IT Service Level Rules Policy DRAFT
Version 6.0 5/07/08

Policy: The University will define Basic Information Technology Services and maintain IT Service Level Rules, as operational policy approved by the ISPC, that specify the availability of services to members of Pacific's user community.

KEY POINTS OF THE POLICY

1. This policy establishes the idea of Basic Services and details what services are available to faculty, staff, students and other members of Pacific's user community.

MISCONCEPTIONS REGARDING THIS POLICY DISPELLED

1. The Office of Information Technology does not provision services arbitrarily.

2. This policy does not prescribe particular implementations, but particular service level rules may strongly influence implementation.

COSTS

1. Extending or limiting services to different classes of users can affect the cost of provisioning, especially for those services with per person licensing components.

1. What is the name of the proposed policy?
>   IT Service Level Rules Policy

2. What is this policy about?
>   This policy establishes who gets what Information Technology services and for how long.

3. How does this policy relate to existing policy?
>   This policy builds on the following IT Policies:
>   Email Policy
>   Data Retention Policy
>   Accountability Policy

4. How does this policy relate to our direction for technology?
>   It is imperative that we establish a common understanding of what IT systems and services are provided to the various classes of user in the Pacific Community. Without these rules, OIT will not be able to successfully provision and de-provision services.

5. Why do we need it now?
>   These Service Level Rules have been in an interim state for the last few years. However, the increasing centralization of core IT systems and services makes this more and more a three-campus issue. By making this a University Policy, it can be more formally dealt with by the Information Technology Strategy and Policy Committee.

6. How will this policy affect operations and behavior?
>   This policy will form the basis of a common understanding that can lead to more uniform implementations, greater efficiency and lower costs.

7. What are the potential undesirable effects or impacted populations?
>   All three campuses should work towards a common provisioning standard. This may impact various populations, either granting more access, or limiting access.

8. What are the barriers to acceptance of this policy?
>   The time involved to sort this all out.

Policy: The University will define Basic Information Technology Services and maintain IT Service Level Rules as operational policy approved by the ISPC, that specify the availability of services to members of Pacific's user community.

Note that the line above is University Institutional Policy and that what follows is University Operational Policy. Both are approved by the Information Strategy and Policy Committee (ISPC).

Definitions

Authentication is the process for confirming who a person is.

Authorization is the process of enabling them to access any particular institutional service.

Status is the classification or set of classifications associated with an individual. For example, current faculty, former staff, prospective student, alum, etc. are statuses. A person's status generally has a precise definition and is stewarded by a corresponding administrative office. In practice, a person's status may change with some regularity and the appropriate authorization changes need to stay in sync.

Identity Management System (IMS) is the set of systems and services that manage authentication and authorization.

Person Registry is a database within the IMS that relates people to their status.

Service level prescribes and documents what services are associated with what university statuses. They are operational policy.

Service Level Engine is software that scans the Person Registry looking for status changes and/or new entries. When a new entry or change is found, the Service Level Rules are applied and the appropriate authorizations are granted or taken away. (Technically, the Service Level Rules Engine sends messages via a connector to individual applications asking them to create accounts, remove accounts, add or remove a user from an access list, and other functions.)

Basic IT Services are those core IT services made available to most members of the Pacific Community.

Authorized Registrant (AR) a person who, as OIT is able to distribute that capability, has the ability to authorize individuals for additional services and/or override the status based specifications below, case by case, under appropriate administrative approval. It is envisioned that ARs in each school or major administrative unit would be empowered to act as necessary according to their units needs.

1. Background

As more and more of our business processes are put on-line and, generally, made accessible through the web, it becomes increasingly important to know who is using our systems and what services to deliver to them as authorized users according to their statuses. This is not simply a matter of security; it is also a matter of appropriate resource management.

Implementation of agreed upon Service Level Rules is fairly straightforward. It is the agreement on, and the documentation of, the Service Level Rules that takes the time. OIT stewards the Service Level Rules as it is the major stake holder in their implementation.

Prerequisite to all services:

1) A PacificNet ID and password (including access to password recovery systems). This is a for-life service, unless otherwise noted.

Basic IT Services

1) Access to PacificNet* on campus via wireless (based on local availability)
2) Access to PacificNet* on campus via hard line
3) Access to PacificNet* from off campus via VPN (some restrictions may apply)
4) Access to appropriate applications via InsidePacific, including but not limited to:
     a) Authenticated Library Services
     b) Authenticated PacificCard Services
     c) Authenticated White Pages Directory Services (and derivative Telephone Directory) that enable update of demographic information (as permitted)
     d) Authenticated Parking Services (as applicable)
     e) Authenticated participation in the emergency notification system, PacificConnect

PacificNet access requires compliance to Pacific's Security Standards and acceptance of Pacific's Appropriate Use Policy. Other restrictions may apply.

Notes:
     i) Basic IT services include access to help through representatives of the OIT Customer Support Center (some restrictions apply) or locally the Unit level. While this is not currently an authenticated service, an eligibility flag likely needs to exist in the Person Registry.

     ii) Basic IT services do not include actual computer equipment and/or local support. Those are supplied at the discretion of the units.

     iii) In addition to individual space, departmental shares get 250 meg/person and additional space may be leased at the current OIT established rate.

