Dokumentnamn	Namn	Version
LTU Behörighetspolicy	Behörighetspolicy	A2
Utfärdat av	**Beslutsdatum**	**Diarienummer**
Gunnar Östlund Jan Lundmark	2016-03-04	2364-13
Beslutat av	**Gäller från och med datum**	**Sida**
Anders Nordin	2016-03-04	1 (7)

Luleå Tekniska Universitet

Behörighetspolicy

Innehållsförteckning

1 Styrning av användarbehörighet

1.1 Unik användaridentitet

Varje individ som skall beredas tillgång till IT-resurser inom LTU skall identifieras med en personlig användaridentitet, nedan kallad LTU-identitet, som lagras i universitetets centrala autentiseringssystem.

Undantag från denna regel är tillåtna under förutsättning att:

- Resursen inte innehåller, eller tillåter förändringar av verksamhetskritisk information.
- Resursen inte ger tillgång till konfidentiell information.
- Resursen inte hanterar personinformation enligt Personuppgiftslagen, PUL.
- Resursen inte är integrerad med andra system där autentisering sker mot LTU-identitet.
- Det användarnamn som eventuellt används vid inloggning inte är detsamma som för personens LTU-identitet.

Tillfälliga eller permanenta undantag från ovanstående kan även beslutas i enskilda fall av universitetets IT-chef om behoven kan anses tillräckliga.

1.2 Styrning av rättigheter

Styrning av rättigheter för åtkomst av IT-resurser skall göras i eller via universitetets centrala katalogtjänst i de fall rättigheterna omfattar mer än ett IT-system. För att rättighetsstyrning skall kunna omfatta flera IT-system krävs att användare identifieras med hjälp av sina LTU-identiteter.

Tillfälliga eller permanenta undantag från ovanstående kan även beslutas i enskilda fall av universitetets IT-chef om behoven kan anses tillräckliga.

1.3 Styrning av lösenord

Lösenord är strängt konfidentiella och skall behandlas i enlighet med detta. Lösenord får inte lämnas ut till obehöriga eller förvaras på sådant sätt att obehöriga kan ta del av det.

Lösenord som används för identifiering av LTU-identiteten får inte återanvändas i andra sammanhang eller mot andra system som inte använder LTU-identiteten för autentisering.

Lösenordet ska även uppfylla följande krav:

- Lösenordet skall vara minst 8 tecken långt.
- Lösenordet skall innehålla minst en versal.
- Lösenordet skall innehålla minst en gemen.
- Lösenordet skall innehålla minst ett tecken som inte tillhör ovanstående kategorier.
- Lösenordet ska bytas minst var 24:e månad (tvingande funktion)

1.4 Granskning av behörigheter

Varje IT-system skall ha en ansvarig granskare som regelbundet reviderar behörigheter i systemet. Denna revision ska ske minst en gång per år.

Vid förändrad "arbetsuppgift" samt vid till eller frånträde av tjänst så skall översyn och uppdatering av behörigheter ske omedelbart enligt fastställda rutiner.

Beslut om avsteg från sådan rutin skall dokumenteras med anledning och beslut från ansvarig Chef.

Personer som (i dagsläget) saknar organisatorisk anknytning till LTU (fd. anställda, konsulter, externa leverantörers anställda, gästlärare med flera) måste knytas till såväl enhet/avdelning som till en ansvarig Chef som har mandat att fatt beslut om dessa personers behörigheter.

2 Användarens ansvar

Användaren är ansvarig för att upprätthålla informationssäkerheten genom att följa beslutade rutiner och använda IT-miljön på ett sådant sätt att de tekniska säkerhetslösningarna inte åsidosätts eller kringgås.

2.1 Användning av lösenord

Användaren ansvarar för lösenordssekretessen. I detta ingår att:

- Alla lösenord som används inom LTU:s IT-miljö är utformade i enlighet med kraven under avsnitt 1.3 .
- Obehöriga inte får tillgång till det personliga lösenordet. I detta ingår även förvaring och inmatning av lösenordet så att obehöriga inte kan ta del av det.
- Inte avslöja sina personliga lösenord vid LTU för andra, inklusive kollegor, familjemedlemmar, överordnade chefer och personal vid IT-service.
- Inte återanvända samma lösenord vid inloggning i olika system vid LTU såvida dessa inte är kopplade till den centrala autentiseringen och använder LTU-identiteter för autentisering.
- Inte använda samma lösenord som används i system vid LTU som används i tjänster utanför LTU oavsett om dessa används i tjänsten, studierna eller privat.
- Säkerställa att inloggning mot LTU:s system endast sker från sådana enheter (datorer, telefoner, pekplattor) eller på sådant sätt att lösenordet inte kan avlyssnas, läsas eller på annat sätt avslöjas för obehöriga.

2.2 Säker inloggningsrutin

Användaren skall vid inloggning med lösenord försäkra sig om att ingen annan kan se vilket lösenord som matas in. Om användaren lämnar datorn utan tillsyn skall obehörig tillgång till datorn förhindras på något av följande sätt:

- Tillgång till datorn förhindras genom att aktivera operativsystemets mjukvarulås (ofta kallat kallad skärmlåsning) så att lösenord måste anges för upplåsning.

- Användaren manuellt loggar ut ur datorn.
- Datorn förvaras inlåst i kontor eller dokumentskåp.

3 Styrning av behörigheter i nätverk

Tillgång till nätverksresurser inom LTU skall endast ges på sådant sätt att enhetens ägare eller användare kan identifieras på ett tillfredsställande sätt. Om detta inte kan ske får enheten inte anslutas till nätverksresurser inom LTU.

