KYRKANS ALLMÄNNA DATASÄKERHETSBESTÄMMELSER

21.3.2019

Innehåll

1 Hantering av datasäkerheten

Delområdets namn	**1.1 Resurstilldelning**
Mål	Tillräckliga resurser har avsatts för skötseln av de praktiska uppgifter som gäller datasäkerheten. Även vikariatarrangemangen har beaktats.
Krav	1. Samtliga IT-områden/församlingsenheter[1] ska ha en utsedd datasäkerhetsgrupp. Dess uppgift är att utarbeta och uppdatera datasäkerhetspolicyn samt bestämmelserna och anvisningarna om datasäkerhet i sitt eget område i enlighet med de riktlinjer som gäller för hela kyrkan. Datasäkerhetsgruppen övervakar dessutom iakttagandet av bestämmelserna och anvisningarna om datasäkerhet, behandlar aktuella datasäkerhetsfrågor samt planerar och ordnar datasäkerhetsutbildning i samarbete med den datasäkerhetsansvariga och kontaktpersonerna för datasäkerhetsfrågor. I stora församlingsenheter kan man vid behov inrätta en egen datasäkerhetsgrupp om det med tanke på verksamhetens omfattning och särskilda behov anses nödvändigt. I detta fall preciserar datasäkerhetsgruppen de bestämmelser och anvisningar IT-områdets datasäkerhetsgrupp har utarbetat så att de motsvarar de lokala behoven och behandlar lokala och aktuella datasäkerhetsfrågor. 2. Varje IT-område/församlingsenhet ska ha en utsedd datasäkerhetsansvarig person. Hans eller hennes uppgift är att fortlöpande och aktivt utveckla datasäkerheten i områdets församlingar. Han eller hon svarar för att ge kontaktpersonerna, cheferna och alla anställda information om anvisningar och bestämmelser som gäller datasäkerhet. Dessutom tar han eller hon emot observationer om händelser och avvikelser i anknytning till datasäkerheten och rapporterar regelbundet om dem till datasäkerhetsgruppen. Händelser och avvikelser som gäller riksomfattande system och tjänster ska också rapporteras till kyrkans datasäkerhetschef. 3. Samtliga församlingsenheter ska ha en utsedd kontaktperson för datasäkerhetsfrågor. Kontaktpersonen ser till att alla anställda får information om bestämmelser och anvisningar som gäller

[1] Ett IT-område är ett avtalsbaserat IT-samarbetsområde mellan två eller flera självständiga församlingsenheter. En församlingsenhet är en självständig församling eller en kyrklig samfällighet. Det som sägs om ekonomiska församlingsenheter i detta dokument, gäller på motsvarande sätt även domkapitlet och Kyrkostyrelsen. Beteckningen IT-områden/de ekonomiska församlingsenheterna avser i detta dokument att frågan gäller alla ekonomiska församlingsenheter men att det är ändamålsenligt att ordna den enhetligt inom hela IT-området. Det är till exempel bra att datasäkerhetsgruppen är gemensam för alla församlingar i IT-området.

datasäkerheten och deltar som stöd för cheferna vid introduktionen av nyanställda i frågor som gäller datasäkerhet. Dessutom tar kontaktpersonen emot anmälningar om observerade händelser och avvikelser i datasäkerheten i sin församlingsenhet och rapporterar om dessa till den datasäkerhetsansvariga och till cheferna i församlingsenheten.

4. Varje församlingsenhet ska ha utsett ett eget dataskyddsombud. Dataskyddsombudets uppgift är att sköta de uppgifter som EU:s dataskyddsförordning ålägger dataskyddsombuden.

5. Arbetsgivaren ansvarar för att den datasäkerhetsansvariga och kontaktpersonen för datasäkerhetsfrågor har tillräckligt med arbetstid för att utföra sina uppgifter.

6. Arbetsbeskrivningarna för anställda som arbetar med datasäkerhet ska uppdateras med avseende på roller och ansvar.

7. IT-områdena/församlingsenheterna ska ha tillräckligt med yrkeskunnig personal för att det realistiskt sett ska vara möjligt att i praktiken uppfylla säkerhetskraven med beaktande av bl.a. personalens semestrar och annan frånvaro.

8. Tilldelningen av resurser för datasäkerhet beaktas i IT-områdets och församlingsenhetens budget och verksamhets- och ekonomiplan.

