

## **Acceptable ICT Asset use policy**

### **Purpose**

Define acceptable use of IT resources, which include but are not limited to computer assets, electronic communication, AIU data communication network, data applications, and any proprietary hardware used to process data on the network.

### **Scope**

This standard applies to staff, faculty, students and other workers employed by AIU including all personnel affiliated with third parties. It is the responsibility of every Information Technology resource user to know these guidelines and act accordingly.

### **Standard**

This standard provides guidelines for compliance to the ICT Acceptable Asset use policy.

### **Computer Assets**

Computer assets are defined as desktop computers, servers, laptop computers, PDA (personal digital devices), printers, routers, switches, hubs; portable storage devices (i.e. flash disks, external hard disks), digital cameras, projectors and any other device that creates, stores, processes, and exchanges AIU information.

1. AIU employees and students are responsible for the reasonable care and protection of the computer assets assigned to them and for meeting all policies and standards governing their use.
2. AIU IT department will routinely check and do software servicing and maintenance on IT assets allocated to AIU employees and students.
3. Computer assets allocated to AIU employees and students must be owned, leased, managed, and approved for institutional use by AIU IT department; and must meet specifications and requirements published by IT department.
4. AIU computer assets will be used in accordance with the [Network Use Agreement policy](#).

### **User Responsibilities**

1. Laptops must not be left unattended for prolonged periods of time.
2. University Deans/Managers are responsible to ensure that their staffs are adequately trained on appropriate use of IT equipment and that they adhere to this policy.
3. Users may not install any software, be it proprietary or free/open-source, without prior approval or consultation of academic dean and IT department.
4. Users shall not grant maintenance access to any non-employee including vendors or contractors without prior approval of IT department.
5. Users shall keep their equipment clean and free from dust.
6. Users shall not eat or drink near their computers.
7. Users are responsible for backing up files stored on their desktop or laptop. IT department does not provide backups at the desktop/laptop level.

### **Prohibited practices/uses**

1. Upgrading equipment without prior approval of the IT department
2. Downloading and/or installing programs that are not specifically approved by the IT department.
3. Using unlicensed software.
4. Copying and sharing software that is installed on university desktops or laptops with other users.

### **Avoiding laptop computer theft**

Due to their size and portability, laptop computers are especially vulnerable to theft. Faculty, staff and students should take the following precautions.

A staff, faculty or student member will be held personally responsible for any university laptop computers, equipment and/or accessories that are stolen during the time they have been assigned to that user.

Below are some tips on how to protect your laptop from being stolen:

- Do not leave a laptop in an unlocked vehicle, even if the vehicle is in your driveway or garage.
- Never leave it in plain sight. If you must leave your laptop in a vehicle, the best place is in a locked trunk. If you do not have trunk, cover it and lock the doors.
- Be aware of the damages extreme temperature can cause to computers.
- Carry your laptop in a nondescript carrying case or bag when travelling.
- Do not leave a meeting or conference room without your laptop. Take it with you.
- Never check a laptop as a luggage at the airport.
- Lock the laptop in your office or classroom during off-hours or in a locked cabinet or desk when possible.
- If theft occurs, immediately notify the IT department.

### **Compliance**

The IT department will monitor and report violations of all acceptable use policies. This will be done through a combination of remote monitoring and on-site visits.

If an IT asset is damaged, lost or stolen and the above precautions were not followed, the person whom the IT asset was provided will be held responsible for assuming part or all of repairing or replacing the laptop. The determination of responsibility will be made by Management in consultation with IT.

## User Agreement

Whereas I have been issued following assets by AIU

**IT Asset:**

**Model:**

**S/No:**

- I understand that the asset issued to me is for educational and AIU sanctioned use only.
- I understand that the asset belongs to AIU and I am the custodian of the asset.
- I understand that I have to use the asset properly and keep the asset in good working condition.
- I understand that I have to return the asset in case I proceed on long leave or in case of separation/withdrawal from the university.
- I understand that under no circumstances the asset can be withheld by me pending any settlement of final dues to me.

Assignee Full Name:

Date:

Signature:

---

IT department use

Assigned by:

Date:

Signature: