Dnr UFV 2013/1490

UPPSALA
UNIVERSITET

Lösenordshantering

Rutiner för informationssäkerhet

Fastställd av Säkerhetchef 2013-11-06
Senast reviderad 2021-03-02

Innehållsförteckning

1 Inledning

Detta dokument anger Uppsala universitets rutiner för kvalitet på, och hantering av, lösenord i enlighet med den svenska akademiska identitetsfederationen SWAMIDs tillitsprofil och lösenordspolicy[1].

Rutinerna har som syfte att stödja hanteringen av lösenord på universitetet, både personliga och systemhanterade, för att så långt som möjlig skydda universitetets information i olika system från obehöriga användare.

Rutinerna gäller för alla IT-tjänster och -system vid universitetet och omfattar både lösenordskvalitet och lösenordsskydd. De baseras på universitetets rutiner för informationssäkerhet (UFV 2017/93) och rutiner för riskhantering (UFV 2018/211).

2 Ansvar

2.1 Efterlevnad

Ansvaret för efterlevnad av dessa rutiner fördelar sig enligt följande:

Prefekt/motsvarande vid sin institution, avdelning eller motsvarande.

Systemägare, e-områdesansvarig/motsvarande för att följa rutinerna i utvecklings- och förvaltningsarbete samt driftuppdrag. Ansvar för efterlevnad gäller även då annan intern eller extern part anlitas för uppdraget. Utförande parts ansvar ska i förekommande fall regleras i ett s.k. servicenivåavtal.

Säkerhetschef för planering, samordning och uppföljning samt kontroll av efterlevnad.

Verksamma vid universitetet för att följa rutinerna.

2.2 Uppdatering av rutinerna

Säkerhetschefen ansvarar för att rutinerna kontinuerligt uppdateras och att underliggande stöddokument fastställs.

3 Definitioner

Gemensam webbinloggning[2] är en lösning för webbaserad inloggning som bland annat möjliggör en enda inloggning till många olika webbtjänster. Det förenklar för användarna och höjer samtidigt säkerheten. Webbtjänster anslutna till gemensam webbinloggning har inte tillgång till lösenord utan enbart till definierade personuppgifter.

[1] https://wiki.sunet.se/display/SWAMID/SWAMID+Policy, *2021-02-26*

[2] https://weblogin.uu.se, *2021-02-26*

Flerfaktorsautenticering/multifaktorautenticering är en metod för att bekräfta en användares identitet med två eller flera olika faktorer i flera steg, vilket ger en högre säkerhet än enbart ett lösenord. Faktorerna består av något man har (kort, dosa, mobiltelefon, mobilt BankID), något man vet (lösenord, PINkod) och något man är (biometri, t.ex. fingeravtryck).

4 Omfattning

4.1 För användare

Allmänt om lösenord

Alla användare har ett huvudlösenord (Lösenord A) som används för inloggning bland annat till universitetets nätverkstjänster och gemensamma tjänster som Primula, Ladok, Medarbetarportalen m.fl.

För vissa tjänster, till exempel Eduroam, har varje användare ytterligare ett lösenord (Lösenord B). Utöver dessa två lösenord kan verksamhets- och/eller systemspecifika lösenord finnas.

Du ansvarar själv för att

- dina lösenord uppfyller hantering och kvalitet enligt rutinerna,
- dina lösenord förvaras på ett säkert sätt och inte sprids till någon annan, varken via e-post, telefon eller på annat sätt,
- omedelbart meddela universitetets servicedesk (servicedesk@uu.se, tel. 4440) om lösenord kommit eller kan ha kommit på avvägar.

Bra lösenord (lösenordssammansättning)

Ett lösenord ska, för att ha bra kvalitet, bestå av minst 10 tecken – varav minst en versal, minst en gemen, och antingen minst ett specialtecken eller en siffra.

Rekommenderade tecken:

- versaler (A-Z), gemener (a-z),
- siffror (0-9),
- följande specialtecken: ~ ! @ # $ % ^ & ( ) _ + - * / = { } [ ] | \ : ; ? < > ” samt
- mellanslag, komma eller punkt.

Använd inte egennamn, årstider, bilmärken eller enbart sifferkombinationer. Ett av världens vanligaste lösenord är t.ex. 123456.

Notera att ett bra lösenord som byts sällan är säkrare än att byta mellan dåliga lösenord ofta.

Har du många olika lösenord kan en lösenordshanterare (se nedan) vara en god hjälp.

