GÖTEBORGS UNIVERSITET

Kontaktperson:
Lena Ström
lena.strom@gu.se
031-786 5489

SWAMID Identity Management Practice Statement Template

1. Inledning

Göteborgs universitet är ett av Sveriges större lärosäten och är medlem i SWAMID sedan flera år tillbaka.

Detta dokument beskriver hur vi uppfyller kraven för tillitsprofilerna SWAMID AL1 och AL2.

4. Organisational Requirement

The purpose of this section is to define conditions and guidance regarding participating organizations responsibilities.

4.1 Enterprise and Service Maturity

This subsection defines the organization and the procedures that govern the operations of the identity provider.

4.1.1 Göteborgs universitet, organisationsnummer 202100-3153, är en statlig utbildningsmyndighet vilket gör att lärosätets verksamhet regleras i lagar, förordningar och regleringsbrev.

4.1.2 De viktigaste lagarna och förordningarna som styr universitetets/högskolans arbete är regeringsformen (SFS 1974:152), tryckfrihetsförordning (SFS 1949:105), myndighetsförordningen (SFS 2007:515), högskolelagen (SFS 1992:1434) och högskoleförordningen (1993:100). Regleringsbrevet utställs årligen av regeringen och styr universitetets uppdrag under ett kalenderår. I övrigt följer lärosätet Sveriges övriga lagar och förordningar.

Lärosätets identitets- och behörighetssystem AIDA innehåller uppgifter om lärosätets organisation samt personuppgifter om alla som är verksamma vid lärosätet. Med avseende på detta måste särskild hänsyn till behandling av personuppgifter tas enligt aktuell personuppgiftslagstiftning.

Som statlig myndighet arbetar lärosätet även med ledningssystem för informationssäkerhet enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet.

4.1.3 Rutiner finns i Regler för IT-säkerhet, punkt 5.5
1516606_it-s--kerhetsregler_-revidering20150212.pdf (gu.se)

“För att förhindra att lagrad information, så som personuppgifter, forskningsdata, sekretessbelagd information och liknande blir tillgänglig för obehöriga, skall alla utrangerade minnesmedier raderas och överskrivas eller destrueras mekaniskt på ett säkert sätt.”

4.2 Notices and User Information

The Member Organisation provides an Acceptable Use Policy (AUP) and a Service Definition including a Privacy Policy (PP) for the organisation Subjects. These

policies are needed to fulfil the SWAMID Policy and the Swedish legislation including the General Data Protection Regulation (EU) No 679/2016.

4.2.1–4.2.4 Alla måste godkänna ansvarsförbindelse via Medarbetarportalen/studentportalen samt förnya godkännandet var 6:e månad eller vid förändringar av avtalet.
Ansvarsförbindelsen hänvisar till regler för användning av GU: s IT resurser.
http://medarbetarportalen.gu.se/sakerhet/blanketter/

4.2.2 Om personen inte godkänner ansvarsförbindelsen kan de inte logga på.
Det finns ingen tidsgräns men man kommer inte vidare om man inte godkänner ansvarsförbindelsen.
Vi loggar vem som har godkänt ansvarsförbindelsen.

4.2.3 Vid ändringar av avtalet måste samtliga användare godkänna det på nytt.

4.2.5 Tjänstebeskrivning: https://idp3.it.gu.se/idp/servicedefinition.jsp

4.3 Secure Communications

This subsection defines how clear text passwords, private keys and shared secrets must be protected to obtain operational security.

4.3.1–4.3.4 Behörigheter till olika system styrs med hjälp av medlemskap i behörighetsgrupper. Behörighet beställs av chef och revideras årligen. Endast behörig personal kan komma åt och administrera både system och applikation.

Privata nycklar och annan skyddsvärd konfiguration skyddas med standard Java keystore och behörighetskontroll.
All nätverkskommunikation mellan inblandade system sker krypterat. Minst 2048-bitar för IdP-nycklar/certifikat används.

4.4 Security-relevant Event (Audit) Records

This section defines the need to keep an audit trail of relevant systems.

