Chalmers Identity Management Practice Statement 2024-09-17

.

1. Inledning

Dokumentet beskriver Chalmers system och rutiner för konto- och behörighetshantering i syfte att uppfylla kraven för både SWAMID AL1 och AL2.

4. Organisational Requirement.

4.1 Enterprise and Service Maturity

4.1.1 Chalmers tekniska högskola AB ägs till 100% av Stiftelsen Chalmers tekniska högskola, organisationsnummer 855100-5799.

Chalmers tekniska högskola AB (Chalmers) bedriver utbildning och forskning inom teknik, naturvetenskap, samhällsvetenskap och därmed samhörande vetenskaper. Chalmers tekniska högskola AB, organisationsnummer 556479-5598, är ett aktiebolag med säte i Göteborg.

Den del av verksamheten som är finansierad av svenska staten är reglerad i ett ramavtal mellan svenska staten, Stiftelsen Chalmers tekniska högskola och Chalmers tekniska högskola AB som gäller till år 2024. Utöver detta sluter Chalmers och svenska staten ettåriga avtal som reglerar högskolans rätt till ersättning, återrapporteringskrav till staten samt uppdrag att bedriva grundläggande högskoleutbildning, forskarutbildning och forskning.

4.1.2 De viktigaste lagarna som styr Chalmers verksamhet är Aktiebolagslagen (SFS 2005:551), Offentlighets- och sekretesslagen (SFS 2009:400) och Lagen om offentlig upphandling (SFS 2016:1145).

Chalmers katalog- och behörighetssystem Chalmers persondatabas (PDB) 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.

Studenters personuppgifter hämtas ur lärosätets studiedokumentationssystem Ladok och därför gäller även förordning (SFS 1993:1153) om redovisning av studier m.m. vid universitet och högskolor för hanteringen av studenters personuppgifter i PDB.

4.1.3 Chalmers arbete med informationssäkerhet utgår från Chalmers Informationssäkerhetspolicy (*C 2019-1092*) och tillämpar ISO/IEC 27000.

All lagringsmedia som används av Chalmers katalog- och behörighetssystem eller dess underliggande stödsystem omfattas av rutin för Hantering av lagringsmedia servrar. Rutinen innebär att all använd lagringsmedia skall skickas för destruktion.

4.2 Notices and User Information

4.2.1 Chalmers föreskrifter för användning av Chalmers IT-resurser (C 2020-0419 - Riktlinjer för informationssäkerhet, C 2020-0420 - Föreskrifter för informationssäkerhet samt C 2020-0459 - Föreskrifter för studenters användande av

IT-resurser) gäller för respektive grupp av användare. Föreskrifterna finns publicerade på Chalmers intranät och i Studentportalen.

Chalmers styrelse har för grundutbildningen fastställt en Arbetsordning (C2010/1283) och en Disciplinstadga (C2014/827). I enlighet med dessa gäller alla Chalmers regler och föreskrifter för Chalmers samtliga studenter.

4.2.2 Användarna godkänner användarreglerna när de får tillgång till kontot.

4.2.3 När användarreglerna uppdateras informeras användarna om detta via ett e-postmeddelande.

4.2.4 Eftersom att samtliga användare anses känna till och följa aktuella användarregler för vi inget register.

4.2.5 Tjänstedefinition finns på https://www.ita.chalmers.se/ServiceDefinitionWebSSO.html.

4.3 Secure Communications

4.3.1 Administrativ tillgång till system för behörighetskontroll är begränsad till ett fåtal individer på IT-avdelningen. Beslut om administrativ tillgång till systemen fattas av enhetschef. All administrativ access till inblandade system sker krypterat med SSH eller RDP.

4.3.2 Privata nycklar och delade hemligheter skyddas på filsystemsnivå i respektive system så att bara administratörer av systemet har tillgång till dem.

I PDB finns en skrapkortsdatabas som innehåller informationen som är tryckt på Chalmers skrapkort. I normalfallet är det enbart applikationen PDB som har tillgång till databasen. När ett skrapkort kopplas till en person nollas respektive fält i databasen.

4.3.3 Chalmers använder TLS eller motsvarande för all kommunikation mellan inblandade system och har inga nycklar med mindre nyckellängd än 2048 bitar.

4.3.4 Inga nycklar eller delade hemligheter för Chalmers IdP eller SPs används längre än tio år.

4.4 Security-relevant Event (Audit) Records

Samtliga inblandade system loggar säkerhetsrelaterade händelser.

PDB har en händelselogg som loggar alla förändringar rörande ett datorkonto.

AD loggar alla händelser till separat syslogserver.

Kerberos loggar alla förändringar avseende konton och alla lyckade/misslyckade inloggningar.

IDP:n (ADFS) loggar alla lyckade/misslyckade inloggningar.

Myaccount (frontend framför PDB) loggar alla lyckade/misslyckade inloggningar samt operationer som gjorts av användaren. Koppling finns till motsvarande händelse i PDB.

