy applies 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: OFFICE365, CHIME and system administration tools & privileged accounts.(BUL-POL-09.03 Privileged Access Network Policy)

Unauthenticated access will be permitted only in exceptional circumstances (e.g. kiosks) and such systems must be explicitly configured for such use.

For all computing devices (e.g. PCs, mobile devices) appropriate accounting information must be kept.

Unused accounts will be disabled, and default or blank passwords will be changed.

Access control methods include explicit logon to devices, Windows share and file permissions to files and folders, SharePoint file permissions to files and folders, user account privileges, server and workstation access rights, firewall permissions, network sone and VLAN ACLs, Webserver (e.g. IIS/Apache etc) intranet/extranet authentication rights, Brunel University login rights, database access rights, encryption and other methods as necessary.

Access control applies to all Brunel University-owned networks, servers, workstations, laptops, mobile devices and services run on behalf of Brunel University.

Role-based access control (RBAC) will be used as the method to secure access to all file-based and database resources contained within Brunel University's Active Directory domains.

2.5 Cloud Systems

The use of cloud-based systems by Brunel University must in all respects meet the access control provisions laid out in this policy and meet the University's Cloud principles
Evaluation of access controls implemented in any cloud system is performed during the vendor assessment and implementation stages of any project, via the completion by business analysts, project managers and cloud vendors of the Cloud Due Diligence Questionnaire.
All completed cloud questionnaires are assessed by the Cyber & Information Security Team, with appropriate remedial actions recommended or risks to be accepted before use is authorised.

2.6 Trusted and Untrusted Access

Access to Brunel University of London services may be withdrawn or require further steps (such as providing multiple factors of authentication – see MFA Policy) based on a number of conditions including (but not limited to) who you are, the endpoint you are using, your location, the date/time and what you are attempting to do.

Examples include:

- *You: If you are a student / member of staff, the department you belong to, the type of job you do*
- *Device: If the device is managed by Brunel or is a BYOD (Bring Your Own Device e.g. untrusted), the operating system, the security conditions (e.g. antivirus, encryption, pin code etc),*
- *Location: If you are on the University secure network, on the campus visitor network, if you are in the UK, if you are in Europe etc*
- *Time/Date: If you are within business hours, is it the middle of the night etc*