Delområdets namn	**1.2 Datasäkerhetspolicy, datasäkerhetsbestämmelser och datasäkerhetsanvisningar**
Mål	Nödvändiga policyer, bestämmelser och anvisningar finns och de hålls uppdaterade och tillgängliga för användarna. Användarna utbildas och informeras regelbundet om nya bestämmelser och anvisningar.
Krav	1. IT-områdena/de ekonomiska församlingsenheterna ska ha en aktuell datasäkerhetspolicy och preciserade bestämmelser och anvisningar som är i linje med de datasäkerhetsbestämmelser som gäller för hela kyrkan. Dokumenten ska alltid finnas tillgängliga för de anställda. 2. Information om gällande datasäkerhetspolicyer, bestämmelser och anvisningar ska ges till hela personalen. Cheferna är skyldiga att förmedla information till sina underordnade. 3. Riskerna i anslutning till datasäkerheten ska utvärderas regelbundet och regelmässigt. Man bör reagera på nya och förändrade risker på ett adekvat sätt. 4. IT-områdena/de ekonomiska församlingsenheterna ska ha välfungerande rutiner för hantering av informationens livscykel. Livscykeln täcker klassificeringen, förvaringen, förmedlingen och förstörandet av information. 5. Information. Regelbunden utbildning i datasäkerhet ordnas för anställda. 6. De anställda ska underteckna en sekretessförbindelse innan arbetet inleds. 7. Volontärer och förtroendevalda som använder församlingens informationssystem eller som i sin uppgift kan komma åt känslig information ska underteckna en sekretessförbindelse. 8. Iakttagandet av datasäkerhetsanvisningarna och datasäkerhetsbestämmelser övervakas och avvikelser åtgärdas. 9. IT-området/församlingsenheten ska låta en utomstående aktör utvärdera[2] nivån på datasäkerheten regelbundet eller i samband med betydande förändringar.

[2] Ledningsgruppen för datasäkerheten inom statsförvaltningen (VAHTI) har utarbetat en omfattande datasäkerhetsordlista (på finska). I detta dokument används begrepp som återfinns i ordlistan och som är etablerade inom dataskyddet. Auditering är en bedömning/testning i syfte att granska till exempel hur dataskyddsmekanismerna fungerar.

	10. IT-området/församlingsenheten har uppdaterade instruktioner om användning av sociala medier.

Delområdets namn	**1.3 Samarbetspartner och hantering av externa tjänster**
Mål	Externa aktörer förutsätts ha samma datasäkerhetsnivå som den som gäller i den egna verksamheten. Datasäkerheten beaktas genast när nya projekt och upphandlingar inleds.
Krav	1. Vid utläggning och upphandling av IT-tjänster ska det förutsättas att externa medarbetare har tillräcklig utbildning och yrkeskunskap. 2. Externa medarbetare ska underteckna en sekretessförbindelse innan arbetet inleds. 3. Externa medarbetare är bundna av samma bestämmelser och anvisningar om datasäkerhet som kyrkans egen personal. Den som anställer en extern medarbetare är skyldig att delge personen i fråga alla relevanta anvisningar. 4. Församlingsenheterna har en utnämnd ansvarsperson för externa aktörer. 5. Nödvändiga datasäkerhetskrav för samarbetspartnerna anges redan i anbudsförfrågan eller avtalsförhandlingarna. 6. Med samarbetspartnerna ordnas tillräckligt ofta möten där man behandlar datasäkerhetsfrågor som t.ex. observerade och inträffade risker samt framtida behov. 7. Ansvarsfrågorna som gäller behandling av personuppgifter ska beaktas i avtal eller i bilagan till avtal med samarbetspartner och utomstående leverantörer då verksamheten uppfyller kännetecknen för personuppgiftsbiträde som definieras i dataskyddsförordningen.

Delområdets namn	**1.4 Verksamhetsprocesser**
Mål	Församlingsenheternas verksamhet är systematisk och repeterbar. I exceptionella situationer reagerar man målmedvetet och förmedlar information mellan IT-områdena.
Krav	1. IT-områdena/församlingsenheterna har välfungerande processer för skötseln av sina IT-funktioner. Processerna ska uppdateras allteftersom situationen förändras. Processerna beaktar datasäkerhetsperspektivet. 2. Församlingsenheterna har en beredskapsplan med en bifogad beredskapsplan för IT-området. Beredskapsplanerna testas regelbundet. 3. De objekt som måste skyddas med tanke på nyckelfunktioner och nyckelprocesser har identifierats och klassificerats. 4. Församlingsenheterna känner till de lagar samt andra föreskrifter och bestämmelser som reglerar deras verksamhet. 5. IT-områdena/församlingsenheterna ska ha fungerande processer för årlig utvärdering och nödvändig uppdatering av datasäkerhetspolicyn och anvisningarna efter behov. 6. IT-områdena/de ekonomiska församlingsenheterna ska ha processer och anvisningar för avvikelser. I dessa tas ställning till hur avvikelser i datasäkerheten observeras, hur man reagerar på dem, hur påföljderna behandlas och hur man återgår till normal verksamhet. 7. Avvikelser i datasäkerheten ska rapporteras och analyseras i efterhand för identifiering av orsakerna till avvikelserna och för vidtagande av ersättande åtgärder. 8. IT-områdenas datasäkerhetsgrupper utbyter information om datasäkerhetsavvikelser och använder sig av andra områdens erfarenheter. Kyrkans datasäkerhetschef svarar för samordningen av verksamheten.

