Lösenordspolicy

- Administrativt
- Definitioner
  - Accessrättighet
  - Attribute based access control
  - Användare/kontotyper/behörighetstyper
    - Användare
      - "vanlig användare"
    - Priviligierad användare
      - t.ex. "root" i ett Linux/unix-system
    - Högst priviligierad användare
    - Systemkonto/tekniskt användarkonto
      - maskin - maskin kommunikation
      - applikation som pratar med en annan applikation
      - 7muffins
  - Auktorisering
  - Autentisering
  - "Four eye principle"
  - Interaktiv pålloggning
  - Role based access control
  - Systemanvändare
- Avsikt
  - Lösenord ska finnas och användas för att förhindra obehörig
    - åtkomst till information
    - utförande av åtgärder
- Omfattning
  - denna policy beskriver organisationens krav
    - avsende
      - lösenords utformning
      - användande
    - för
      - användare
      - priviligierade användare
        - root
        - administratörer
        - etc
      - system/tekniska användare
    - att
      - Lösenord skall finnas och användas av alla användartyper
        - Lösenordet är i detta sammanhang att betecknas som "kvittot" på användarens identitet och behörighet att använda organisationens resurser.
        - Behörighet definieras i 7muffins policy.
      - Ingen access får ske utan att användaren är autentiserad och godkänd för access.
        - all åtkomst till organisationens resurser
          - förutsätter alltså adekvat autentisering
  - Högre krav på lösenords utformning är tillåtna men ska i så fall innan införande och användande beskrivas i separat dokumentation/process
  - I första hand bör flerfaktorautentisering användas.
    - för priviligierade användare vid anslutning till password vault/hoppserver SKA flerfaktorautentisering användas.
    - Exempel
      - Mobilt bankid
      - Freya eID
      - m.m.
- Roller och ansvar
  - användare
    - får ej dela sitt lösenord med andra användare
    - ska omgående anmäla om det konstaterats eller befaras att lösenord avslöjats
    - får ej använda sitt av organisationen tilldelade användarid och lösenord på externa system för icke tjänste relaterade skäl
      - detta gäller t.ex. sociala media, mobiltjänster för eget personlig bruk etc.
    - Information/utbildning om varför ska ske
  - applikationsägare
    - ansvarar för säkerheten avseende systemkonton
  - behörighetsadministration
    - ska ha instruktioner som tydligt klargör att denna policy/detta regelverk ska följas
- Referenser
  - ISO 27002
    - 9 Styrning av åtkomst
      - sid 19 - 28
    - 9.4.3 System för lösenordshantering
  - ISF
    - ISF Good Practice SA.01.04
  - NIST
    - https://pages.nist.gov/800-63-3/sp800-63c.html
    - https://pages.nist.gov/800-63-3/sp800-63c.html
- Multifaktor autentisering (MFA) bör användas
  - Detta är den bästa enskilt bästa säkerhetsåtgärden för åtkomst som kan införas i en organisation!
- Password vault/hoppserver med inspelningsmöjlighet för session SKA användas
  - för all priviligierad access
    - Systemadministratörer
    - System/maskin - maskinkommunikation
- Användning av lösenordshanterare uppmuntras
  - Exempel
    - 1password
    - Lastpass
    - Kortlåda förvarad i säkerhetsskåp
      - får ej delas mellan flera användare
    - SQRL
- Efter x antal misslyckade inloggningsförsök ska kontot låsas
  - uppläsning får ske efter xx antal minuter.
  - alternativt ska kontot låsas och upplåsning kräver kontakt med
    - helpdesk
    - användaradministrationen
    - 7muffins
- Längden på ett lösenord är mycket viktigare än eventuell komplexitet!
  - lösenordet får alltså bestå av stora och små bokstäver och specialtecken men behöver EJ så göra!
  - svenska tecken dvs å, ä, ö kan användas
- Lösenordspolicy
  - Lösenord ska
    - användarid och tillhörande lösenord ska
    - vara individuella
      - utan undantag
        - får alltså ej delas i en grupp
          - detta gäller framför allt även för t.ex. en grupp med priviligierade användare t.ex. systemadministratörer
    - vara minst 15 tecken långa
      - samma minimilängd för alla behörighetsgrupper
        - it-security baseline konfigureringsexempel
          - Linux
            - minlen=15
          - Windows
      - Exempel på bra lösenord/lösenordsfraser
        - KalleAnka är en serietidning som jag gillar
        - Min dotter är helt underbar!
