1.0 ASSET PROTECTION: EQUIPMENT/ DOCUMENTATION

1.1 Protection Procedure: Purchase of New Equipment

The following procedures will help to ensure that the maximum amount of equipment is available for use, by students and staff, at all times.

1.2 In order to ensure best security practice, the Security Manager should be contacted when any order is placed for individual or multi-items of computer, audio-visual or laboratory equipment with a value in excess of £10,000. For smaller items (£10,000 or less) IT Services staff will be able to give advice on Server, PC or laptop enclosures or other IT security devices.

1.3 Procedure: Security of Equipment

All computer/ AV equipment should be secured dependent on its use:

- Public or open access facilities: IT and AV equipment should be secured or protected. Access control to the area should be considered, where ≥ £30k of equipment is in use. CCTV or IPTV should be considered to monitor the area and an intruder alarm may be installed to protect the area when not in use. The Security Manager must be informed during the planning process, so that a risk analysis can be discussed and implemented if required. IT Services should be consulted for further advice on types of bolts, devices and securing mechanisms.

- Restricted access facilities: Where ≥ £30k of equipment is in use, an intruder alarm must be installed to protect the area whenever it is not in use. The use of security devices (as above) is recommended for valuable single items. The door to the area must be double locked when the area is vacated. The area must be identified to the Security Manager, so it can be incorporated into the security team’s patrol routine.

- AV equipment should be secured to an agreed security specification, dependant on its functionality. AV staff and/ or the Security Manager will provide advice.

- All valuable portable IT equipment such as laptops and Tablets, must be locked away out of sight when not in use and especially overnight.

- A security risk analysis may be conducted by the Security Manager (in conjunction with IT Services and the University Insurers) at any time, with any resultant report or recommendations to improve security made to the HoD

- Computers should always be password protected and switched off if possible when not in use to protect them from unauthorised access to information. For further advice on security of information and acceptable IT use, see the University's IT Services web site.
  https://www1.essex.ac.uk/it/about/acceptable-use-policy/default.aspx

- For further advice on security of hardware and equipment, contact the Security Manager.

1.4 Security Hardware

All requests for the installations of locks, CCTV, intruder alarms or access control will be subject to a risk analysis. Such equipment is not to be purchased, installed or removed without prior consultation with the Security Manager who will advise on approved installers and security response. Where CCTV is installed the requirements of the Data Protection Act and then after May 2018, the EU GDPR and University CCTV Policy must be followed.

1.5 Temporary security measures must always be considered where there may be occasional additional risks such as building works, the erection of scaffolds or the removal of existing security equipment. Advice from the Security Manager must be sought during the planning of this type of work.

1.6 The installation and maintenance costs of intruder alarms, access control or other security systems in public/ communal areas will usually be meet by the EMS. The installation and maintenance costs of intruder alarms, access control, CCTV or other security systems installed in Schools or Departmental areas must be met by the School or Department. A guide to call-out repair costs and maintenance can be provided in advance of installation from the Security Manager.

1.7 Other Valuable University Property

Some other valuable University property, such as that used for Graduation ceremonies, historic documents etc. are held for safe keeping by the EMS (whilst not in use). All requests for use, display or removal are to be made to the Security Manager.

1.8 Departments who hold valuable items are to ensure that all necessary security measures have been taken to ensure there safe keeping.

2.0 Insurance Cover

2.1 The replacement cost of University property stolen through burglary may be claimed from the University's insurance. Property left in unlocked drawers, or within insecure/ unlocked or un-alarmed areas may not be covered. The insurance policy currently has an excess of £5,000 which is to be met out of the departmental budget responsible for the property. Departments are therefore advised to ensure that all valuable items are physically protected to an appropriate level. Loss of or damage to personal work related property is covered. Other personal property may be covered at the discretion of insurers.

Please see link below to the University Finance Sections web pages

https://sp.essex.ac.uk/sections/finance/SitePages/INSURANCE.aspx

3.0 Mail Receipts and Deliveries

3.1 All mail delivered to the University Post Room will be sorted, dispatched and distributed from that location to Schools and Departments throughout the University.

3.2 Internal mail will only be delivered to and collected from recognised mail points. Schools and Departments must have a secure delivery and collection point, which is visible to University staff at all times. If it is impossible to arrange constant supervision of the collection/ delivery point, then it must not be accessible to unauthorised personnel. Mail deliveries and collections from Schools and Departments within the University must never be left unattended whist on route through the University. Recorded and Registered Mail must be signed for and a record of its delivery kept in the appropriate log held in the Post Room.

3.3 The Security Section will secure mail which is delivered out of hours in the Post Room.

4.0 University Logo, Headed Paper and Stationery

4.1 Headed paper and stationary displaying the University logo, staff names, telephone numbers etc., must be treated carefully to avoid fraudulent use. Headed paper, order forms, compliments slips etc. should be locked away when not in use. Old out of date or unwanted headed paper must be disposed of correctly by shredding or using the University's confidential waste disposal system.

4.2 Any persons found using University stationery or the University logo for personal business or other purposes may be subject to disciplinary action.