RICHMOND, THE AMERICAN INTERNATIONAL UNIVERSITY IN LONDON, INC.

ACCESS CONTROL POLICY

Version 1.0 – March 2023

_____

1. CONTEXT AND OVERVIEW

Information assets are necessarily associated with the physical devices on which they reside. Information is stored on workstations. laptops and servers and transmitted on the University's physical network infrastructure. In order to secure the University's data, thought must be given to the security of the University's physical Information Technology (IT) resources to ensure that they are protected from standard risks.

The purpose of this policy is to ensure that both logical and physical access to information and systems is controlled and procedures are in place to ensure the protection of information systems and data.

Availability, confidentiality and integrity are fundamental aspects of the protection of systems and information and are achieved through physical, logical and procedural controls. It is vital for the protection of systems and information to ensure that authorised users who have access to University systems and information are aware of and understand how their actions may affect security.

- **Availability**: systems and information are physically secure and will be accessible to authorised persons when required.
- **Confidentiality**: systems and information will only be accessible to authorised persons.
- **Integrity**: the accuracy and completeness of systems and information are safeguarded.

Authorised users referred to in this document are members of the following groups. All parties (either as part of a contract of employment or third-party contract) who have access to, or use of IT systems and information belonging to, or under the control of the University, including:

- University Staff
- University Faculty
- University Adjuncts

Any other party utilising University resources, collectively these will be known as 'Users' unless there are exceptions that apply to a specific group.

All authorised users are subject to this process.

If you are discovered contravening this policy, you may be subject to the University Disciplinary Policy.

2. CONTEXT AND OVERVIEW

All authorised users are set up with role-based access to the appropriate systems during the onboarding process.

- Access to specific systems and information will be subject to the University Starters Leavers and Mover (SLAM) process.
- Generic logons are not generally permitted across the University; however, use of generic accounts under exceptional 'controlled' circumstances is permitted, this will be managed by IT.
- The appropriate level of access to systems and information will be determined upon the prospective users required business need, job function and role.
- A signed confirmation by the user may be required indicating that they understand and appreciate the conditions of access and security. If authorisation to use systems and information is granted, unique logon credentials and passwords will be provided to the applicant. Further instructions on how to maintain the security of systems and information with due regard to the procedures below may be given.

2.1 SYSTEMS

- If an employee changes role or their contract is terminated, their line manager must follow the steps in the SLAM Process. This ensures that access to information systems is maintained and appropriate.
- If an employee is deemed to have contravened any of the Information Security policies or procedures, potentially jeopardising the availability, confidentiality or integrity of any systems or information, their access rights to the system/information will be reviewed by their line manager, HR and IT.
- If a specific access limit is exceeded or control circumvented several times by a user, the line manager, HR and IT will review the access rights of the user and if necessary remind the user of the relevant access and security.
- If a number of unsuccessful log-on attempts are exceeded, the user will be informed that they need to contact the IT Department to ask for access rights to be re-established. In these circumstances, access rights may need to be reviewed.
- If it is deemed that it is no longer appropriate or necessary for a user to have access to systems and/or information, then the user's line manager will need to inform the HR department that access rights must be altered/removed immediately.

- If any system/information rights are altered or removed, the relevant documentation will need to be updated accordingly.

2.2 AUTHENTICATION CONSIDERATIONS

The base level of security that the device must adhere to is as follows:

- All systems must be accessed by secure authentication of user validation. As a minimum this must entail the use of a username and password.
- Logon to systems/information must only be attempted using authorised and correctly configured equipment in accordance with University policies.
- After successful logon, users must ensure that equipment is not left unattended and active sessions are terminated or locked as necessary. Systems must be logged off, closed down or terminated.
- System logon data must not be copied, shared or written down.

3. PASSWORDS

All users must be appropriately authenticated. Users must follow good security practices in the selection and use of passwords.

Suitable password expiry and complexity rules will be enforced according to the level of access granted and the sensitivity of data handled.

Where necessary, additional forms of authentication will be required.

4. PHYSICAL ACCESS AND CONTROLS

Maintaining the physical security of offices and rooms where information, data and processing facilities are accessed and located is vitally important. There must be methods of physically securing access to protect information and data.

4.1 CHOSING A SITE

When possible, thought should be given to selecting a site for IT operations that is secure and free of unnecessary environmental challenges. This is especially true when selecting a datacentre or a site for centralised IT operations. At a minimum, the University's site should meet the following criteria:

- A site should not be particularly susceptible to fire, flood, earthquake, or other natural disasters.
- A site should not be located in an area where the crime rate and/or risk of theft is higher than average.
- A site should have the fewest number of entry points possible. If these criteria cannot be effectively met for any reason, the University should consider outsourcing its data in whole or in part to a third-party datacentre or hosting provider, provided that such an organisation can cost effectively meet or exceed the organisation's requirements.

4.2 SECURITY ZONES

At a minimum, the University will maintain standard security controls, such as locks on exterior doors, to secure the University's assets. In addition to this the University must provide security in layers by designating different security zones within the building. Security zones should include:

Public

This includes areas of the building or office that are intended for public access.

- **Access Restrictions**: Only open during staffed hours
- **Additional Security Controls**: None
- **Examples**: Building Reception (area prior to barriers)

Organisation

This includes areas of the building or office that are used only by employees and other persons for official University business.

- **Access Restrictions**: Only University personnel and approved/escorted guests
- **Additional Security Controls**: Access cards
- **Examples**: Hallways, private offices, work areas, meeting rooms

Private

This includes areas that are restricted to use by certain persons within the University, such as directors, facilities staff or IT personnel, for security or safety reasons.

