P U R D U E U N I V E R S I T Y

Service Level Agreement (SLA)

Between the Identity and Access Management Office (IAMO) and the designated Purdue University administrative or academic group (the Client) for the electronic distribution of Purdue University network services to the Client for purposes of identification, authentication and authorization.

I. PARTIES

This document constitutes an agreement between the designated Purdue University administrative or academic group, called the Client, and the Identity and Access Management Office (IAMO) of the IT Networks and Security (ITNS) group within the Office of the Vice President for Information Technology (OVPIT).

II. PURPOSE

A. Background and Goals

1. The purpose of this Service Level Agreement (SLA) is to define the practices, guidelines, approvals, and security requirements for Client's access to the Purdue University identification, authentication, and authorization services provided by the IAMO.

B. Definitions and Principles

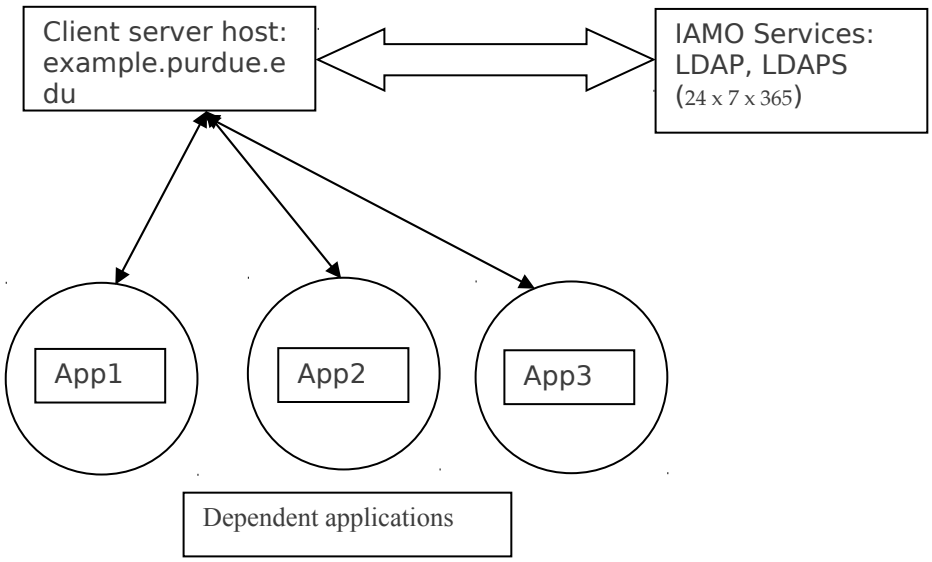
1. For the purposes of this SLA, *Purdue University* includes, but is not limited to, the West Lafayette Campus, other Purdue campuses including Statewide Technology, Continuing Education, and other official Purdue stakeholders.
2. The IAMO is the steward of identity, authentication, and authorization data used to identify, authenticate, and authorize entities that use Purdue University information technology resources.
3. The IAMO provides network-based identification, authentication, and authorization services to approved Clients. For the purposes of this SLA, these services will hereafter be called the *IAMO Services*.
4. Approved *Clients* are Purdue University administrative and academic groups for whom the use of the IAMO Services is necessary for conducting official business, and to support distributed operations.
5. Best security practices will be used to administer the Client systems which access the IAMO Services, and the IAMO systems which provide the services. Best security practices for different computing environments are given at the

"SecurePurdue" web site: http://www.purdue.edu/securepurdue/bestPractices/adminResources.cfm. Best practices change over time, and Client systems are expected to follow best practices as they evolve.