3.1 Identifiering av utrustning i nätverk

Identifiering kan ske på följande sätt:

- Registrering av enhetens unika nätverksadress i därför avsett register.
- Inloggning direkt mot nätverket med personlig användare ingående i samarbetet kring Eduroam (vilket inkluderar LTU-identiteten).
- Utrustningen har en identifierad ägare, nyttjar trådbundet nät, står fast placerad på sådant sätt att obehöriga inte kan ansluta utrustning till samma nätverksuttag samt tilldelats en fast nätverksadress inom någon av LTU:s IP-nät med IP-nummerserie (13.240.0.0/16).

Utrustning som inte kan identifieras på något av ovanstående sätt får inte anslutas till universitetets nätverk.

3.2 Uppdelning i nätverk

Universitetets nätverk skall vara uppdelat på ett sådant sätt att tillräckligt skydd erhålls för att:

- Upprätthålla tillräcklig informationssäkerhet i enlighet med universitetets informationssäkerhetspolicy.
- Möjliggöra skalbar indelning av resurser utifrån deras behov av behörighetsstyrning och/eller åtkomstskydd.

3.3 Skydd av nätverksutrustning

Centrala resurser i LTU:s nät ska ha tillräckligt fysiskt åtkomstskydd.

Dessa resurser ska vara identifierade och klassificerade samt dokumenterade.

Denna dokumentation ska revideras en gång per år.

4 Styrning av behörigheter till operativsystem

4.1 Autentisering av användare

Användare av samtliga datorsystem vid LTU skall vara identifierade så att det är möjligt att i efterhand avgöra vem som använt en dator vid varje specifik tidpunkt. För att detta skall vara

möjligt måste minst ett av följande krav vara uppfyllda:

- Att personlig inloggning används för att identifiera användaren innan denne får tillgång till operativsystemsresurser samt att in- och utloggning registreras i loggfil som inte är åtkomlig så att den kan manipuleras av användaren själv.
- Att tillgång till datorn endast ges genom personligt utkvitterande av nyckel, engångskod, smartcard eller motsvarande, att användarens identitet är verifierad och noterad i logglista med information om mellan vilka tidpunkter tillgången givits.
- Att inloggning för en mindre grupp anställda sker med gemensam inloggningsidentitet där användaren vid en viss tidpunkt i efterhand entydigt kan fastställas ur tjänstgöringsschema eller motsvarande dokumentation. Lösenordet skall i detta fall även bytas varje gång en person lämnar gruppen.

För tillgång till operativsystemsresurser skall samtliga datorer vid LTU vara försedda med lösenordsskydd med syfte att säkra identifiering av användare, vilket sker genom inmatning av användarnamn och lösenord.

4.2 Lösenordsrutin

Lösenordet ska alltid uppfylla de krav som ställs i avsnitt 1.3 . Byte av lösenord skall ske i följande fall:

- Om lösenordet inte uppfyller gällande krav på utformning som ställs i aktuell version av detta dokument.
- Om misstanke finns att obehöriga har fått kännedom om lösenordet, t.ex. genom obehörigt intrång i system eller oförsiktig lösenordshantering.

Kontroll och test av samtliga lösenord ska ske vid skapande eller byte, i syfte att hitta svaga lösenord som är alltför enkla att gissa sig till. Exempel på sådana lösenord är ”Abcd1234” eller användarnamnet med stor bokstav i början och en extra etta på slutet.

5 Styrning av behörigheter till information och tillämpningar

5.1 Begränsning av behörigheter till information och tillämpningar

Behörighetstilldelning till information eller resurser i LTU:s IT-miljö ska så långt det är möjligt vara rollbaserad och/eller styras på behörighetsgruppnivå.

Alla resurser ska vara kopplade till en eller flera behörighetsgrupper, som i sin tur har en eller flera medlemmar (personlig LTU-inloggning).

Varje behörighetsgrupp som inte administreras av ITS skall ha en ansvarig gruppägare som ansvarar för att gruppen endast innehåller aktuella medlemmar.

6 Mobil datoranvändning och distansarbete

6.1 Mobil datoranvändning och kommunikation

Anslutning till LTU's nät skall ALLTID ske via krypterad anslutning (te.x. med ssh eller VPN)

6.2 Distansarbete

Användare som har en enhet som är LTU:s egendom och anpassad för distansarbete har ansvar för att denna inte förändras på sådant sätt att säkerheten vid anslutning till LTU:s nät riskeras.

7 Övervakning, loggning och uppföljning

Loggning verksamhet kopplad till behörighetstilldelning och behörighetsansvar ska ske i tillräcklig omfattning så att lagkrav och verksamhetskrav efterlevs.

Det som bör beaktas och förtydligas vid kravställning på loggning är:

- Vilka resurser kräver spårbarhet på åtkomst och förändring?
- Vilka har haft åtkomst till resurs eller information och under vilken tid?
- Vilka förändringar har skett på behörighetstilldeningen och av vem?
- Hantering av skapade loggar vad avser arkivering, analys, tillgänglighet/konfidentialitet mm.
- Mandat att besluta om skapande, förändring och delgivning(offentlighetsprincipen) av loggar?

8 Automatisk utloggning

Automatisk utloggning eller automatisk skärmlåsning bör användas på samtliga klientenheter som används för att hantera information vid universitetet. Denna funktion får inte användas som ett substitut för manuell utloggning eller låsning då en enhet lämnas utan tillsyn, utan endast som ett komplement som kan bidra till att minska risken vid glömska eller oaktsamhet.

Användaren skall alltid själv, oavsett om automatisk låsning/utloggning finns implementerad, manuellt förhindra obehörig tillgång till systemet i enlighet med avsnitt 1 .