Identity Management Policy and Practice Statement

Document Revision Information

Document Identifier	NIKHEF
Document Version	1.1 (IN FORCE)
Last Modified	2014-10-30
Last Edited By	DLG

Table of Contents

Document Revision History

Version	Editor	Comments
1.0	*DG*	*Endorsed version by Nikhef MT, 10 December 2009*
1.1	*DG*	*Restructured technical details into ancillary documentation and policy alignment following consolidation of implementation trajectory. Add explicit support for security incident response for Qualified Third Parties. This version is materially the same as the agreed MT implementation process.*

1 Introduction

The Nikhef Identity Management system NikIDM is the organisational ICT system of the Nikhef Collaboration that implements the interface of Nikhef with regards to generic authentication and authorization for its Users.

The NikIDM system is the authoritative source of authentication, attributes, and roles for all user entities for managed ICT services, and is a source system for other ICT entity types at Nikhef. Any user data and assertions provided by other managed ICT systems at Nikhef will not be in conflict with this Policy and the NikIDM source systems.

The NikIDM also provides authentication, attribute management, and authorisation capabilities for the Nikhef collaboration and the Institute when interacting with third-party service providers and educational and research federations.

1.1 Eligibility and Scope

Any person with a valid and current registration as Nikhef Employee or Nikhef Guest in the Nikhef human resources system is ipse facto eligible for enrolment in the NikIDM. Other persons that have a relationship with Nikhef may also apply for enrolment in the NikIDM when sponsored by a Nikhef Employee; their eligibility will be decided upon by the Registrars, taking into account the scientific and business objectives of the registration in relation to the objectives and mission of Nikhef.

The Head of the Nikhef Computer Technology group, so empowered by Nikhef Management, has the discretionary right to decide if an applicant meets this eligibility requirements.

The NikIDM will not enrol applicants that have no relationship with Nikhef.

1.2 Purpose of the Nikhef Identity Management System

The purpose of the Nikhef Identity Management System (NiKIDM) is to enable authentication of Users using information and communications facilities of Nikhef and Nikhef Partners, their unique and persistent identification towards ICT systems and their systems managers, the release of relevant attributes and information about the Users and to facilitate the participation of Users towards educational and research services provided anywhere in the world, through the participation of Nikhef and/or Nikhef Partners in collaborations, consortia, and federations that provide or mediate access to such services.

The NikIDM collects Personal Data and Sensitive Personal Data as defined in the WBP2000, as well as non-personal data about its Users solely to fulfil the Purposes of the NikIDM as stated above.

The NikIDM system service may in addition contain non-user, non-personal entities that support the ICT services at Nikhef.

1.3 Terms, definitions, and Glossary

Directory
: The system that persistently stores identified and associated attributes for entities that currently are or at any time have been enrolled in the NikIdM Service.

Registrars
: Those designated individuals that are entitled to validate applicants and have been granted administrative access to the Directory.

Consumers
: Those entities that are entitled to obtain data from the Directory. These entities are either defined by name, or are anonymous entities whose access is determined by their host network address.

IdM Service
: The service that provides authentication and attribute association for entities associated with Nikhef Partners as well as all those entities that are associated with the official activities of Nikhef.

Nikhef
: The national institute for sub-atomic physics, Nikhef, being comprised of the FOM Institute for sub-atomic physics and the organizational units of the collaborating Universities of Nijmegen, Utrecht, UvA, VU, and any other Dutch universities that are involved with sub-atomics physics, as defined in the Nikhef collaboration agreement ("Nikhef Overeenkomst 1996" and/or any subsequent version or amendment thereof).

Nikhef Collaboration
: The collaboration Nikhef

Nikhef Employee
: Any person having a valid and current registration in the Nikhef human resources system with the status of employee

Nikhef Guest
: Any person having a valid and current registration in the Nikhef human resources system with the status of guest

Nikhef Management
: The Director of Nikhef, or in his absence the institute manager, or in both their absence any member of the Nikhef management team

Institute
: The FOM Institute for sub-atomic physics

IdM Registry
: The registry for entities enrolled in the NikIDM Service that do not have a registration in the Personnel Registry, or for whom not enough information is stored in the Personnel Registry.

BSN
: Burger Service Nummer

Face-to-Face Meeting
: A meeting in-person between an applicant and a NikIDM Registrar.

User
: Any entity, not being or acting in the role of Registrar, who is enrolled in the Directory and that can be associated to a natural person.

Account
: Any entity, not being a Registrar and not being an information system component, enrolled in the directory.