Group 1: Current Faculty

1) Basic IT Services
2) Assignment of an email box and pacific.edu email address
3) File and web space on PacificSpace (250meg/person)
4) Access to joint Calendaring (Exchange)
5) Dial-tone and a telephony account (for on-campus offices)
6) Access to appropriate *additional* applications via InsidePacific, including but not limited to:
     a) Authenticated access to courses taught (if any), including grade entry
     b) Appropriate access to Banner for Student System management **
     c) Authenticated Employee Self Service Applications
     d) Other applications by specific individual authorization
7) Access to the Blackboard Course Management System

** *Banner access may be granted by the appropriate information steward and expires on the date of termination unless extended in writing signed by a Cabinet member and the University IT Security Officer.*

Group 2: Admitted Students

1) Basic IT Services

2) Provisioning of Email addresses of the form xxx@yyy.pacific.edu pointing to email boxes provided by a third party.

Group 3: Admitted students who do not matriculate

1) All Services are terminated at a specified <u>Non-Matriculation Date (NMD)</u> [Oct. 1st.]
    a) Their PacificNet ID is recycled.

Group 4: Current Students

1) Basic IT Services
2) File and web space on PacificSpace (250meg/person)
3) Dial-tone and a telephony account (for on-campus housing)
4) Provisioning of Email addresses of the form xxx@yyy.pacific.edu pointing to email boxes provided by a third party.
5) Access to appropriate *additional* applications via InsidePacific, including but not limited to:
    a) Authenticated access to courses taken
    b) Authenticated access to Telephony Accounting System
    c) Authenticated Student System Self Service Applications
6) Access to the Blackboard Course Management System (CMS)
7) Access to the Blackboard e-Portfolio System (ePS)

Group 5: Current Staff, including supplemental staff

1) Basic IT Services
2) Assignment of an email box and pacific.edu email address.
3) File and web space on PacificSpace (250meg/person)
4) Dial-tone and a telephony account (for on-campus offices)
5) Access to joint Calendaring
6) Access to administrative applications (as authorized)
7) Access to appropriate *additional* applications via InsidePacific, including but not limited to:
    a) Authenticated Employee Self Service Application
    b) Other applications by specific individual authorization
8) Access to the Blackboard Course Management System (CMS)

Banner access may be granted by the appropriate information steward and expires on the date of termination unless extended in writing signed by a Cabinet member and the University IT Security Officer.

Group 6: Emeriti

1) Basic IT Services
2) Access to appropriate *additional* applications via InsidePacific, including but not limited to:
    a) Authenticated Employee Self Service Applications (Residual Information)

Group 7: Surviving Spouses and Domestic Partners of Deceased Emeriti
(Did not include Basic IT Services)

1) Access to appropriate applications via InsidePacific, including:
    a) Authenticated Library Services
    b) Authenticated PacificCard Services
    c) Authenticated White Pages Services (and derivative Telephone Directory)
    d) Authenticated Parking Services (Complimentary)

Group 8: Former Employees -Good Graces (not Emeriti)

1) Residual email box access for 3 months
2) Email forwarding for one year. After one year, the email address is recycled
3) Residual access to their file space for 3 months.
4) InsidePacific access including, but not limited to:
      a) Residual and/or historic information (only) supplied by Banner Self Service for
       Employees, if any, for a period of 5 years.
5) After the 3 months, email box and file space falls under the Data Retention Policy retroactive to separation. In any event, access after 3 months is only available by HR authorization. Retrieval fees may apply.

Banner access expires on the date of termination unless extended in writing signed by a Cabinet member and the University IT Security Officer

Group 9: Former Employees - Terminations

Note: Employees that do not leave in good graces (as indicated by HR), including former faculty, are, in general, immediately un-authorized for any services, except:

1) Residual and/or historic information (only) supplied by Banner Self Service for Employees, if any, for a for a period of 5 years.
2) Email box, file space and CMS content (if any) is subject to Pacific's Data Retention Policy, as applicable, from the date of termination. In any event access is only available by HR authorization. Retrieval fees may apply. Note that the email address is recycled, immediately.

Note: Banner access, if any, expires on the date of termination. No exception is provided.

Group 10: Former Students (as defined by the registrar)

1) Residual access to their file space for 6 months from designation.
2) Access to appropriate applications via InsidePacific
3) After the three months, file space (if any) is deleted.
4) Email address is retained (without time limitation).
5) Residual access to ePortfolio for 6 months from designation.

Group 11: Alumni (As defined by the Alumni Office)

1) Residual access to their file space for 12 months. After the 12 months, file space (if any) is deleted.
2) Access to appropriate additional applications via InsidePacific, including but not limited to:
      a) Authenticated White Pages Services
3) Email address and box are retained (without time limitation) for students provisioned through a third party. All other students receive forwarding only for 6 months.
5) Residual access to ePortfolio data (if any) for 12 months. After the 12 months, ePortfolio data is deleted.*

Group 12: Current Regents

TBD

Group 13: Former Regents/Former presidents

TBD

Group 14: Parents of Current Students

TBD

Group 15: Parents of Alumni and Former Students

TBD

Group 16: Unclassified Students (those not admitted, but taking courses)

1) Basic Services
2) Provisioning of Email addresses of the form xxx@yyy.pacific.edu pointing to email boxes provided by a third party.
3) Access to the Blackboard Course Management System (CMS)
4) Access to the Blackboard e-Portfolio System (ePS)

Group 17: Former Unclassified Students.

 1) Residual access to email for 3 months from designation.
 2) Residual access to ePortfolio for 3 months from designation.

Group 99: None of the above.

1) Services and authorizations as assigned by the Unit's AR on a case by case basis.