5. Operational Requirements

5.1 Credential Operating Environment

5.1.1 Chalmers lösenordspolicy kräver minst 10 tecken långa lösenord med komplexitetskrav (se Policy om egenskaper för lösenord).Rate limiting görs på inloggningsförsök mot AD (max 150 försök på 10 minuter).

5.1.2 Chalmers använder TLS eller motsvarande för all kommunikation mellan inblandade system och har inga nycklar med mindre nyckellängd än 2048 bitar.

Chalmers synkroniserar inte lösenord med externa leverantörer, t.ex. molntjänster.

5.1.3 När en person får sitt datorkonto informeras den om att datorkontot är personligt och inte får delas med andra samt att lösenordet inte får lämnas ut till någon annan (se respektive föreskrift för användning av Chalmers IT-resurser)

5.1.4 Ingående system sköts på ett fackmannamässigt vis. Systemen patchas regelbundet, ofta automatiskt. Brandväggar skyddar och begränsar nätverksaccess. Endast utsedd personal har administrativ access.

5.2 Credential Issuing

5.2.1 Chalmers använder sig av DNS-domänen chalmers.se.

5.2.2 Chalmers IdP har ett globalt unikt entityID.

5.2.3 Alla Chalmers datorkonton (CID) är unika och återanvänds ej.

5.2.4 En person kan ha flera konton knutna till sin personpost. Vid inloggning anges vilket konto man vill använda.

5.2.5 Personinformation för olika typer av konton:

- Anställda hämtas från Chalmers personalsystem med automatik
- Studenter hämtas från LADOK med automatik
- Gäster läggs upp manuellt av PDB-registrator

För samtliga kategorier finns minst förnamn, efternamn och födelsedatum. Födelsedatum används bara när det inte finns ett personnummer, samordningsnummer eller interimspersonnummer (från Ladok). Dessa används som förregistrerade identifierare.

Godkända identitetshandlingar är:

- inom Sverige giltig identitetshandling enligt Polisens regelverk för utlämning av pass,
- ett pass som uppfyller ICAO Doc 9303,

- ett nationellt identitetskort inkl. information om medborgarskap enligt EU-förordning 562/2006 eller

Vi kallar de som administrerar konton på Chalmers för PDB-registratorer. För att få de rättigheter som rollen medför görs en kontroll av identitetshandling och detta registreras genom medlemskap i en grupp i PDB.

PDB-registratorer innehar ofta även rollen TCS-registrator som är en utökning av rollen PDB-registrator med skillnaden att en TCS-registrator själv har fått sin identitet kontrollerad genom att personligen uppvisat godkänd identitetshandling och därmed uppfyller kraven för AL2. TCS-registrator kan höja en persons tillitsnivå från AL1 till AL2 genom att utföra en identitetskontroll samt kontrollera att person, identitetshandling och datorkonto stämmer överens. Om allt är i sin ordning markerar TCS-registratorn personen som kontrollerad i PDB. Status för om en person är identitetskontrollerad lagras som ett attribut i personobjektet i PDB. Endast TCS-registratorer kan förändra attributet om identitetskontroll i PDB. Alla operationer i PDB loggas i en händelselogg. Det går utifrån händelseloggen att se vilken TCS-registrator som gjort en identitetskontroll på vem och när.

Personer som arbetar för eller i samarbete med Chalmers får sitt datorkonto av PDB-registratorer eller av servicedesk. För studenter som kommer på förstagångsregistreringen erhålls datorkonto i samband med utdelning av övrig information vid detta tillfälle. För de studenter som inte kommer på denna registrering kan de erhålla sitt datorkonto vid IT-avdelningens helpdesk.

För att ett konto skall aktiveras behöver ett lösenord kopplas till ett konto. Innan detta är gjort fungerar inte datorkontot. Detta kan ske via ett skrapkort, som innehåller 4 positioner med olika lösenord med olika längd som hör till datorkontot (CID). Position 1 innehåller ett 10 tecken långt lösenord som uppfyller våra komplexitetskrav och är det som sätts som lösenord för datorkontot (CID). Position 4 innehåller en fyrsiffrig PIN-kod som används för inpassering. Position 2-3 används för närvarande inte. Den som får ett skrapkort behöver själv skrapa fram sitt lösenord och rekommenderas att byta lösenordet men det är inte ett krav. Det går också att sätta engångslösenord med hjälp av samma sorts skrapkort. Lösenordet fungerar då bara för att sätta ett nytt lösenord i PDB:s webbgränssnitt.

Skrapkort kan lämnas ut av PDB-registratorer (AL1) och TCS-registratorer (AL1 eller AL2). För personer med tillitsnivå AL1 görs normalt sett en identitetskontroll men skrapkort kan även delas ut om personen är känd eller om någon annan kan intyga personens identitet i enlighet med Skatteverkets föreskrifter om identitetskort (SKVFS 2009:14). För personer med tillitsnivå AL2 görs identitetskontroll enligt ovan innan skrapkort lämnas ut.

