**Instructions**

1. Requestor/User fills in identification information in Section 1.
2. User reads applicable policies and signs acknowledgement in Section 2.
3. Requestor/User selects appropriate access level/role in Section 4.
4. Supervisor approves system access request in Section 3.
5. The Data Steward(s) sign in Section 5 to authorize the access.
6. The Enterprise System Custodian grants authorized access and provides log-in credentials to the user.

**Routing Instructions**: On completing Section 5, route form to the ASU HelpDesk. (Reese 107). The HelpDesk will route the form to the appropriate Enterprise System Custodian for implementation.

|  |  |  |  |
| --- | --- | --- | --- |
| **Section 1: User Information** | | | |
| **Name:** |  | **Ram ID #:** |  |
| **Birthdate:** |  | **Telephone:** |  |
| **Department:** |  | **Building/Office:** |  |
| **Requestor’s Name:** | (if requestor is other than the user) | **Requestor’s Phone:** |  |
| **Classification:** | 🞏 Faculty 🞏 Staff 🞏 Consultant | | |
| **Status:** | 🞏 Part-time 🞏 Full-time 🞏 Temporary | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Section 2: User Policies Acknowledgement** | | | |
| The policies listed below govern user responsibilities regarding system access. These and other Campus Technology policies are available from the ASU Home Page🡺 Administration 🡺 Campus Technology 🡺 [Policies and Forms](http://www.asurams.edu/web/general-campus-technology/policies-procedures) page at <http://www.asurams.edu/web/general-campus-technology/policies-procedures>. Please read these policies and familiarize yourself with your responsibilities.   1. [Acceptable Use Policy](http://www.asurams.edu/c/document_library/get_file?p_l_id=733560&folderId=734593&name=DLFE-1710.pdf) 2. [Computer Accounts Policy](http://www.asurams.edu/c/document_library/get_file?p_l_id=733560&folderId=734593&name=DLFE-1713.pdf) 3. [Enterprise Systems Access Policy](http://www.asurams.edu/c/document_library/get_file?p_l_id=733560&folderId=734593&name=DLFE-1714.pdf) 4. [Password Security Policy](http://www.asurams.edu/c/document_library/get_file?p_l_id=733560&folderId=734593&name=DLFE-1715.pdf)   🞏 I have read and acknowledged the policies above and agree to abide by all applicable laws and restrictions that govern use of this enterprise system. | | | |
| **User’s Signature:** |  | **Date:** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Section 3: Supervisor Authorization** | | | |
| **Supervisor’s Signature:** |  | **Date:** |  |
| **Supervisor’s Name:** |  | **Supervisor’s Phone:** |  |
| **Supervisor’s Title:** |  | | |
| **Supervisor’s Email** |  | | |

|  |  |
| --- | --- |
| **Section 4: Access Level/Role** | |
| **Account Request:** | 🞏 New Account 🞏 Modify Account 🞏 Remove Account |
| **Role/Access Level** (check one)**:** | 🞏 Guest 🞏 Standard User 🞏 Workgroup Administrator |
| **\*\* OIIT ONLY\*\*** | 🞏 IT Intern 🞏 Helpdesk Analyst 🞏 Application Administrator  🞏 Domain Administrator |

|  |  |  |  |
| --- | --- | --- | --- |
| **Section 5: Data Steward(s) Authorization** | | | |
| **Data Steward A:** | Director, Technology Support | | |
| **Data Steward’s Signature:** |  | **Date:** |  |
| **Data Steward B:** | VP, Office of Information and Instructional Technology (OIIT) | | |
| **Data Steward’s Signature:** |  | **Date:** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Section 6: Enterprise System Custodian** | | | |
| **Account Action:** | 🞏 Account Created 🞏 Account Modified 🞏 Account Deleted/Disabled | | |
| **Account Settings:** | User Name: | | |
|  | 🞏 Training Required 🞏 User has completed training | | |
|  |  | | |
|  |  | | |
| **Custodian’s Name:** |  | **Date Completed:** |  |

**Access Levels**

* **Guest:** This permission is reserved for non-ASU users. Access is temporary and permissions are extremely limited.
  + Run local software applications
  + Access the internet
* **Standard User:** This is the default permission for ASU faculty/staff/students.
  + Run software applications
  + Access the internet
  + Access to network resources (printers, copiers, etc)
  + Create files/folders/setting changes to own account
* **Workgroup Administrator:** This permission is reserved for lab managers and [non-OIIT] departmental technical support staff in order to perform administrative tasks on workstations within their support area.
  + Install/Uninstall hardware and software
  + Access all files and folders on a workstation
  + Make system/setting changes on a workstation
  + Manage print jobs

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* OIIT ONLY\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Access Levels**

* **Intern/Student Worker : Manage Lab Computers, install software, hardware on lab computers as assigned**
* **Helpdesk Analyst: Administer all applications and software installed on desktop computers**
* **Application Administrator: Administer/Manage assigned applications and log onto required servers.**
* **Domain Administrator: Full access to domain and all applications/ desktops/ servers**