4.2 För systemförvaltare

Allmänt om IT-system

- Alla system ska vara kopplade till universitetets gemensamma webbinloggning om inte särskilda skäl föreligger. Skälen ska finnas dokumenterade.
  I den gemensamma webbinloggningen finns systemstöd för efterlevnad av rutinerna.
- För system som har egen lösenordshantering ansvarar systemägaren för efterlevnad.
- Om ett system inte använder universitetets gemensamma webbinloggning ska lösenord lagras i en säker envägskrypterad ("hashad") form inom systemet, för att försvåra om lagrade informationen skulle kommas åt av obehöriga.
- För outsourcing eller molntjänster ska krav på lösenordshantering finnas med i anskaffningsförfarandet och regleras i avtal.
- Flerfaktorautentisering ska användas för åtkomst till IT-system eller tjänster som enligt rutinerna för informationsklassning innehåller konfidentiell information. De system som idag inte har stöd för detta bör uppgraderas när så är möjligt, och avvikelser från detta dokumenteras i förvaltningsplan eller liknande.

Lösenordskvalitet

Ett lösenord med bra kvalitet är tillräckligt långt och komplext sammansatt för att minska risken för att en inkräktare kan gissa sig till det.

Längd och komplexitet på lösenordet formar tillsammans den s.k. entropin för lösenordet. Ju högre entropi ett lösenord har, desto svårare är det att gissa eller testa sig fram till. För mer information, se *NIST SP 800-63*[3]

Lösenordskontroll

I universitetets gemensamma webbinloggning finns teknikstöd för att säkerställa god lösenordskvalitet. Vid lösenordsbyte kontrolleras lösenord så att de

- är sammansatta enligt kraven ovan,
- inte återfinns i kataloger över lösenord av dålig kvalitet (som sifferkombinationer, egennamn, årstider, bilmärken etc),
- inte är detsamma som, eller för lika, det närmast föregående lösenordet

När användaren skriver in sitt förslag till nytt lösenord visas kvaliteten på lösenordet enligt en färgskala;

- Rött – uppfyller inte universitetets minimikrav,
- Gult – uppfyller minimikraven,

[3] https://www.nist.gov/itl/tig/projects/special-publication-800-63, *2018-08-01*

- Grönt – överträffar minimikraven.

Lösenord går inte att spara innan minimikraven uppfylls.

Lösenordsskydd

Säker lösenordshantering innebär att inloggningstjänsten skyddar lösenord från otillbörlig åtkomst och användning. Utöver detta ansvarar varje användare för att hålla sina lösenord hemliga och säkert förvarade.

Datalagring och transport av lösenord

För att reducera risken för obehörig åtkomst till lösenord gäller följande för lagring och transport av lösenord:

- Lösenord ska aldrig kommuniceras via e-post, telefon eller motsvarande.
- Elektronisk lagring och transport:
    - Lösenord ska alltid lagras och transporteras i krypterad form, även på backup-media
    - Lösenord ska aldrig presenteras i läsbar form
- Personal med teknisk åtkomst till datorer och datamedia där lösenord lagras (s.k. priviligierade behörigheter) ska underteckna särskilda ansvarsförbindelser.
- En aktuell, uppdaterad lista över medarbetare med priviligierade behörigheter ska finnas vid den organisatoriska enhet som sköter driften av systemet, normalt avdelningen för universitetsgemensam IT.

Skydd mot nätbaserade gissningsattacker

För att minska risken för automatiserade gissningsattacker ska inloggningen vara skyddad genom begränsningar som förhindrar någon att göra många upprepade inloggningsförsök (lösenordsgissningar) på kort tid, så kallad *rate limiting*.

Universitetets gemensamma webbinloggning har skyddet utformat så att enbart ett visst antal försök får göras inom en timme, sedan låses kontot automatiskt under ett specificerat antal minuter.

4.3 Lösenordshanterare

En lösenordshanterare – en programvara eller tjänst som genererar och lagrar lösenord för olika andra tjänster – är ett hjälpmedel för att få en säkrare lösenordsmiljö.

Det finns en mängd olika varianter av lösenordshanterare på marknaden. Både betalprogram, gratisprogram och appar, som alla fungerar på olika sätt.

Skyddsbehovet för resursen som omfattas av lösenordet bör vara det som avgör vilken modell som passar bäst.

Lösenordshanterare är extra viktigt för användargrupper med höga behörigheter i många system, som IT-drifttekniker.

För råd och stöd, kontakta säkerhetsavdelningen, security@uu.se.

4.4 Undantag

Om det i enskilda system finns särskilda skäl att inte följa ovanstående rutiner för lösenordskvalitet och/eller lösenordsskydd kan undantag godkännas av e-områdesansvarig/systemägare.

Undantag ska dokumenteras i systemets förvaltningsspecifikation eller motsvarande dokument. Dessutom måste särskild hänsyn tas vid åtkomst av data hämtad från andra system.