# Application and System Installation and Support Responsibilities and Requirements

## PURPOSE

The purpose of this document is to list the minimal set of responsibilities and requirements for procuring, installing, integrating or hosting applications, devices and systems at AUB and connecting them to AUB's network and infrastructure.

Once installed these systems will be subject to regular review to ensure compliance with AUB security, privacy, and other policy requirements. Non-compliant systems may be immediately shut down in order to ensure security and operational integrity of AUB systems and infrastructure.

## APPLIES TO

These responsibilities and requirements apply to anyone wishing to procure or install an application, device or system that utilizes or integrates with any data, computing, storage or network resources that are owned, operated or managed by AUB.

## WHO SHOULD BE AWARE OF THESE RESPONSIBILITIES AND REQUIREMENTS

Anyone who is interested in acquiring or installing an application, device or system that will utilize or integrate with AUB systems, data, or infrastructure.

## ROLES AND RESPONSIBILITIES

| Position/Office/Role | Responsibilities |
|---|---|
| **Requestor : Individual or department requesting a system or device** | Must ensure compliance with the guidelines defined in this document.<br><br>May consult IT prior to procuring any system or application that will utilize AUB compute, storage or network resource |
| **Office of IT (OIT)** | Monitor use of AUB IT resources, and ensure that only compliant applications, systems and devices are connected to AUB infrastructure and data resources.<br><br>OIT is responsible disconnecting any non-compliant systems, applications or devices.<br><br>OIT support responsibilities are limited to applications, systems or devices that are procured through the OIT or have the explicit agreement of the OIT to support them. |
| **Procurement Office** | Responsible for ensuring that procurement requests for systems, applications or devices, or contractors or third parties for the development or support of systems are reviewed by OIT to ensure that compliance with these guidelines are met. |

## DEFINITION & ABBREVIATIONS

- Hosting: Placing a system, device or application at any of AUB's data centers or AUB's cloud environment
- Integrating: Connecting or utilizing our infrastructure including applications, databases, network, storage or any other computing device.
- AUB Data resources: Data that is owned by AUB such as the financial, patient or student data.
- Standalone Systems or Applications: Applications, systems and devices that do not require connection to any other systems or applications

## RESPONSIBILITIES AND REQUIREMENTS

AUB Community members are encouraged to coordinate all acquisitions of applications, systems or devices that will be used at AUB or for AUB related work with the Office of Information Technology (OIT).

AUB Community members who choose not to coordinate application, system, or device acquisitions with the OIT must comply with the following:

1. **Compliance with AUB Policies:** All systems, applications, and devices used at AUB or for AUB related work must comply with all relevant AUB policies. These policies include, but are not limited to, the following:
    a. Information and computer Resources Acceptable Use Policy
    b. Identity Access Management Policy (IAM)
    c. Data Classification Policy
    d. AUB Password Standard and Guidelines
    e. Information Security framework

2. **Hosting:** Anyone requesting an application, system or device be hosted in an AUB managed datacenter or cloud environment must:
    a. Ensure that the application, system or device meets the minimal requirements for running on one of the OIT supported virtual environments. Request to Physical hardware will be assessed by OIT and approved on as needed basis.
    b. Provide OIT ahead of time with the required storage and network bandwidth requirements and projected yearly growth.
    c. Obtain OIT approval for any storage or compute needs on an annual basis. OIT may charge fees to cover hosting costs.
    d. Will be provided a cloud based infrastructure with our preferred vendor for a charge to be determined based on the need.

3. **Connection to AUB Network:** Any application, system or device that requires connectivity to an AUB managed network must be DHCP capable and Dot1x authentication compatible (for wireless networks).

4. **Integration with other AUB systems or data sources:** Anyone requesting access from an application, system or device to AUB data sources (such as Banner, EBS, FMIS, etc.) must obtain the written approval of the appropriate AUB data owner. Once approval is obtained,
    a. Access will be restricted to the specific fields or tables as outlined by the data owner.
    b. Access will be provided through API's or using OIT supported middleware (e.g. Informatica).
    c. Direct access to data, tables or records will not be provided.
    d. Applications and systems integrating with AUB's active directory infrastructure must be compliant with federation (whether SAML, Oauth, OpenID… )

5. **Security Responsibilities:** Anyone installing an application, system or device at AUB or for AUB related work, must ensure the following:
    a. All applications, systems and devices are kept current with security patches, have antivirus installed and updated, and are monitored and secure from any malware or potential vulnerabilities at all times.
    b. All applications, systems, and devices have access control capabilities, and are properly configured to restrict access to authorized users only.
    c. Applications, systems and devices will be subject to vulnerability and penetration testing by the OIT on a regular basis. All discovered vulnerabilities must be addressed immediately by the system or application owner. OIT reserves the right to shut down or disconnect any system that poses a security risk.
    d. All applications should have a logging capability that covers access logs and system logs that maybe required to investigate any security incident

6. **Support Responsibilities:**
    a. It is the responsibility of the requestor to handle all support issues related to the application, system or device they procure. This responsibility includes, but not limited to, the following:
        i. System and end user configuration.
        ii. End user training.
        iii. Working directly with the vendor or service provider for any technical support issues
        iv. Maintaining applications and API's up to date to ensure connectivity with other systems
        v. Decommissioning and retiring the systems when it is no longer used.

    b. OIT support is limited to the following:
        i. Network support:
            1. OIT will provide an IP address to network devices based on availability, and on predetermined network segments.
            2. OIT does not provide network administration for third party solutions and will help requestor on a best effort basis
            3. Maintain the virtual environment if the applications/systems are hosted at OIT.

    c. Support for applications, devices, or systems not procured through OIT will be provided on a "best effort basis". This Includes, but is not limited to, the follow:
        i. User, system and network administration
        ii. End user training
        iii. Maintenance, upgrades and system patching. Although the OIT will coordinate with the users before applying any upgrades, security updates may be applied immediately, regardless of the impact on the systems.
        iv. Configuration
        v. Vendor support

## PROCEDURE

All requests for the installation of applications or systems must be submitted to the office of IT to assess and make sure it meets the guidelines as set in this document. It is highly advisable that IT be consulted with before procuring such systems to ensure compliance.

## EXCEPTIONS

Exceptions to these responsibilities and requirements must be approved by the Office of the CIO.

## GUIDELINES COMPLIANCE

All university community members should abide by this policy. Violation of this policy will be subject to corrective and disciplinary actions.

## RELATED POLICIES AND GUIDELINES

- Information and computer Resources Acceptable Use Policy
- Identity Access Management Policy (IAM)
- Data Classification Policy
- AUB Password Standard and Guidelines

## NEXT REVIEW DATE:

*to be filled in after approval (all policies must be reviewed at least every 3 years)