2 Datasäkerhet i datanät

Delområdets namn	**2.1 Användning och utveckling av datanät**
Mål	Datasäkerhetskraven beaktas när datanät planeras och används.
Krav	1. All datakommunikation mellan Kyrknätet[3] och externa nät ska gå via Kyrknätets centraliserade brandvägg. Direkta uppkopplingar till internet eller andra nät får upprättas endast av särskilt vägande skäl. Om direkta förbindelser upprättas (t.ex. administrationsanslutning till en server för en extern aktör) ska denna trafik isoleras från Kyrknätet (t.ex. med hjälp av separata internetanslutningar) och dokumenteras noggrant. 2. IT-områdets datanät ska vara datasäkert och väldokumenterat. IT-området och Kyrkostyrelsen går tillsammans igenom datanätets säkerhet. 3. Ingen annan utrustning än församlingsenhetens/IT-områdets egen utrustning som uppfyller kraven i detta dokument får anslutas till församlingsenheternas Kyrknät. För eventuell besökaranvändning anskaffas en separat internetanslutning där trafiken är isolerad från Kyrknätet. 4. Då trådlösa nät skapas ska de datasäkerhetsrisker som är förknippade med dem beaktas. Identifieringen av terminaler och krypteringen av kommunikationen ska genomföras med certifikat och starka krypteringsalgoritmer enligt rekommendationerna i standarden 802.1x. 5. Åtkomsten till administrationsanvändargränssnitten i den aktiva nätutrustningen ska skyddas med starkt[4] lösenord. 6. Tjänsterna i Kyrknätet kan användas utanför verksamhetsställen som hör till Kyrknätet under följande förutsättningar: a) en säkerhetsregel för användning av dem har skapats i Kyrknätets brandvägg och tjänsten finns i en säkerhetszon som är ämnad för användningsändamålet, b) tjänsten har offentliggjorts via de centraliserade distansarbetstjänsterna i Kyrknätet.

[3] KYRKNÄTET är Evangelisk-lutherska kyrkan i Finlands skyddade intranät till vilket alla församlingsenheters nät är anslutna.

[4] Ett starkt lösenord är minst 10 tecken långt och innehåller minst tre teckentyper (siffror, versaler, gemener och specialtecken), och det är inte ett årtal, datum, ett ord i något språk eller ett namn eller en modifiering av ett ord eller namn.

7. Det är förbjudet att använda kyrkans medlemsdatasystem utanför Kyrknätet. Det är förbjudet att utanför Kyrknätet använda funktionella tillämpningar som har gränssnitt mot medlemsdatasystemet eller i vilka uppgifter om medlemsdatasystemet har lagrats. Fjärranvändning av program kan tillåtas endast om användningen av uppgifter som hämtas via gränssnittsanslutningar till medlemsdatasystemet förhindras. Till exempel genom ett särskilt begränsat gränssnitt där funktioner som utnyttjar dessa uppgifter har tagits ur bruk.

8. Servrar som innehåller medlemsuppgifter eller på vilka medlemsuppgifter behandlas ska finnas inom Finlands gränser och de serverutrymmen där serverutrustningen finns ska minst uppfylla kraven enligt Finansministeriets nivå 3 (VAHTI 2/2013).

9. IT-området ska förse Kyrkostyrelsen med omfattande dokumentation över servermiljön och de servrar där medlemsuppgifter lagras eller på vilka medlemsuppgifter behandlas samt en utvärderingsrapport utförd av en extern aktör som verifierar utrymmenas och miljöernas överensstämmelse med kraven.