6. The IAMO Services may return incidental data as part of the normal operation of their protocols. The Client will hold any incidental data received in strict confidence according to best security practices and current regulations, will not capture or retain local copies of the data except as explicitly permitted by this SLA, will use the data only for the purposes defined in this SLA, and will not redistribute it to or make the data available for use by any third party. *For definitions of each service type please see Appendix B: Service Definitions.*

7. A *Service Configuration* comprises:

1) The IAMO Services being provided by the IAMO servers to the Client host and their *Service Levels* (see (8) below);
2) The Client host acting as the consumer of the IAMO Services; and
3) The Client applications that depend directly or indirectly on the Client host because of its access to the IAMO Service.
4) These dependent Client applications may be hosted on the Client host or some other host, but if they depend on the Client host's access to the IAMO Services then they are part of the Service Configuration. (See Example 1)



Example 1: Service Configuration

8. A *Service Level* specifies the hours during which a specified IAMO Services is expected to be available. Current Service Levels are University Business Hours (8:00 AM-5:00 PM Monday-Friday) and "24 x 7 x 365*" (continuous availability). Service Levels are part of a specific Service Configuration. N.B.: All Service Levels are subject to planned downtime announced through the ITaP Change Management Forward Schedule of Changes (FSC). Planned downtime announced through the FSC shall not be considered a violation of the agreed upon Service Levels.

III. RESPONSIBILITIES

A. The Client:

1. Agrees to the specific Service Configurations listed in Appendix A.
2. Agrees to provide, as requested by the Director of the IAMO, information on the Client's use of the IAMO Services.
3. Agrees that the initial and production security requirements for Client hosts listed in Service Configurations in Appendix A of this SLA must be met before the SLA comes into force.
4. Agrees to follow best security practices as described on the SecurePurdue web site (http://www.purdue.edu/securepurdue/bestPractices) in the administration of Client hosts listed in Service Configurations in Appendix A, and agrees to provide, at the request of the Director of the IAMO, information pertinent to the best security practices used to administer those Client hosts.
5. Agrees to use the IAMO Services only for the purposes defined in this SLA.
6. Agrees to notify the IAMO prior to any proposed changes to an existing Service Configuration, including but not limited to, additions to or changes of any dependent applications.
7. Agrees to report interruptions and errors in the IAMO Services to the IAMO or a designated agent of the IAMO (e.g., the ITaP Customer Service Center).
8. Agrees to abide by Purdue's Information Technology Incident Response Policy (http://www.purdue.edu/policies), and agrees to report all security incidents to the IAMO, including, but not limited to, logged events that show, or may show, compromise of any of the Client hosts or applications that use the IAMO Services directly or indirectly.
9. Agrees to perform, or allow to be performed, both initial and subsequent security audits of the Client hosts as specified in the Service Configurations in Appendix A.

10. Agrees to subscribe to the ITaP Change Management notification system in order to receive notice of planned changes and enhancements to the IAMO Services, and notifications of unplanned outages.
11. Agrees to provide and maintain complete and accurate information for the designated technical contact's campus email address and campus phone number.

B. The IAMO:
1. Will receive the signed Client SLA and arrange for secure access to the IAMO Services by the Client hosts, as specified in the Service Configurations given in Appendix A.
2. Will monitor the IAMO Services to ensure their correct, reliable and secure delivery per the agreed Service Levels requested in Appendixes A.
3. Will notify the Client in advance of any planned changes or enhancements to the IAMO Services, by posting notice to the ITaP Change Management system. The Client will be notified of planned changes and enhancements through the Forward Schedule of Changes (FSC) published by ITaP's Change Management system.
4. Will notify the Client of any unplanned interruptions to or errors with the IAMO Services, by posting notice after the fact to the ITaP Change Management system.

IV. TERMINATION

A. This SLA may be terminated by the IAMO for any reason or for no reason, ninety (90) days after presentation to the Client of a written notice of termination signed by the Director of the IAMO.
B. This SLA may be terminated by the Client for any reason or for no reason, thirty (30) days after presentation to the IAMO of a written notice of termination signed by the school or department head who authorized this SLA, or his or her successor or designee.
C. This SLA may be temporarily suspended *without notice* by the IAMO in case of emergency. If possible, the IAMO will attempt to notify the Client if service is suspended for this reason. A temporary, emergency suspension shall not be considered a violation of the agreed upon Service Levels.