Service Manager
: The person or persons responsible for the policy and practices related to a particular service.

Purpose
: The limitative and exhaustive list of purposes for which the NikIDM is and may be used as defined in section 1.2, and as intended in Article 7 WBP 2000.

Repository
: The public or private web page or pages that contain information on the NiKIDM system, policies, and published practices.

IdM Manager
: The designated individual responsible for the policy and operations of the NikIDM.

NikIDM (the Nikhef Identity Management System)
: The ensemble of systems, networks, facilities, and the associated policies, practices and procedures that enables the fulfillment of the Purpose of this Policy.

Registry
: The archive of records pertaining to the directory that document identities, the processes by which Users are enrolled and removed from the IdM, and eligibility records.

Qualified Third Parties
: Those third parties with which Nikhef has entered into specific agreements, and for whom Nikhef and the NikIDM have accepted specific responsibilities and liabilities. Such parties may include, but are not limited to, research and academic federations in which Nikhef participates, providers of services to Nikhef that use or rely on the NikhefIDM system.

WBP2000
: Wet Bescherming Persoonsgegevens 2000 (*Data Protection Act* 2000)

SSO
: Single Sign On

AVA
: Attribute and Value Assertion (the attribute name and its value or values as defined in the Directory)

IdP
: Identity Provider

AUP
: Acceptable Use Policy for Nikhef users, as endorsed by Nikhef management. See http://www.nikhef.nl/aup

Operations Practice Statement
: The authoritative document describing the technical and operational controls that govern the NikIDM and Directory systems. See https://wiki.nikhef.nl/nikhef/ctb/NikIDM/OperatingPractices

Attribute Release Statements
: The authoritative document describing the information and attributes released by the NikIDM and Directory to services. See https://wiki.nikhef.nl/nikhef/ctb/NikIDM/Services

2 General Architecture

The NikIDM and the Directory implementing the NikIDM is used to store information about Users, Accounts and other system entities used within the Nikhef ICT infrastructure. It is used to authenticate users for access to Nikhef systems and resources, and for access to other services at Nikhef offered to internal and guest users, including on-line web and non-web services, to store attributes and contact information for users.

The Directory and the information there may be used to authenticate users any service offered by or on behalf of Nikhef. The information contained in the Directory may be released to other parties in order to facilitate and enable access to services that support the business and scientific objectives and the mission of Nikhef, insofar as it is necessary to gain access to such service and where the service provider has valid reasons or legitimate interest in obtaining and processing such data.
Information may also be released on the initiative of and with the consent of the user for any service that does not constitute a risk or liability to Nikhef, and then only in accordance with the Nikhef Acceptable Use Policy.

The NikIDM and Directory systems are classified as high-value services and appropriately protected with technical and policy controls. The technical and policy controls shall be documented in an Operations Practice Statement.

The NikIDM systems, comprising both the Directory and any authentication systems (such as WebSSO, Radius, or OpenID), will be used by Services to authenticate and to provision information about the authenticated entity (User).

The information released shall be limited to only such information (‘attributes’) that is necessary to perform the service. This attribute release shall be as specified in section 8.

3 Identity

The Nikhef Identity Management systems contains different kinds of entities:

- Users
- Generic Accounts
- Other information systems (non-human) entities

Identity vetting processes are solely defined for Users, and are not applicable to Generic Accounts and non-human entities. Where association of Generic Accounts with identity is desired, it is the responsibility of the Service recognizing the Generic Accounts to make and maintain such an association.

Users will be entered and retained in the directory by Initial Enrolment, followed by specific Service Enrolment and/or Attribute Enrolment. Acceptance criteria for the various enrolment steps and processes are defined in the respective sections following.

3.1 Initial Enrolment

Users are employees, guests, or affiliates (others).

The registration process for Users MUST record at least the following data

- Full name of the applicant
- Occupational or home telephone number of the applicant
- Email address of the applicant
- Reasons for the application
- For Users other then employees and guests: the name and contact data, or uid, of the Nikhef employee acting as the sponsor for this application.
- Name of the IdM Registrar
- Foreseen expiration date of the account

All enrolments must be endorsed by either being enrolled in the personnel registry or by the Personnel Department for Employees and Guests, or a Nikhef Employee for affiliates.

The User accepts all terms and conditions imposed by contact, by this Policy, by the AUP, and by the relevant implementation procedures. The User SHOULD confirm this consent in writing; the Sponsor MAY subsume this responsibility on behalf of the User, if the User cannot reasonably be expected to do so.

