Admin UW NetID group design

ANALYSIS	
Customers	Identify customers and their business needs: who needs the groups, when do they need them, for how long, and for what business reasons (email, sharing, access control, etc.).
	Primary: Expanded 2FA on the Web (P2) project needs the group to apply 2FA to admin UW NetIDs.
	Other: Microsoft Infrastructure, Authentication Service
Application Use	Identify what applications the customers needs to use with the groups.
	Primary: UW IdP and Azure AD will use the group to apply 2FA policy.
	Other: Active Directory, Authentication service (2FA)
Membership (Business Definition)	Define the desired group membership(s) – who's included and who isn't – in business terms and business rules used by the customer to describe the group membership(s).
	All active Admin UW NetIDs, including Workstation, Server/Domain, and Enterprise Admin UW NetIDs.
Business Process	Identify the business process (e.g. student registration, course enrollment, employment, research administration) that masters data that matches the desired group membership(s).
	UW NetID Service Offering self-service credential creation.
System of Record	Identify the authoritative system of record where the institutional data is defined and mastered.
	Identity Registry (UW NetID Registry)
Business Domain	Identity the business domain(s) from UW Data Map.
	-reference invalid-
Subject Area	Identify the subject area(s) from UW Data Map.
	-reference invalid-
DESIGN	
Type	Define the group type. Do the reference groups represent a simple group, a role, or a permission?
	Simple reference group, represents a UW NetID type or subtype.
Home Group	Choose a home group that aligns with the UW Group Naming Plan and the business domain of the related institutional data.
	u_uwnetid_
Group IDs	Define the group IDs and subgroup IDs that customers need to identify and reference. Some business processes master data that can be used for IDs.
	u_uwnetid_admin
Display Name	Define user-friendly display name values for contexts where groups are searched, listed, or selected by display name. Some business processes master data that can be used for display names.
	Admin UW NetIDs
Lifecycle Policy (Creation)	Define when the groups will be created. Some reference groups are created or "pre-provisioned" automatically. Other reference groups are created only by customer request.
	The group is a being created by customer request.
Lifecycle Policy (Deletion)	Define when the groups will be deleted.
	The group is expected to have a long lifecycle that aligns with the lifecycle of its purpose; it will be deleted only with careful planning and change management.
Membership (Direct)	Define the direct memberships of the groups and subgroups.
	Admin UW NetIDs will be direct members. No subgroups.
Membership (Exceptions)	Define how membership exceptions are managed, both additions and deletions.
	-none-

Membership (Grace Period)	Define the grace period on membership, if needed. No grace
Membership (Opt-in)	Define the opt-in policy for the membership, if needed. -none-
Membership (Opt-out)	Define the opt-out policy for the membership, if needed. -none-
Contact Person	Define the contact address. iam-support
Description	Define descriptions that help potential customers understand fit for purpose and use, including lifecycle policy, membership policy, data quality standards, appropriate use guidelines, access control policy, ownership, and contact information. Some business processes master data that can be used for descriptions. Note: proposed text will change when real-time affiliation group process is turned on. "Active Admin UW NetIDs. This is an automatically generated group from the UW Identity Registry. It is updated nightly."
More Information	Define where additional information for customers will be located. **TBD**
Application Settings (Exchange)	Define the status and settings for use in UW Exchange. Exchange enabled = no
Application Settings (Google)	Define the status and settings for use in UW Google Apps. Google enabled = no
ACCESS CONTROL	
Data Custodian	Identify the responsible data custodian(s). Subject area: Master Data Business domain: Personal Identifiers - UW NetID Nathan Dors, Director, UW-IT Identity and Access Management
Classification	Determine the appropriate UW data classification (Public, Restricted, Confidential). Restricted
Access Control Policy	Decide and document the access control policy including membership viewer control, sender control, appropriate use guidelines, terms and conditions of use, etc. Access Control Policy The group membership is classified as Restricted because it warrants careful management and protection to safeguard its integrity and availability. The access policy allows it to be provisioned where there are legitimate business needs for access. Other access may be authorized by the data custodians on a case-by-case basis, based on establishing a business need.
Membership Viewer Control	Define the membership viewer control, including exceptions to the access control policy. No viewer restrictions
Sender Control	Defined the sender control, including exceptions to the access control policy. N/A
IMPLEMENTATION	
Data Source	Identify the service that will be used as the data source for provisioning. It may or may not be the same as the system of record. Identity Registry
Membership (Technical)	Define the technical definition of the memberships in terms used by the data source and its data elements, as well as any additional filtering. Entity has active category 46 record

Provisioning	Define a provisioning model for data integration and reconciliation that ensures the groups are created in accordance with their lifecycle policy and managed in accordance with their data quality standards. 1. Person Registry Group provisioning process for daily reconciliation (identity registry exports) 2. Real-time "affiliation" group provisioner (irws-watcher)
De-Provisioning	Define a de-provisioning model that ensures the groups are deleted in accordance with their lifecycle policy. N/A
Monitoring	Define a monitoring solution that helps identify incidents and problems, particularly those that impact availability and reliability. Existing provisioning process tooling (IRWS export reports, irws-watcher monitor)
Data Quality Standards	Define data quality standards under normal operations, including data validation rules, timeliness of updates, defined error rates, integrity monitoring, and reliability. The standards will depend on the business process, system of record, data source, provisioning and de-provisioning models, monitoring, and operations. **TBD**
Internal Documentation	Define what internal documentation will be developed and where it will be maintained. New section of institutional group documentation for UW NetID type / sub-types.
Customer Documentation	Define what customer documentation will be developed and where it will be maintained. **TBD**
Communication Plan	Define the communication plan to inform audiences about the new reference groups. **TBD**
OPERATIONS	
Request Fulfillment	Define how requests will be fulfilled. For example, standard requests for information, access to memberships, membership exceptions, email settings, design changes, etc. N/A
Incident Management	Define how incidents will be handled. **TBD**