- **Access Restrictions**: Only specifically approved personnel
- **Additional Security Controls**: Access cards or physical keys
- **Examples**: IT Comms Room

4.3 DOOR ACCESS

The use of keys and access cards or other perimeter controls is acceptable and should be used appropriately for the areas being protected.

- Employees, contractors and students have suitably authorised ID cards provided by the Estates & Facilities team.
- Employees must wear their University access cards and University lanyards to distinguish themselves from visitors who are not issued access cards and University lanyards.
- The use of access cards or keys to buildings, rooms, secure cabinets, safes etc. must be controlled and recorded. Keys must be stored in secure areas/locked cabinets when not in use and must be identifiable by recording serial/ID markings of all keys. The location of keys must be known at all times and a signing in/out recording mechanism must be maintained to record the serial/ID of keys against individual names when keys are used.
- All cupboards and under-desk cabinets are locked, and server room access is logged and requires key for escorted access or maintenance.
- Access cards must be issued to on an individual basis. Access cards must have their names and employee numbers recorded against the registered access card number including date and time of issue.
- Access cards must only be used by the registered user and must not be lent out or given to others. In emergency situations, Estates and Facilities staff can enable access.
- Access cards issued to personnel who no longer work for the University or students who have left must be deactivated and recovered immediately – a record of this action must be kept, in accordance with the SLAM process.
- Access to and knowledge of access cards, door lock codes or access to keys for locks, are restricted to authorised personnel only and must not be shared with any unauthorised person.
- Access codes used for secure locking mechanisms must be changed on a regular basis as specified by the Facilities manager in line with professional best practice.

- Direct access to secure locations, or access to adjoining offices which could provide access, must be locked and secured using appropriate locking mechanisms.

4.4 VISITORS

- All visitor details are recorded in building reception and given a visitor badge. Either escorted to the office by reception\security or received by University staff.
- Appropriate recording mechanisms need to be in place to record the names, dates, times and signatures for the signing in and out of visitors to University locations. All visitors must be accompanied by a University member of staff.
- People who are not displaying access cards must be challenged unless accompanied as a visitor. Any person not known to location personnel must be challenged in order to establish who they are and whether authorisation has been provided for them to be there. If there is any doubt about the identity of the individual, the appropriate line manager must be contacted to confirm the individual's identity.
- All contractors must have and display appropriate identification and be made aware of the requirements within this procedure.

4.5 24/7 SURVEILLANCE

The University is situated within Chiswick Park which has 24/7 security staff who both patrol and monitor CCTV covering access to the building. Additionally vehicle access to the park is restricted to registered vehicles.

4.6 PHYSICAL EQUIPMENT

Systems that store University data are often sensitive electronic devices that are susceptible to being inadvertently damaged. In order to minimise the risk of damage or theft, the following guidelines must be followed:

- Observance and maintenance of the physical security of rooms and offices where PCs and/or critical information processing equipment is located needs to be a paramount consideration. For example, do not house critical equipment in publicly accessible locations, close to windows, in areas where theft is a high risk. Locate servers and business critical equipment in locations with adequate environmental and fire controls.
- Access to information systems areas will only be allocated to staff following any required University checks.

- The external data centres that host University data are ISO 27001 compliant and have very secure access control in place.
- Environmental controls should keep the operating environment of University systems within standards specified by the manufacturer. These standards often involve, but are not limited to, temperature and humidity.
- Proper grounding procedures must be followed when opening system cases. This may include use of a grounding wrist strap or other means to ensure that the danger from static electricity is minimized.
- Strong magnets must not be used in proximity to University systems or media.
- Except in the case of a fire suppression system, open liquids must not be located above University systems. Technicians working on or near University systems should never use the systems as tables for beverages. Beverages must never be placed where they can be spilled onto University systems.
- Uninterruptible Power Supplies (UPSs) and/or surge-protectors are suggested for all core systems.

4.7 FIRE PREVENTION

It is the University's policy to provide a safe workplace that minimises the risk of fire. In addition to the danger to employees, even a small fire can be catastrophic to IT systems. Further, due to the electrical components of IT systems, the fire danger in these areas is typically higher than other areas of the University's office. The guidelines below are intended to be specific to the University's information technology assets and should conform to the University's overall fire safety policy.

- Fire, smoke alarms, and/or suppression systems should be used, and must conform to local fire regulations.
- Electrical outlets must not be overloaded. Users must not chain multiple power strips, extension cords, or surge protectors together.
- Extension cords, surge protectors, power strips, and uninterruptible power supplies must be of the three-wire/three-prong variety.
- Unused electrical equipment should be turned off when not in use for extended periods of time (i.e., during non-business hours) if practical.
- Periodic inspection of electrical equipment must be performed. Power cords, cabling, and other electrical devices must be checked for excessive wear or cracks. If overly-

worn equipment is found, the equipment must be replaced or taken out of service immediately depending on the degree of wear.

- Chiswick Park take responsibility for smoke alarm monitoring and appropriate action on a 24/7 basis.

5. BREACHES OF POLICY

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to assets, or an event which is in breach of security procedures and policies.

All University employees, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible. This obligation also extends to any external University contracted to support or access the University's infrastructure.

If you are discovered contravening this policy you may be subject to the University Disciplinary Policy or termination of any contract or service provided.

Revision History

Version	Change	Author	Date of Change
1.0	Initial version	Paul Saunders	01-03-23