Based on this information, the Account may be activated by setting the *schacUserStatus* attribute to the value *urn:mace:terena.org:schac:userStatus:nikhef.nl:affiliation:active* in the Directory.

The following attributes MUST be defined for the new Account

- *uid, cn, sn, schacExpiryDate, mail*

Other attributes MAY be defined at this stage. If a posix service is enabled, and no pre-existing corresponding account on the Nikhef network exists, a new non-conflicting *uidNumber* MUST be chosen.

The value of the '*uid*' attribute MUST be unique, and MUST NOT be re-used within the NikIDM system for an entity different than the one to which it was previously assigned.

When an entity is enrolled which hold a previous registration in the NikIDM, the *uid* may be assigned again to the same entity, provided all requirements for renewal and re-registration are met.

For those entities that have an entry in the personnel registry and in pre-existing ICT management systems at the time of introduction of the NikIDM, a transition process will be defined.

3.2 Expiration and extension

The expiration date MUST be set for all users, and this expiration date SHOULD be commensurate with the intended purpose of the account.

For Guests and Employees, the expiration date must not be set past 1 months of expiration of the registration or employment contact term.

For all other Users, the expiration date must not be set beyond 13 months of the current date.

The expiration date for a User may be extended after re-validation of eligibility and after verification of the mandatory attributes for enrolment, in accordance with the maximum terms here specified.

Whenever the Expiration date for a User is reached, the Account shall be de-activated.

3.3 Termination

When the contract relationship with an employee is terminated prematurely, or when a Guest leaves the organization before the expiration date has been reached, the Account should be de-activated as soon as reasonably possible.

Whenever a User no longer has a legitimate need for registration, or when a Sponsor or Registrar becomes aware of such a fact, the Account should be de-activated as soon as reasonably possible. Both Users and Sponsors must notify the Registrar of such facts.

3.4 Service enrolment and authorization

Users may subscribe to Services that use the NikIDM for authentication and authorization purposes (such as interactive login, email, source code management systems, access to specific systems, etc). Access to a service may be enabled by granting specific AVAs, by inclusion in specific directory groups, or a combination thereof.

Each Service has one or more Service Managers, who are responsible for granting and revoking access to the service according to the service terms of use. The Service Manager

may delegate all or part of the responsibilities to the Registrars. The list of Service Managers in maintained in the Repository

When enrolling for a Service, the following information MUST be recorded

- List of initial services requested, as well as the list of initially granted services
- List of the system classes on which the service is granted
- Names of the service grantors

Based on this information, the corresponding *authorizedService* attribute, the *host* attribute where applicable, and other service-specific attributes may be set to allow access to the granted services. Also, the Account may be included in a directory-group whose membership grants access to specific system classes. Services must only be thus authorized with the consent of the service manager or responsible.

The Registrars are responsible for the material implementation of the service enrolment and enabling.

3.4.1 Service specific authorization and additional controls

Each Service may set additional policies and implement additional access controls. Such controls may include but are not limited to limitations on source network address, knowledge or possession of additional authentication factors or pass phrases, membership of specific groups or the possession of specific roles.

Each service where additional controls are applied may publish these constraints in the Repository. In absence of a published policy, the Service Manager is authoritative to define, implement, enforce and audit any such additional controls.

The additional controls applied shall be commensurate with the risks associated with the Service, the sensitivity of any data used within or in conjunction with the Service, and the intended audience of the Service.

3.4.2 Service termination

Services can be terminated independent of the Account to which they are associated. Whenever a User no longer has a legitimate need for a service, or when a Sponsor or Registrar becomes aware of such a fact, the service authorization should be withdrawn as soon as reasonably possible. Both Users and Sponsors must notify the Service Manager of such facts.

The Service Manager may terminate, regulate or control service authorization at any time, and should inform the User thereof.

3.5 Attribute and group enrolment

Attributes and directory group membership MUST be used only in accordance with the Attribute Semantics specification in this document or relevant standards. The Registrars shall confirm and validate any applications for Attribute Enrolment based on these Semantics.

Where the Attribute Semantics specification is incomplete or unclear, the NikIDM Manager will interpret the standards and conventions pertaining to the requested attribute and decide accordingly, taking into account the requirements of Qualified Relying Parties. Following this decision, the Attribute Semantics specification will be updated.

3.6 Renewal and re-registration

Only those accounts for Users where sufficient information has been recorded to re-establish, positively and verifiably, that the User that (re)applies is the same User that previously had access to the Account, may be re-registered and/or re- enabled.