4.4.1 Alla aktiviteter som inloggningsförsök, utloggning, lösenordsbyte, kontoskapande, ändring av behörigheter och inaktivering loggas med tidsstämpel, administratörens UID om det görs via gränssnitt plus annan relevant data på IdP och AIDA (Webbgränssnitt för användaradministration).

5. Operational Requirements

The purpose of this section is to ensure safe and secure operations of the service.

5.1 Credential Operating Environment

The purpose of this subsection is to ensure adequate strength of Subject credentials, such as passwords, and protection against common attack vectors.

5.1.1 Nya konton samt byten av lösenord till dessa gås igenom av GUKONTO:s API där en och samma algoritm körs för generering av lösenord enligt följande:
Mellan 8 och 16 tecken långt (Automatgenererade får 9-tecken).
Manuellt byte måste bestå av minst 8 tecken samt följ ADts krav på komplexa lösenord.

5.1.2 Tillbörlig kryptering används (TLS)
Patchning och övervakning sker regelbundet.

5.1.3 Användarregler inklusive lösenordspolicy finns och är publicerade här:
https://medarbetarportalen.gu.se/digitalAssets/1516/1516606_it-s--kerhetsregler_-revidering20150212.pdf

Användaridentitet, lösenord och tilldelad behörighet skall vara personlig. Lösenorden skall hållas hemliga och får inte lånas ut.

5.1.4 Riskreducerande åtgärder- Brandvägg och endast relevanta portar för tjänsten är öppna utåt. SSH åtkomst låst till GU:s nät. Uppdateringar sker regelbundet via RedHat Satelite samt så är SELinux aktiverat på samtliga berörda servrar

5.2 Credential Issuing

The purpose of this subsection is to ensure that the Identity Provider has control over the issuing process including issuing of credentials and binding of other information to the Subject. Furthermore, the Identity Provider and its Subjects must be uniquely identified.

5.2.1 Identitetshanterarens DNS-domän är gu.se och denna domän används som scope för attribut.

5.2.2 EntityID för identitetsutfärdaren https:/idp3.it.gu.se/idp/shibboleth

5.2.3 Vi återanvänder aldrig kontonamn och varje användare får minst en unik identifierare (eduPersonPrincipalName). De användarnamn som delats ut sparas och kan inte delas ut till en annan person.

5.2.4 Om en person har flera roller så tilldelas den personen flera konton. Vid inloggning anges kontot för den rollen man vill använda.

5.2.5 Vid personlig utdelning av kontouppgifter godtar vi ett pass eller identitetskort som uppfyller Polisen krav https://polisen.se/tjanster-tillstand/pass-och-nationellt- id-kort/besok-passexpedition/giltiga-id-handlingar/, nationella id-kort inom EU och internationella pass. Identitetskontrollen innefattar:
Att det är en äkta och godkänd id-handling
Att legitimationshandlingen är giltigt
Namn
Födelsedata/personnummer
Jämföra foto med person framför sig

Namn och personnummer/samordningsnummer/interimsnummer är förregistrerade och kontrolleras manuellt vid personlig utdelning. Detta ger SWAMID AL2.

I vår självservice kan man identifiera sig med svensk e-legitimation tillitsnivå 3 eller 4, samt Antagning.se och eduID (minst AL2).
Personnummer från tjänsterna ovan används som identifierare. Detta ger SWAMID AL2.

Vid självservice sätter användaren ett eget lösenord och vid personlig utdelning sätter administratören ett lösenord.

Vid självservice krävs svenskt personnummer.

Utländska studenter som inte är på plats i Göteborg har möjlighet att få en tidsbegränsad PIN-kod skickad via e-post alternativt brev till registrerad hemadress efter kontakt med vårt Servicecenter. I ärendet bifogas bild på pass för kontroll av personuppgifter.
PIN-koden kan tillsammans med en CAPTCHA användas för att sätta ett lösenord på kontot. Detta ger SWAMID AL1.
Fördefinierad identifierare är förnamn, efternamn, interimspersonnummer (födelsedata), e-postadress och hemadress. Denna information hämtas från Ladok.

Ovan rutin måste göras om varje gång en utländsk student har glömt sitt lösenord.