V. MODIFICATION

A. This SLA may be amended upon request from the Client's designated technical contact and upon approval by the Director of the IAMO. Such modifications may include: (1) adding new Service Configurations; (2) deleting existing Service configurations; (3) modifying existing Service Configurations; (4) designation of a new technical contact; (5) changes to the

technical contact's email address or campus telephone number. These modifications shall not alter any of the other terms of the SLA.

B. This SLA may also be modified after thirty (30) days notice from the Director of the IAMO to the Client if such modifications are required due to changes in state or federal laws, administrative regulations, University policies, or commonly accepted best security practices.

VI. PENALTIES

A. Violations of this SLA by the Client or the IAMO will be adjudicated by the OVPIT Executive Director of Networks and Security.

B. Penalties for Client violation of this SLA include, but are not limited to, the temporary or permanent suspension of Client access to IAMO Services.

VII. CLIENT DEFINITIONS

A. For the purposes of affecting this SLA, these specific Purdue University Client definitions are in force:

1. Area Name:_____
___

2. Department or School:_____
___

3. Department or School Head: _____
___

4. Service Configurations: See Appendix A

VIII. SIGNATURES

A. Department or School Head

Print Name:_____

Signature_____

Date_____

B. IAMO Director:

Print Name:_____

Signature_____

Date_____

IX. Appendix A: Service Configurations

Instructions: For each Service Configuration requested, please complete sections A, B, C, D and E below, making as many copies of this page as necessary. For definitions of each service type please see Appendix B: Service Definitions.

A. Technical contact information:

1. Name: _____
2. Campus Email Address: _____
3. Campus phone: _____

B. Client host DNS) name and IP Address (This **must** be the FQDN and static IP Address registered in DNS for each Service Configuration):

_____

_____

_____

C. Services requested (for each service below, please mark either "yes" or "no" in the "Service requested" column, and check mark one of the "Service Level Desired" columns. N.B.: either of the Service Levels is subject to planned downtime announced through ITaP's Change Management system.

Service type	**Service requested (yes, no)**	**Service Level Desired: 8:00 AM-5 PM Monday-Friday**	**Service Level Desired: 24 x 7 x 365***
CAS			
I2A2 identification (SSL)			
I2A2 authentication (SSL)			
I2A2 authorization (SSL)			
I2A2 LDAP			
I2A2 LDAPS (SSL)			
I2A2 RADIUS (Pal 1)			
BoilerKey Service			
Apache LDAP authentication			

D. Dependent Client Applications (please add additional lines as needed)

App. Name	Website URL if Applicable	Description of Client Application

Appendix A continued on next page.

E. Local data caching requirements. Please list any requirements to make local copies of any data received through the IAMO Services. If you do not plan to cache data, **please answer "none".**

Appendix B: Service Definitions

1. Central Authentication Service (CAS) - single sign-on for the web (http://www.ja-sig.org/products/cas). We prefer CAS to I2A2 authentication if both solutions are appropriate for the client system.

2. I2A2 identification (SSL) – service for lookup of specific identification attributes given an individual's personal key.

3. I2A2 authentication (SSL) – service for proving an identity by supplying a password.

4. I2A2 authorization (SSL) – service for determining that the proven identity has the correct set of characteristics for authorization to the requested resources.

5. I2A2 LDAP – I2A2 to LDAP protocol converter that understands a limited subset of the Lightweight Directory Access Protocol, described in RFC 2251. I2A2 LDAP requires the start TLS protocol for encryption.

6. I2A2 LDAPS (SSL) – I2A2 to LDAP protocol converter that understands a limited subset of the Lightweight Directory Access Protocol described in RFC 2251 using SSL encryption.

7. I2A2 RADIUS (Pal 1) – I2A2 to RADIUS protocol converter that enables authentication via the Remote Authentication Dial In User Service (RADIUS), described in RFC 2865.

8. BoilerKey – RSA Two-Factor authentication for SAP portal and various clients that need the additional security of two factor authentication.

9. Apache LDAP Authentication (http://directory.apache.org/) – An embeddable LDAP directory server entirely written in Java. This is to be used with services that are unable to use CAS authentication.