Sufficient evidence for such a re-binding is a positive match between a current and historic registration in the Nikhef personnel registry where the registered BSN matches, and where the personnel registry has recorded the *uid* of the User. For other entities, a match between a historic hand-written signature in the NikIDM Registry and a current hand-written signature, supported by a Face-to-Face Meeting with the presentation of a valid government-issued photo-ID, and where the *uid* has been recorded, is sufficient.

3.7 Compromise and revocation

When an Account becomes compromised, or when there is reasonable doubt about the integrity of the information contained in the Directory, the Registrar must suspend or disable the User, for as long as the account is compromised. The User can at any time request suspension or disabling of the User's Account.

Where specific agreements or contracts with Qualified Third Parties exist that require that the Qualified Relying Party is informed about such a suspension and revocation, the Registrar is responsible for informing the Relying Party about such compromise. Information regarding the User or the compromise released shall be limited to the minimum what is necessary to comply with the agreement or obligation.

Where no specific agreements or contracts exist, no notification shall be made.

Following a revocation or disabling, and during a suspension, the User shall not be able to authenticate to any NikIDM system component.

3.8 Generic Accounts

Generic accounts are used in Services for several purposes, such as allowing access to specific computing systems, storage services, and others, e.g. in the context of inter-organisational distributed computing infrastructures, or for other purposes.
The Directory MAY contain Accounts that are not associated with a User, called Generic Accounts. Generic Accounts MAY be disabled and re-enabled any time, as they are not related to identifiable persons in the NikIDM.
These Accounts may be used by Consumers if and only if the Consumer itself will retain audit information and logs sufficient to identify the use of the Account within its service domain.
Generic Accounts MUST NOT have any of the following attributes or values set:

- schacUserStatus attributes with values starting with
  urn:mace:terena.org:schac:userStatus:nikhef.nl:identity-vetting:...
- eduPersonAffiliation
- eduPersonPrimaryAffiliation
- eduPersonScopedAffiliation
- eduPersonPrincipalName
- eduPersonAssurance

At this time the Directory will not support 'walk-in' entities that have no defined relationship with Nikhef.
Generic accounts must have an associated Sponsor who is a Nikhef employee, the Nikhef HR department, or a Registrar. The Sponsor or Sponsors are individually and collectively responsible for the generic account, and for the authentication of the generic account enabling use of any services thereby.
When the Generic Account has soft authenticators associated with it (such as a password), these authenticators shall be subject to the expiration policy.

3.9 Non-human entities

The Directory may contain non-human entities, such as but not limited to networked systems, automount mount points, directory groups, mail aliases and lists, virtual mail users, and entities used to authenticate other services, such as replication services and slave servers.

These entities are entered into the database by the Service Manager, and must not have influence on any other entities in the Directory or on Consumers.

3.10 Hardship Clause

Where the enrolment or approval process described in this section leads to obvious injustice and hardship due to a implementation of the process being unduly hard, a time-limited and documented exception may be implemented after the explicit approval of either the NikIDM Manager, the Head of the Computer Technology Group, or Nikhef Management.

Any such exception must be followed by immediate and concrete steps to address the deficiencies created within a limited time period commensurate with the discrepancy induced.

The invocation of the hardship clause MUST not compromise the integrity or trustworthiness of the NikIDM with respect to any Consumer.

4 Operational Requirements

4.1 Systems management security

The Directory and NikIDM systems including the IdP SSO shall be run on managed systems running a recent and supported version of an enterprise-class operating system and as updated and maintained through the regular maintenance processes of the operating system vendor or distributor.

The technologies shall be documented in the Operations Practices Statement, and shall be reviewed periodically for suitability and security.

Access to these systems and services must only be over confidential and integrity-protected channels, and must be authenticated for any administrative access.

The data in the directory is contained in a database, and backed-up at least every 24 hours to an off-site location. The backup is performed over a site-local network to a trusted third party under contract.

Restoration of data from the off-site backup will proceed only after a sampled validation of its correctness.

Re-usable authentication tokens and pass phrases for Users must be kept on persistent storage only in encrypted form. All other authentication tokens should be stored in encrypted form only or be adequately protected by system mechanisms. Pass phrases must not be sent in clear-text over any network for any entity.

4.2 Interfaces

4.2.1 LDAP

The Directory may be accessed via the LDAP protocol only over secure connections ('ldaps'). Access is controlled by the Directory in accordance with the Attribute Release Policy.