3 Datasäkerheten i arbetsstationer och mobila enheter

Delområdets namn	**3.1 Tillämpningar och operativsystem i arbetsstationer**
Mål	Arbetsstationernas operativsystem uppdateras regelbundet. Arbetsstationer med operativsystem som inte längre omfattas av tillverkarens support har tagits ur bruk.
Krav	1. Alla operativsystemversioner som används i församlingsenheternas arbetsstationer och som är anslutna till Kyrknätet ska omfattas av tillverkarens support och vara avsedda för företagsbruk. 2. Arbetsstationerna ska vara utrustade med tidsenliga program med automatisk uppdatering för bekämpning av virus och skadlig programvara samt dessutom ha en brandvägg på programnivå. 3. Säkerhetsuppdatering av operativsystem och program ska installeras i tid i alla arbetsstationer. 4. Funktionen hos programmen i arbetsstationerna kontrolleras efter uppdateringar på testarbetsstationer. 5. Datatrafiken från programmen ska övervakas och avvikande trender ska åtgärdas. [5] 6. Hårddiskar i bärbara Windows-arbetsstationer ska krypteras.

[5] IT-områdenas virtuella brandväggar ger möjlighet att följa datatrafiken från IT-områdets nät till Kyrknätets kärna på programnivå.

Delområdets namn	**3.2 Användning av arbetsstationer**
Mål	Arbetsstationerna används endast av församlingsenhetens anställda för utförande av arbetsuppgifter. Installation av otillåtna och onödiga program förhindras genom begränsade lokala administratörsrättigheter[6].
Krav	1. Församlingsenheternas arbetsstationer (med undantag av utrustning särskilt angiven för annat bruk) får användas endast för utförande av arbetsuppgifter som arbetsgivaren ger. 2. Personliga arbetsstationer får aldrig upplåtas för användning till utomstående, t.ex. familjemedlemmar eller besökare. Arbetsstationens innehavare är själv ansvarig för konsekvenserna av sin oaktsamhet. 3. Det är tillåtet att använda en adekvat skyddad och uppdaterad arbetsstation i offentliga nätverk (t.ex. hotellens gästnätverk och hemnätverk). 4. Det är förbjudet att i arbetsstationer installera andra program (som t.ex. spel) än de som behövs för arbetsuppgifterna. 5. De automatiska inställningarna för att låsa skrivbordet i arbetsstationerna ska tas i bruk. På arbetsstationer för specialbruk (demonstration) kan avvikande inställningar för låsningstid användas. 6. Arbetsstationernas diskresurser och tjänster får inte delas på nätet för användning av annan utrustning eller andra tjänster. 7. När man bär med sig konfidentiella uppgifter ska USB-minnen med krypteringsegenskaper användas. När annan minnesutrustning än arbetsgivarens ansluts till arbetsstationerna ska minnesutrustningens datasäkerhet säkerställas.

[6] Systemets administrationsroll, där de användare som hör till det har omfattande användarrättigheter till målsystemet, servern eller arbetsstationen.

Delområdets namn	**3.3 Administration av arbetsstationer**
Mål	Administrationsrättigheter till arbetsstationerna ges endast till professionella IT-personer. Överenskomna dataskyddsinställningar används i alla arbetsstationer i församlingsenheterna.
Krav	1. Arbetsstationer som ansluts till datanätet ska namnges enligt gemensamma regler så att konflikter med överlappande namn kan undvikas. 2. Datasäkerhets- och webbläsarinställningarna i arbetsstationerna ska göras centraliserat så att användarna inte kan ändra dem. 3. Aktuell dokumentering upprätthålls över program i användning. 4. Endast utsedda IT-personer får ha sådana rättigheter till arbetsstationer som möjliggör installation av program. 5. I arbetsstationerna får inte finnas lokala användarnamn eller grupper som kan användas av de anställda. Rättigheten att använda sådana gäller endast administrativa ändamål. Ett undantag från detta är användarnamn för besökare i datorer i gemensam användning. 6. Eventuell fjärradministration av arbetsstationer ska begränsas så att den kan utföras endast från arbetsstationer eller stödservrar som används av utsedda IT-personer. Fjärruppkoppling till arbetsstationer kan upprättas endast av berättigade, utsedda administratörer. Innehavaren av arbetsstationen ska informeras innan fjärrstödåtgärden vidtas och vid behov ska hans eller hennes samtycke inhämtas i förväg.

