1. Federation Participant Information

1.1 The InCommon Participant Operational Practices information below is for:

InCommon Participant organization name

2.2 ´0HPEHU RI &RPPXQLW\µ[4] is an assertion that might be offered to enable access to resources made available to individuals who participate in the primary mission of the university or organization. For example, this assertion might apply to anyone whose affil LDWLRQ LV ´FXUUHQW VWXGHQW IDFXOW\ RU

What subset of persons registered in your identity management system would you LGHQWLI\ DV D ´0HPEHU RI &RPPXQLW\µ LQ 6KLEEROHWK InCommon Participants?

Faculty, staff and active students

2.3 Please describe in general terms the administrative process used to establish an electronic identity that results in a record for that person being created in your electronic identity database? Please identify the office(s) of record for this purpose.)RU H[DPSOH ´5HJLVWUDU·V 2IILFH IRU VWXGHQWV +5 I

The Office for Student Assistance is responsible for collecting and managing student information. Faculty and staff information is managed by Human Resources. Student, faculty, and staff records are maintained in our University ERP database and electronic credentials (userids) are generated via an automated process based on the information contained in these records. This automated process is managed by Information Technology Services.

2.4 What technologies are used for your electronic identity credentials (e.g., Kerberos, userID/password, PKI, ...) that are relevant to Federation activities? If more than one type of electronic credential is issued, how is it determined who receives which type? If multiple credentials are linked, how is this managed (e.g., anyone with a Kerberos credential also can acquire a PKI credential) and recorded?

Kerberos, Active Directory

2.5 If your electronic identity credentials require the use of a secret password or PIN, and there are circumstances in which that secret would be transmitted across D QHWZRUN ZLWKRXW EHLQJ SURWHFWHG E\ HQFU\SWLR used when accessing campus services), please identify who in your organization can discuss with any other Participant concerns that this might raise for them:

Our policy is to encrypt sensitive information such as authentication credentials.

2.6 ,I \RX VXSSRUW D ´VLQJOH VLJQ-RQµ (SSO) or campus-wide system to allow a single user authentication action to serve multiple applications, and you will make use of this to authenticate people for InCommon Service Providers, please describe the key security aspects of your SSO system including whether session

[4] "Member" is one possible value for eduPersonAffiliation as defined in the eduPerson schema. It is intended to include faculty, staff, student, and other persons with a basic set of privileges that go with PHPEHUVKLS LQ WKH XQLYHUVLW\ FRPPXQLW\ H J OLEUDU\ SULYLOHJ GHULYHG IURP RWKHU YDOXHV LQ HGX3HUVRQ$IILOLDWLRQ RU DVVLJQH identity database. See http://www.educause.edu/eduperson/

2.11 Would you consider your attribute assertions to be reliable enough to:

[X] control access to on-line information databases licensed to your organization?

[X] be used to purchase goods or services for your organization?

[X] enable access to personal information such as student loan status?

Federation Participants must respect the legal and organizational privacy constraints on attribute information provided by other Participants and use it only for its intended purposes.

2.12 What restrictions do you place on the use of attribute information that you might provide to other Federation participants?

Attribute information provided by Pace University identity systems should only be used for the purpose for which it has been provided. Attribute information must not be aggregated or provided to any third party. Any other uses are prohibited.

2.13 What policies govern the use of attribute information that you might release to other Federation participants? For example, is some information subject to FERPA or HIPAA restrictions?

Pace University FERPA policy (*https://www.pace.edu/registrar/transfer-credits/student-records#ferpaPolicy*) governs the handling of educational records and as noted in that policy, students may elect to suppress their directory information. "*Statutory and Regulatory Influences" and "Data Classification Policy" from the University's* Information Security Plan may be provided, upon request.

3. Service Provider Information

Service Providers are trusted to ask for only the information necessary to make an appropriate access control decision, and to not misuse information provided to them by Identity Providers. Service Providers must describe the basis on which access to resources is managed and their practices with respect to attribute information they receive from other Participants.

3.1 What attribute information about an individual do you require in order to manage access to resources you make available to other Participants? Describe separately for each service ProviderID that you have registered.

Not Applicable (NA) – At this time, Pace University is not acting as a Service Provider

3.2 What use do you make of attribute information that you receive in addition to basic access control decisions? For example, do you aggregate session access records or records of specific information accessed based on attribute information, or make attribute information available to partner organizations, etc.?

NA

Additional Notes and Details on the Operational Practices Questions

As a community of organizations willing to manage access to on-line resources cooperatively, and often without formal contracts in the case of non-commercial resources, it is essential that each Participant have a good understanding of the identity and resource management practices implemented by other Participants. The purpose of

Service Provider may be more willing to accept your assertions to the extent that this

applications for some period of time. This avoids people having to remember

[3.2] As a Service Provider, please declare what use(s) you would make of attribute information you receive.

[3.3] Personally identifying information can be a wide variety of things, not merely a name or credit card number. All information other than large group identity, e.g., ´PHPEHU RI FRPPXQLW\ µ VKRXOG EH SURWHFWHG ZKLOH

[3.4] Certain functional positions can have extraordinary privileges with respect to information on your systems. What oversight means are in place to ensure incumbents do not misuse such privileges?

[3.5] Occasionally protections break down and information is compromised. Some states have laws requiring notification of affected individuals. What legal and/or institutional policies govern notification of individuals if information you hold is compromised?

[4.1] Most InCommon Participants will use Internet2 Shibboleth technology, but this is not required. It may be important for other participants to understand whether you are using other implementations of the technology standards.

[4.2] As an Identity Provider, you may wish to place constraints on the kinds of applications that may make use of your assertions. As a Service Provider, you may wish to make a statement about how User credentials must be managed. This question is completely open ended and for your use.