4.2.2 IdP and Single Sign On interfaces

The SSO interface is provided via the SimpleSAMLphp software, and provides at least a SAML2.0 end-point compliant with the SAML2Int WebSSO profile. Access to the SAML WebSSO service is controlled via the trusted remote SP meta-data file, and attributes are released according to the Attribute Release Policy.

The NikIDM offers a OpenID interface. Any information released through this interface shall be compliant with the Attribute Release Policy. The OpenID URL authenticated by this service, including the implied user name, shall be deemed public information.

NikIDM may offer additional 'SSO' interfaces. Such interfaces must be integrity and confidentiality protected, and must comply with the Attribute Release Policy.

Access to the authentication interface of the IdP MUST be over secure and encrypted links.

The IdP software will be maintained such that it remains secure and compatible with the service providers and federations with which Nikhef has entered into agreement.

4.2.3 Web and web-based management

Where web-based access to the NikIdM is provided, it MUST be over secure and encrypted links only.

Where web-based services connect directly to the NikIDM or to the Directory, access to the web application MUST be over secured and encrypted links only, and the web application MUST use secure and encrypted links to communicate with the NikIDM or the Directory. A web application must not persistently store, on disk, in sessions, or otherwise, re-usable authentication information on the server side. No re-usable authentication information must be returned to the web user in any form.

4.2.4 Unix

Command-line LDAP and Unix utilities (such as the Pluggable Authentication Modules, PAM) to connect to the Directory MAY be used, exclusively using the secure LDAPS protocol and exclusively over links that are secure and encrypted links, or use a local hard-wired interface.

4.2.5 Windows

Currently no access policy for Windows clients or domains is defined.

4.2.6 Kerberos

Currently no access policy for Kerberos is defined.

4.3 Account expiration process

For every Account the attribute *schacExpiryDate* MUST be set. The attribute *schacExpiryDate* SHOULD be set to the registered expiry date in the source Registry or be set commensurate with the intended use of the Account. After expiry, a periodic process run at least once every 36 hours MUST ensure that the *schacUserStatus* attribute for *nikhef.nl:affiliation* will be reset to *expired*, thus ensuring that the Account is no longer visible to Consumers.

Expired Accounts for Users may be re-enabled at a later date, if and only if it can be positively and verifiably determined that the Account will be used by the same User who previously had access to the Account. Sufficient evidence for such a re-binding is a positive match between a current and historic registration in the Nikhef personnel registry where the registered BSN matches. For other entities, a match between a historic hand-written signature in the NikIDM Registry and a current hand-written signature, supported by a Face-to-Face Meeting with the presentation of a valid government-issued photo-ID is sufficient.

Within 13 months of expiry, knowledge of the passphrase associated with the Account in the Directory will be sufficient, provided that no known compromise of the Account or the Directory has occurred.

When re-enabling any User, the full set of attributes for a User, including all Services to which a User is authorized and any groups to which the User belongs must be reviewed. When re-enabling a User past one (1) month of expiration, the Registrar should re-assert eligibility of a User to use Services with the respective Service Managers, and re-assert eligibility for all *schacUserStatus*, *eduPersonEntitlement*, *authorizedService,* and *eduPersonAffiliation* attributes.

4.4 Attribute and Service expiration

Specific attributes and authorization to use specific Services may be revoked or expired any time:

- On request of the Service Manager for the service to which access is being revoked
- When a Registrar is informed about a status change of the user within Nikhef or within the underlying registry
- On request of the User

Where specific agreements or contracts with Qualified Third Parties exist that require that the Qualified Relying Party is informed about such a expiration or revocation, the Registrar is responsible for informing the Relying Party about such action. Information released regarding the change shall be limited to the minimum what is necessary to comply with the agreement or obligation.

Where no specific agreements or contracts exist, no notification shall be made.

Following the revocation or expiration of attributes or of service authorizations, the NikIDM and the Directory will no longer supply such attributes or authorizations to Consumers.

4.5 Enrolment and visibility to Consumers

The Directory contains all Users that are currently affiliated with Nikhef or have been affiliated at any time in the past. All these entities are visible to Registrars, but not necessarily to any other Consumers of the Directory.

Only those Users who have a *schacUserStatus* attribute value *nikhef.nl:affiliation* set to *active* will be fully visible to Consumers and Users of the directory service. Users that are *suspended* may be partially visible to Consumers and Users of the directory service, but must not authorized to actively use any services and no entitlements nor trusted attributes must be released for such Users.

Generic Accounts MAY be visible to any Consumer.

4.6 End-user security requirements

The passphrase Users use to authenticate to the Directory MUST be at least 9 characters long and conform to current best practice in choosing high-quality pass phrases. Passphrases and other soft authenticators must not be re-used. Authenticating materials must not be shared or made public in any way.