Engångslösenord kan även lämnas ut av en TCS-registrator via videosamtal (AL1). Användaren måste då tillhandahålla en högupplöst bild av en giltig och godkänd identitetshandling. TCS-registratorn verifierar att legitimationen uppfyller kraven och att den kan knytas till en person i PBD och att personen konto inte är spärrat eller inaktivt. Därefter upprättas ett videosamtal där användaren visar upp samma identitetshandling som det skickats bild på. TCS-registratorn verifierar dels att

handlingen är den samma som den inskickade och dels att den identifierar användaren. Om TCS-registratorn är nöjd tilldelas användaren ett engångslösenord.

I samtliga fall av manuell handläggning används person- eller samordningsnummer som förregistrerad identifierare; om ingetdera är tillgängligt används en riskbedömd kombination av namn, födelsedatum och land.

Det andra sättet att koppla ett lösenord till ett konto är att logga in i myaccount.chalmers.se via en betrodd identitetsutfärdare i SWAMID eller svensk e-legitimation. Personmatchningen sker då på person-, samordnings- eller interimspersonnummer i Ladok, eller eduPersonPrincipalName, och personen får den tillitsnivå som identitetsutfärdaren signalerar, dock högst AL2. För svensk e-legitimation anses tillitsnivå 3 eller högre motsvarar AL2. myaccount.chalmers.se verifierar att en Swamid-IdP inte signalerer en högre tillitsnivå än vad den är godkänd för, via dess metadata som hämtas från Swamid. Vid all inloggning i myaccount.chalmers.se krävs att identitetsutfärdaren omautentiserar användare, och man blir automatiskt utloggad efter 5 minuters inaktivitet.

5.2.7 Alla självuppgivna uppgifter som lagras i PDB kan användaren själv ändra. Exempel på möjlig självuppgiven information är privat mobiltelefonnummer, privat e-postadress och rumsnummer.

Via myaccount.chalmers.se kan användare få reda på sitt CID, sätta lösenord samt PIN-kod för passerkort.

5.3 Credential Renewal and Re-issuing

5.3.1 Användare kan byta lösenord.

5.3.2 Användare som kan sitt lösenord, kan använda det för att sätta ett nytt lösenord i en självservicetjänst, där man anger kontonamn, det gamla lösenordet och det nya lösenordet.

5.3.3 Användare kan få sitt lösenord återställt via någon av de rutiner som beskrivs i 5.2.5. De förregistrerade identifierarna beskrivna i 5.2.5 används för att säkerställa att det är samma person som genomför återställningen som är innehavaren av kontot.

5.4 Credential Revocation

5.4.1 Ett konto kan spärras av flera anledningar exempelvis: missbruk, disciplinärende, obetald kåravgift, misstänkt phishing eller på egen begäran. Detta kan ske både manuellt och med automatik och resulterar i att kontostatus i PDB sätts till ”spärrad” och kontot blir då oanvändbart (inaktiverat i AD och Kerberos). I samband med att ett konto spärras skapas ett ärende i IT-avdelningens ärendehanteringssystem.

Alla konton är tidsbegränsade och när tiden löpt ut inaktiveras kontot med automatik.

- För studenter är ett konto aktivt så länge de är registrerade på en kurs med tid för omtentor tillagt (inte längre än 15 månader efter kursstart).
- För anställda är konton aktiva så länge de är anställda enligt Chalmers personalsystem.
- För gäster är konton aktiva till det datum som är satt (max 3 år).

5.4.2 För att häva en spärr behöver orsaken till att kontot spärrades vara hanterad och tillhörande ärende avslutat. IT-avdelningen försöker kontakta användare via någon alternativ kanal, t.ex. telefon eller privat email, men om ingen sådan är tillgänglig måste vi vänta på att användaren kontaktar oss. Konton med statusen ”spärrad” markeras tydligt med röd bakgrund i PDB så att personen som hanterar kontofrågor enkelt kan se det. När ärendet är hanterat och personen åter skall få tillgång till kontot sätts ett nytt lösenord på samma sätt som 5.3.

5.4.3 Chalmers Cyber- och informationssäkerhetsgrupp (CCIG) arbetar både reaktivt och förebyggande för att förhindra säkerhetsincidenter, och de följer upp varje ärende kring spärrade konton.

5.5 Credential Status Management

5.5.1 Datorkonton administreras med PDB. PDB innehåller information om vilka konton vi har och vilken status ett konto har, exempelvis aktivt/inaktivt. Alla förändringar loggas i en händelselogg. Vi tar aldrig bort datorkonton ur PDB.

5.5.2 Identitetsutfärdaren användes även för interna system. Vi har mer än 95% tillgänglighet (>99% under 2016–2017).

5.6 Credential Validation/Authentication.

5.6.1 Vi följer SWAMIDs rekommendationer.**5.6.2** Det går inte att autentisera sig mot IdP:n med ett konto som är spärrat eller inaktivt.

5.6.3 För att logga in i IdP:n måste användaren uppge kontonnamn och lösenord.

5.6.4 En IdP-session är giltlig i 8 timmar, därefter måste användaren autentisera sig enligt 5.6.3 igen.