Overview of USF’s Affiliate/Guest (“VIP”) system, as of February 2011

1. **Applicable Policy/Regulations/Standards:**
    a. Be able to trace each user of a “restricted” USF service back to an identity record and, if the person is not directly a member of USF, to a (Faculty/Staff) sponsor that is.
    b. Certain service-providers, such as the ID-Card Office and Wireless-Network group, can establish local, temporary identities and identifiers for providing their services to guests in accordance with their own policies and procedures; however, those identities and identifiers must be clearly differentiated from the USF system-wide identities and identifiers, even for guests.
    c. Separate the “guest” population into 2 main groups, especially for determining eligibility for services and retention:
        i. Sponsored ones, which we have more confidence in their identity, since a USF employee is held responsible – These are eligible for services based on their group membership, just like people from the student and employee systems-of-record.
        ii. Self-registered (deferred to a future release) ones, which we have little trust in their identity, since it’s self-reported with minimal verification – So far these are only eligible (even if they provide “sufficient identifiers”) for disposable NetIDs and disposable ID-Cards.
    d. For sponsored “VIPs”, require at least the following minimal pieces of identity information, but also allow collection of other pieces (e.g. planned location on campus):
        i. First-name
        ii. Last-name
        iii. Date-of-birth
        iv. Email-address (obviously external)
        v. Phone (within USA only)
        vi. Group membership
            1. Group sponsor (employee/staff)
            2. Planned end-date (if any)
    e. For self-registered “VIPs”, plan to require at least the following minimal pieces of identity information, but also allow collection of other pieces (e.g. phone):
        i. First-name
        ii. Last-name
        iii. Date-of-birth
        iv. Email-address (obviously external)
        v. Phone (within USA only)
    f. For sponsored “VIPs”, apply the same “sufficient identifiers” restriction (which we have as our “silver rule” – you must have a first-name, last-name, and date-of-birth or SSN) before allowing them to “feed” elsewhere.
        i. For example, people who don’t meet our “silver rule” are kept out of our central person-registry and do not receive an official USFID (e.g. U12345678). At best they can receive a temporary Affiliate-ID (e.g. A12345678), which is treated differently by our service-providers.

g. For self-registered "VIPs", plan to support an "open ID" or create a temporary USF NetID (e.g. 'usf001') during the web registration process, and deliver the activation code via email or phone. Create ID-Card upon demand (at the ID-Card office, not online).
    i. Do not allow password resets on temporary NetIDs.
    ii. Purge temporary USF NetIDs after a set period of time, e.g. 3 months.

h. For all "VIPs", ensure that provisioned-services are appropriately terminated (for "guests/VIPs" too) upon the end-date of the corresponding sponsorship/affiliation, typically 6 months after being added to the group. Note that ID-Cards cannot be "terminated", but their status can be set to "inactive".

i. Also ensure all "guests/VIPs" are included in periodic audits of (active) provisioned-services versus current university roles/affiliations.

2. External Requirements:

a. Make it relatively easy for "trusted" USF employees to sponsor a guest (visiting researchers, volunteers, external auditors, etc.) for services. Also make it relatively easy for sponsors to *manage* their guest(s), including ending their relationship earlier than planned, or extending it beyond originally planned.

b. Reduce the need to put identity-records in the student and employee systems of non-student-related-people and non-employee-like people, e.g. contractors, volunteers, seminar-attendees, summer-campers, vendors, external auditors, trustees.
    i. This is not to be used to "shortcut" the employee identity creation process.

c. Eventually offer a self-registration capability, so that minimal (virtually "public") services like wireless-access and open-use computer-labs can be automatically provisioned without involving a USF sponsor.

3. Internal Requirements:

a. Provide a means (at least manually by the IT-Security office) to provision and de-provision "trusted sponsor" status to employees. So far only a few dozen appear necessary, but we must allow for this to increase as more people become aware of the new process and stop using undesirable methods for getting their guests into USF systems.

b. Allow the same employee to sponsor multiple "guests/VIPs" groups, and allow multiple employees to be sponsors of a group, but keep a record of who added/sponsored each guest.

c. Use a single identifier in the provisioning system for both "guests/VIPs" and identities from our (student and employee) systems-of-record.

d. Since we want to store more attributes (and history) than are directly relevant to our provisioning system, use a place outside of (at least the "normal" portion of) the provisioning system to store "system of record" information that can vary over time about "guests/VIPs" (e.g. someone sponsored by the Math department one year might come back the following year sponsored by the Physics one).
    i. Since our provisioning system is "homemade", we could do this by adding a few extra tables and web pages.

4. Links:

a. http://it.usf.edu/services/netid/vip-netid