4.7 Attribute Specification

The Directory will contain Attributes and their associated values. In addition, attributes may be constructed based on information contained in the Directory or obtained from trusted sources.

Attributes and attribute-value assertions are registered in the Directory by Registrars only after eligibility of the entity is confirmed, and only in compliance with the guidelines given in this Appendix.

Where no specific guidance is given, the attribute MUST be used only in accordance with the relevant Standards and specifications regarding the definition of the schema and attributes. Where ambiguity in the schema semantics exists, the use of the attribute MUST be assessed and SHOULD be added to the definitions in this section.

A registry of attributes shall be maintained in the Repository. Where no standard vocabulary exists, permissible values shall be listed in the Repository.

Attributes should be released only in accordance with the Attribute Release Policy.

5 Site Security

5.1 On-line systems security

All computer systems associated with the Directory and the NiKIDM are located in a secure environment where access is controlled and limited to authorized personnel.

Network security zones must be defined in the Operations Practice Statement, and sensitive systems MUST be placed in a network security zone commensurate with their risk level. Directory services and IdM services that contain key material used to sign assertions MUST be in network security zones where systems access is limited to designated personnel and a limitative set of known operators. They shall not be hosted in a network zone that offers general access to Users.

The LDAP servers may only be accessed through the secure protocols over TLS ('ldaps'). No insecure access over the network is allowed for any directory server.

5.2 Security requirements of dependent services

Any service that uses the NiKIDM for authentication purposes MUST ensure that re-usable authentication data, such as user names and pass phrases, are never sent in clear-text over any network. Any service MUST, in turn, impose this same requirements on any subordinate services.

Services SHOULD ensure that attributes that contain Personal or Sensitive Personal data are sent only over encrypted channels, and MUST ensure that such attributes are only send over encrypted channels when transmitted over the public Internet.

5.3 Physical Security

All systems and networked equipment related to the NikIDM is located in secure rooms where access is controlled and limited to designated personnel. The rooms are secured with multi-modal locks, that can be operated either by personalised and authenticated proximity cards, or by means conventional keys under the control of named individuals.

The rooms are located in the Nikhef building. The rooms are fitted as standard IT housing facility, including appropriate power and cooling systems. All rooms are located above sea level but in an area prone to flooding. Automatic fire suppression systems are installed.

6 Publication and Repository Responsibilities

6.1 Repository

Information regarding the NiKIDM, including contact information, references to meta-data and fingerprints, and this Policy and any derived policies and procedures that can be disclosed will be made available to Qualified Third Parties.

Information regarding Nikhef and its activities is available from

http://www.nikhef.nl/

and information regarding the NikIDM and this Policy from

http://sso.nikhef.nl/policy

and other NikIDM specific information from

http://sso.nikhef.nl/

Changes and updates to contact information will be communicated to Qualified Third Parties that have expressed interest in such communications, and where needed to meet contractual obligations.

Operational Practice Statements and Attribute Release Statements shall be maintained in a repository to which access may be restricted to qualified entities. The Attribute Release Statements shall be available to Users.

https://wiki.nikhef.nl/nikhef/ctb/NikIDM#Operational_and_Policy_Registry

6.2 Implementation Procedures

Implementation procedures associated with this Policy may either be public or confidential. Public procedures will be published in the Repository.

7 Audits and Liability

7.1 Liability

It is the intention of Nikhef to operate the NikIDM according to and in compliance with all policies and procedures described in this document, and for this service to be continuously available. However, The NikIDM service availability is on a best-effort basis only, and Nikhef does not assume any liability for unavailability of this service or inability to use the service by any entity, for whatever reason.

Nikhef makes economically reasonable efforts to ensure that authentication of Users is valid and that any attributes released comply with this Policy and with the policy of third parties with which Nikhef has entered into agreements ('Qualified Third Parties').

Qualified Third Parties are required to release a list of required Attributes for use of any service. Qualified third parties are required to request and obtain those attributes from the NikIDM on which they base their own authorization decisions. Nikhef assures that the values for those attributes, when released, comply with this Policy.

Granting access to a services by a third party despite failure or declination of the NikIDM to release any specific attribute regularly required by said service, will release Nikhef from any liability with respect to damages resulting from use of said service. That is, we require that Qualified Third Parties treat a systems failure of the NikIDM, or the failure to authenticate, or the failure to release attributes required by the third party, as a denial.

