**Florida State University**

#### ITS Data Access Request

***LDAP Proxy Request***

**Department:**

**Requested by:**

**Date:**

**CRM:**

**Service Now: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# Requestor / Approvals

Please complete the information in each column. Add the names of “additional contributors” to ensure that persons who are involved in the process have been included in the development of this request.

**Requestor Information:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Name** | **Phone** | **E-Mail** |
| **Project Sponsor - Dean, Dept. Head, Chair** |  |  |  |
| **Requestor** |  |  |  |
| **Technical Contact - Department** |  |  |  |
| **Technical Contact - Vendor** |  |  |  |
|  |  |  |  |
| **Additional Contributors** |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Approvals: (request approval, sign and acknowledgement)**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Name** | **Job Title**  | **Signature** |
| **Consumer Dean, Dept. Head, Chair / Project Sponsor** |  |  |  |
| **Data Steward(s)** | Kim Barber | Director, HR Operations |  |
|  | Phaedra Harris | Director, Acad & Stu Services |  |
|  | Bill Hunkapiller | Director, Info Security & Privacy |  |
| **Technical Signoff - move** |  |  |  |

## 1.1 Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Updated By** | **Description of Change** |
| 1.0 |  |  |  |
| 2.0 |  |  |  |
| 3.0 |  |  |  |
|  |  |  |  |
|  |  |  |  |

##

# 2 Access Request Description

## 2.1 Executive Overview

Please provide 1-2 succinct paragraphs that describe the nature and purpose of the data access request in language that a reader not intimately familiar with this business process, application, system, etc. will understand.

# 3 LDAP Details

|  |  |
| --- | --- |
| Application Name |  |
| Target Date for Production |  |
| Production IP addresses |  |
| Development IP addresses |  |
| Who will access the application (Students, employees, applicants, etc.) |  |
| Attributes to be stored by application Y/N |  |
| Primary Contact (Name and email) |  |
| Secondary Contact (Name and email) |  |
| Group Contact (Name and email) |  |

Uid (FSUID) and objectClass are automatically released.

Request attributes.

|  |  |  |
| --- | --- | --- |
| Attribute Name | Description | Request this attribute |
| fsuEduFirstName | Legal first name |  |
| fsuEduLastName | Legal last name |  |
| fsuEduPreferredFirstName | Preferred first name (not populated if not set in PeopleSoft. |  |
| fsuEduPreferredLastName | Preferred first name (not populated if not set in PeopleSoft. |  |
| fsuEduAffiliation | Affiliation example Student, Employee, Retiree, ApplAdmit etc. |  |
| fsuEduOfficialEmployeeEmail | Employee email @fsu.edu |  |
| fsuEduOfficialStudentEmail | Student email @my.fsu.edu |  |
| userPassword | Password for authentication only accounts.  |  |
| fsuEduEMPLID | EMPLID from PeopleSoft |  |
| employeeStatus | Active or does not exist |  |
| fsuEduStudentStatus | C for continuing, ENROLLED for currently enrolled or does not exist |  |
| displayName | Legal Name (prefix, first, middle, last, suffix) |  |
| Request Additional attributes |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# *4.0      Data Security*

By signing this document, you agree to the following:

Security controls to protect data as required per data classifications of Protected, Private, and Public will be implemented, monitored, and maintained (For more information, refer to the University Data Classification Guidelines.) .

Data will be shared only with individuals authorized.  This DAR does not authorize sharing this data with other campus units, external entities, or third-parties.

Data will be used only for the intended purpose documented in the data sharing agreement.

If the requester transfers to another campus unit or leaves the University, the Department will notify the Data Access Request group as soon as possible, not to exceed three days beyond the separation.

Any suspected or confirmed unauthorized access of Protected or Private data will be reported to the FSU Office of Information Security and Privacy (ISPO) within 24 hours of discovery.