För att byta från AL1 till AL2-nivå krävs antingen:

- Att användaren besöker något av våra Servicecenter och uppvisar sin legitimation. Personnummer, alternativt riskbaserad bedömning av förnamn, efternamn och födelsedata, används för att säkerställa att det är avsedd person. Detta ger SWAMID AL2
- Identifierar sig med svensk e-legitimation tillitsnivå 3 eller 4. Personnummer används för att säkerställa att det är avsedd person. Detta ger SWAMID AL2
- Identifiera sig via eduID (minst AL2). Personnummer, alternativt manuell riskbaserad bedömning av förnamn, efternamn och födelsedata, används för att säkerställa att det är avsedd person. Detta ger SWAMID AL2.

Anställda och studenter får två olika kontotyper. Grundbehörigheterna på dessa typer skiljer sig åt.
Alla användarkonton exponeras mot SWAMID.

5.2.6 Vi loggar förändring av tillitsnivå på konton.

5.2.7 Information i vår katalogtjänst kommer alltid från ett källsystem såsom Ladok, Primula och POP (vår person-organisationsdatabas). Ändring av information görs av användaren själv eller av en administratör i respektive system.

5.2.8 Alla våra kontoadministratörer samt IT-tekniker som arbetar och har tillgång till systemen är alltid minst tillitsnivå AL2.

5.3 Credential Renewal and Re-issuing

The purpose of this subsection is to ensure that Subjects can change their credential and get new credentials when lost or expired.

5.3.1 En person kan byta sitt lösenord enligt samma metoder som i punkt 5.2.5 eller om man känner till sitt nuvarande lösenord.

5.3.2 Känner användaren till sitt nuvarande lösenord måste det uppges för att byta lösenord.

5.3.3 Vi använder samma rutiner som i 5.2.5 för återställning av lösenord där de förregistrerade identifierarna som användes vid kontoaktiveringen används

5.4 Credential Revocation

The purpose of this subsection is to ensure that credentials can be revoked.

5.4.1 Inaktivering sker enligt livscykelhantering. Studentkonton raderas 12 månader efter senast avslutad kurs. Anställdas konton inaktiveras 21 dagar efter att anställningen avslutats i Primula. Externa medarbetares konton inaktiveras när giltighetstiden för kontot gått ut. Giltighetstiden för externa konton är maximalt 2 år och kan förlängas av behörighetsadministratörer på avdelningen.

Återaktivering sker om personen återupptar sina studier eller sin anställning/uppdrag på Göteborg universitet.
Inaktivering kan även ske vid misstanke om missbruk, beställning kommer då från säkerhetsenheten på Göteborgs universitet.
Inaktivering kan även ske på användarens begäran

5.4.2 När vi ser ett onormalt beteende på ett konto så sätter vi om lösenordet och inaktiverar kontot samt kontaktar användaren för att byta sitt lösenord.
Återaktivering av ett konto sker på beställning av säkerhetsenheten och användaren får åter tillgång till sitt konto genom samma rutiner som i 5.2.5.

5.4.3 Vi följer MSBs regelverk samt informerar och utbildar kontinuerligt våra användare. IRT utreder varje säkerhetsincident och implementerar nödvändiga åtgärder för att undvika återupprepningar av incidenten

5.5 Credential Status Management

The purpose of this subsection is to ensure that credentials are stored accordingly and that Identity Management systems have a high degree of availability.

5.5.1 Alla utfärdade identiteter finns lagrade i AD och loggfiler. Användarnamnen raderas aldrig och kan inte återanvändas för nya användare.

5.5.2 Identitetsutfärdaren används även för inloggning till universitetets interna system och är övervakade och tillgängliga 24/7/365.

5.6 Credential Validation/Authentication

The purpose of this subsection is to ensure that the implemented

Validation/Authentication processes meet proper technical standards.

5.6.1-5.6.3 Vi uppfyller Swamids rekommendationer enligt SWAMID Identity Assurance Level 2 Profile (SWAMID AL2).

Vid inloggning krävs att användare uppger sina kontouppgifter.

5.6.4 Livslängden på våra SSO-sessioner är nio timmar.