The mere sole fact of authentication of a User to the NikIDM does not imply eligibility of the User for any service by any party.

7.2 Audits

Nikhef will cooperate with a compliance audit of the NikIDM at least once every 12 months. Such an audit may be requested by Qualified Third Parties with which the Nikhef has entered into a common agreement. Any direct costs associated to such compliance audit are to be borne by the requesting party.

7.3 Security Incident Response

Nikhef has a Computer Security Incident Response Team (CSIRT) to address various issues related to computer and network security, from prevention to incident handling.

Any party may report suspicious behaviour, misconduct, or security incident that involves any of the Nikhef users or systems (either as a target or as the origin). All reasonably authenticated or legitimately reported incidents will be investigated and duly acted upon.

The Nikhef CSIRT team and NikIDM Registrars will always collaborate in security incident response with Qualified Third Parties.

The CSIRT can be contacted at security@nikhef.nl and at https://www.nikhef.nl/security

8 Privacy and confidentiality

8.1 Recorded subscriber data

User data will be recorded in the Directory as well as in supporting registries. By enrolling in the Directory, the applicant agrees that all data provided will be stored in an automated retrieval system and that all Registrars will have access to all information provided.

By subsequently requesting specific attributes and services, the User agrees that the data collected to assert eligibility for these attributes and services will be collected and stored in the Directory and in supporting off-line registries.

Where the user provides personal data, Nikhef will make reasonable and commercially viable efforts to ensure that these data remain confidential, except for those attributes and values that are explicitly defined as public or releasable in the Attribute Release section of this Policy.

Stored in the Directory are only those data stored in Attributes as defined in the "Attributes Specification" in this document. Sensitive Personal Data as defined in the WBP2000 will not be stored in an on-line or automatically retrievable system. Other Personal Data MAY be stored in an on-line system to which access is controlled and limited to authorized personnel for administrative, operational, accounting, monitoring and security purposes only.

8.2 Attribute Release Policy

8.2.1 Administrative release

Any and all attributes will be released to Registrars, who MUST use these attributes for administrative, operational, accounting, monitoring and security purposes only.

8.2.2 Operational release and service classification

The information released shall be limited to only such information ('attributes') that is necessary to perform the service. The User shall be informed about the Attribute Release through Attribute Release Statements that are maintained in the Repository, and by notification on initial service access for external services as defined below.

To achieve appropriate information and attribute release practices, services shall be classified as:

- Internal Services, being those services offered directly by Nikhef or offered using systems hosted within the Nikhef managed network, where their operation and data processing is controlled by Nikhef ICT personnel and whose security risk and incidents are under the aegis of the Nikhef CSIRT;
- Necessary External Services, being those external services that whose necessary is implied for any Users at Nikhef in support of the Nikhef mission, or necessary for the User in order to fulful obligations with regard to Nikhef; and

- Optional External Services, being any external service which is made available to Users, but where refraining from the use of such a service does not impair the User, and where the User has a free and unconstrained choice to use or refrain from use of such service.

For Internal Services, any attribute contained in the Directory and NikIdM system may be released for use in the service of such release is reasonably needed to provide the service to the User in a user-friendly and rich way. This release will be implicit.

For Necessary External Services, only those attributes that are minimally necessary for operating the service, or in which the service operator has a legitimate interest, shall be released by the NikIDM system. Nikhef may rely on trusted third parties, specifically those in the SURF family, to assess the necessity of attribute release for any particular service. The User shall be informed of the attributes and their values before release.

Nikhef and the NikIDM may offer access to Optional External Services, either directly or through federated agreements. For access to these services, attributes may be requested from the NikIDM service by such services. NikIDM, or qualified mediators on behalf of Nikhef including the SURF federation platform, will present the User with the set or information about to be released to service before such access is enabled. The User shall at that point have a free choice as to whether or not to proceed and release such information to the Service. The User shall thus be informed of the attributes and their values, and by accepting the attribute release is deemed to have consented freely to the release of this information. Where possible and relevant, information about the status, terms, conditions, an privacy policy of the service shall be made known to the User.

The release of attribute to any specific service shall be documented in the Attribute Release Statements.

Authenticator data shall not be readable, except for the purposes of system operation and by Registrars.

8.2.3 User Release and review

All identity and service attributes and group memberships of the User except for authenticator attributes are released to the User, for as long as the User is able to authenticate to the Directory and the affiliation of the User has not expired.

The User at any time can request a listing of the all attributes, except for authenticator attributes, by contacting a Registrar, who will comply with such a request forthwith.