    - de senaste xx lösenorden får ej återanvändas
      - it-security baseline konfigureringsexempel
        - Linux
        - Windows
    - inte mer än två lika tecken i rad
      - alltså ej
        - 333
        - bbb
        - etc
      - it-security baseline konfigureringsexempel
        - Linux
        - Windows
    - kontrolleras mot lösenordslistor dvs s.k. "vanliga mindre bra" eller "knäckta" lösenord
      - it-security baseline konfigureringsexempel
        - Linux
        - Windows
    - för priviligierade konton ha ett bäst före datum
      - Efter detta datum ska lösenordet spärras.
        - it-security baseline konfigureringsexempel
          - Linux
          - Windows
    - lösenord som kan kopplas till respektive person eller funktion ska ej användas
      - Använd alltså EJ
        - ditt personnummer eller del av personnummer, eller någon närstående personnummer
        - något som går att koppla till din fru/man, dina barn
        - din adress
        - servernamn
        - applikationsnamn
        - varianter på detta
        - etc
    - lagras åtskilt från data för tillämpningssystem
    - lagras på ett säkert sätt
      - vilket i normalfallet innebär kryptering med vedertagna godkända algoritmer
    - överföras på säkert sätt
      - överföring i klartext över interna eller externa nätverk får ej ske
    - ej synas/sparas i loggfiler
    - om lösenordet avses användas för "Disaster Recovery"
      - skrivas ner
      - förvaras i försseglat kuvert
      - i vårdskåp med åtkomstlogg och strikt begränsad access.
- Byte av lösenord
  - Lösenord ska normalt EJ vara tidsbegränsade
  - Lösenord SKA bytas omedelbart
    - När misstanke föreligger att någon kan ha sett dig använda lösenordet/tagit del av ditt lösenord.
      - Du behöver INTE vara säker på din sak. Minsta misstanke räcker...!!
    - När någon byter arbetsuppgift
  - vid byte ska föregående/det gamla lösenordet anges
  - Om/när ett AI system upptäcker konstigheter
    - skall lösenordet spärras
    - byte därefter ske av användaren
  - ska ske innan nya "system" (programvaror, databaser, datorer, lagringssystem, routrar, brandväggare etc) med av leverantören förinstallerade användaridentiter och standardlösenord får tas i drift
    - överflödiga/icke använda "inbyggda" konton och åtkomsträttigheter skall tas bort eller, om så ej är möjligt, inaktiveras
- Anställd
  - Start / börjar sin anställning
    - Överlämning av användarid och initialt lösenord
      - ska ske på säkert sätt
        - oskyddade (klartext) elektroniska meddelanden får ej användas
        - extern part ska undvikas
    - Initialt lösenord ska bytas vid första inloggning
  - Byte av arbetsuppgift/enhet
    - Alla accesser ska spärras
      - T.ex. genom att lösenord spärras
  - Slut / anställningens upphörande
    - Signal från HR-system ska ske omgående
    - Access ska låsas omgående
    - Byte av lösenord bör ske
    - Efter 7muffins tid ska användarid tas bort
    - Ansvar: Närmaste chef
      - HR-chef
- Konsult / tillfälligt anställd
  - Start / uppdragets början
    - Behörighet till vilka system
      - uppdragsledare / närmaste chef
    - Överlämning av användarid och initialt lösenord
      - ska ske på säkert sätt
        - oskyddade (klartext) elektroniska meddelanden får ej användas
        - extern part ska undvikas
    - Spärr av lösenord ska förberedas och kopplas till uppdragets längd
  - Byte av arbetsuppgift/enhet
    - Alla accesser ska spärras
      - T.ex. genom att lösenord spärras
  - Slut / uppdragets upphörande
    - Signal från leverantörsnekcontra/inköpssystem ska ske omgående
    - Access ska låsas omgående och automatiskt i enlighet med upphandlad uppdragslängd
      - Close of Business aktuell dag
      - ___
    - Byte av lösenord bör ske
      - Close of Business aktuell dag
    - Efter 7muffins tid ska användarid tas bort
    - Uppdragsledare/närmaste chef
      - Chef inköpsavdelning
- Hjälp med lösenordsbyte
  - Användaren ska identifieras på säkert sätt
  - Tilldelat lösenord ska bytas vid första inloggning
    - it-security baseline konfigureringsexempel
      - Linux
      - Windows
  - individuellt unikt lösenord av minst 15 teckens längd ska användas
    - it-security baseline konfigureringsexempel
      - Linux
      - Windows
  - Ett generellt "standardlösenord" av typen Sommar2019 etc får alltså ej användas
- System / maskin - maskin kommunikation
  - password vault ska användas