8.3 User Acceptance

By applying for registration in the Directory, the applicant is deemed to have accepted the terms and conditions of this Policy, and consent to the processing and storage of her or his Personal Data under this Policy for the defined Purpose of the NikIDM.

User data is collected and augmented in order to provide to the User one or more services that use the NikIDM for authentication or authorisation. User data is stored for these reasons and for administrative, operational, accounting, monitoring and security purposes, either currently or in the future.

By enrolling in the NikIDM, the user agrees that the attributes will be released according to the Policy described here.

If there are material changes to the release policy for Necessary External Services, the Users are informed of this change via a Nikhef-wide announcement. Users can object to a proposed change within two weeks following the announcement. In case no consensus resolution of the objection can be reached, Nikhef Management is empowered to decide on any objections raised, taking into account applicable regulations, contracts and laws.

8.4 Logging and auditing data

The NikIDM systems, the Directory, and any systems used to interconnect the Directory to internal and external processes, will record logging and auditing data for administrative, operational, accounting, monitoring and security purposes only. This logging and auditing data will be stored in the on-line systems of the NikIDM and may be stored in all centralised logging facilities used by Nikhef and the Nikhef Data Processing Facility. Such records must be kept for a period of at least 119 days, and may be stored for a period up to 2 years.

These time limits apply solely to the records intended above, and do not extend to data stored in the Directory itself or to the Registries.

9 Compromise and Disaster Recovery

9.1 Suspension and termination

Registrars and Security Officers may, for administrative, operational and security purposes, regulate or terminate access to any service, may add, modify, or remove any attribute and value, and may deny the possibility to authenticate, for any User. Such an act shall not result in any additional privileges being granted to the User, and must not compromise the integrity or trustworthiness of the NikIDM with respect to any Consumer.

Any such regulation or termination shall be documented, and include the reason for the intervention and the list of actions taken, and this documentation shall be submitted to the NikIDM Manager.

Unless it conflicts with any operational or security requirements, the User shall be informed of any regulation or termination of access in a timely fashion.

In case of any suspected or confirmed security incidents, Service Managers are authorised to regulate or terminate access to any service for which they are responsible, irrespective of any actions taken or not taken in the NikIDM or by Registrars.

9.2 Force Majeure

In exceptional cases ("Force Majeure incidents"), any qualified individual endorsed by either a Registrar, the NikIDM Manager, the Head of the Computer Technology Group, or Nikhef Management, may perform any action with respect to the NikIDM. Such an act shall not result in any additional privileges being granted to any User, and must not compromise the integrity or trustworthiness of the NikIDM with respect to any Consumer.

Any action shall be constraint to the most limitative measure compatible with adequately addressing the incident.

Any Force Majeure incident and all actions taken must be fully documented and submitted for retro-active endorsement by the NikIDM Manager and Nikhef Management.

9.3 Retention of documentation

All documentation related to regulation, termination or the handling of Force Majeure events shall be retained for a period of at least three years.

10 Subscribers and Subscriber Compliance

10.1 Acceptance Use Policy

All persons using Nikhef services, or enrolled in the Directory, are subject to the Nikhef Network Acceptable User Policy, as documented on the URL

https://www.nikhef.nl/aup

This AUP is brought to the attention of Users when they become subscribers of the Directory, or when they are granted access to Nikhef ICT services.

10.2 Authentication tokens, compromise and incidents

The User is required to choose a strong pass phrase, in accordance with current best practice and of at least 9 characters in length, containing sufficient entropy. The User must keep all authentication data confidential, and not share such data with any other party.

When the User becomes aware of any disclosure of authentication data, the User must contact the Nikhef computer security incident response team as soon as reasonably possible. The User must cooperate fully with the response team when dealing with the security incident.

Authentication tokens and pass phrases for Users must not be stored in clear-text and must not be transmitted in clear over any network.

10.3 Expiration of authentication tokens

Software based authentication tokens and pass phrases for Users and Generic Accounts are valid for at most 13 months, after which period they must be replaced. When tokens or pass phrases are not replaced, the User will be suspended, and must not be allowed to authenticate to the NikIDM, will not be allowed to use any Services, nor be able to obtain any validated attributes, until the token or pass phrase has been changed.

Expired or compromised authenticators and pass phrases shall not be re-used.

10.4 Compliance

Nikhef networks and computer systems are monitored for anomalies. Anomalies are investigated and, if found to be originating from a user of the Nikhef services, the relevant user is contacted and appropriate measures taken.

Measures are defined in the AUP and may include termination of service as well as any other measures allowed by contract or law.