Delområdets namn	**3.4 Användning av mobila enheter**
Mål	Grunderna för datasäkerheten i mobila enheter ska säkerställas. Via förkomna eller stulna smarttelefoner, surfplattor eller motsvarande kan uppgifter (e-postmeddelanden, diskutrymme i molntjänster, lokaliseringsdata) hamna i fel händer.
Krav	1. En mobil enhet som ägs av arbetsgivaren får aldrig upplåtas för användning till utomstående, t.ex. familjemedlemmar eller besökare. Innehavaren av enheten är själv ansvarig för konsekvenserna av sin oaktsamhet. 2. Uppdateringar av operativsystem i arbetsgivarens anordningar ska göras i rätt tid. De som använder egna personliga anordningar ska själva se till att anordningarna uppdateras på ändamålsenligt sätt. Ägaren till anordningen står själv för kostnaderna för att åtgärda problem som användningen av anordningen eventuellt orsakar. 3. I mobila enheter som används för att behandla arbetsrelaterad information (till exempel för att läsa tjänsteepost) ska skärmen låsas med pinkod. 4. Det är förbjudet att installera program som inte hör till tillverkarens egen nätbutik (Google Play, Apple App Store osv.) i arbetsgivarens anordningar, med undantag av program som IT-områdena fått tillstånd att installera. Ägaren till personliga anordningar ansvarar själv för att installerade program härstammar från pålitliga källor. Beakta också de rättigheter som programmen kräver i din telefon. Kontrollera då och då de installerade programmens rättigheter i din mobila enhet. De installerade programmens lämplighet för kommersiell användning ska också beaktas när program installeras i en mobil enhet som är avsedd att användas i arbetet. 5. När Bluetooth-uppkoppling används är det viktigt att säkerställa att anordningen inte hela tiden är synlig för alla andra anordningar.

4 Datasäkerheten på servrar

Delområdets namn	**4.1 Tillämpningar och operativsystem på servrar**
Mål	Operativsystemen i servrarna uppdateras regelbundet. Servrar med operativsystem som inte längre stöds av tillverkaren har tagits ur bruk.
Krav	1. De operativsystemversioner som används i IT-områdenas/församlingsenheternas servrar ska omfattas av tillverkarens support. Servrar med eventuella föråldrade operativsystemversioner ska nättekniskt (t.ex. med virtuella nätverk) isoleras från den övriga arbetsstations- och servermiljön. 2. Säkerhetsuppdateringar till servrarnas operativsystem ska installeras på alla servrar enligt följande: kritiska uppdateringar senast inom en månad från att de publicerats och övriga säkerhetsuppdateringar inom två månader. 3. Servrarna ska vara utrustade med moderna program med automatisk uppdatering för bekämpning av virus och skadlig programvara. Alternativt ska det nätsegment där servrarna finns skyddas separat med en brandvägg som kan filtrera bort skadlig programvara från datakommunikationen. 4. Alla servrar med föråldrade operativsystem ska uppdateras eller kopplas bort från nätet.

Delområdets namn	**4.2 Administration av servrar**
Mål	Servrarna har placerats så att tjänstens oavbrutna funktion och servrarnas fysiska säkerhet är garanterade. Servrarnas administrationsanvändarnamn används inte i dagligt bruk av arbetsstationerna.
Krav	1. För att undvika konfliktsituationer på grund av överlappande namn ska servrar som kopplas upp till datanät namnges enligt gemensamma regler. 2. Utsedda IT-personer ska för serveradministrationen ha personliga användarnamn som inte brukas i den dagliga användningen av arbetsstationerna. 3. Servrarna ska placeras i ändamålsenliga låsta apparatutrymmen. Apparatutrymmena ha en fungerande passerkontroll samt kylnings- och brandsläckningssystem efter behov. 4. För kritiska servrar ska en störningsfri strömtillförsel tryggas med hjälp av batterier eller reservströmkällor. 5. Kritiska servrar felsäkras med beaktande av bland annat serverduplicering, belastningsutjämning, reservapparatlösningar och underhållsavtal.

Delområdets namn	**4.3 Säkerhetskopiering och dokumentering**
Mål	Servrarnas funktion dokumenteras heltäckande och säkerhetskopieras regelbundet. Genom dokumentering och säkerhetskopiering blir det enklare att återgå till det normala efter allvarliga fel och att bereda sig på systemförändringar.
Krav	1. Tillräckligt med säkerhetskopior ska regelbundet tas av servrarna. Det ska finnas processer och tydliga anvisningar för återställandet från säkerhetskopior. 2. För varje server utarbetas ett detaljerat serverdokument som innehåller information om serverns läge och användningsändamål, de viktigaste tekniska apparat- och programuppgifterna, datakommunikationsinställningarna, säkerhetsinställningarna, beroendet av andra servrars tjänster och resurser samt utsedda ansvarspersoner och deras kontaktuppgifter. Dokumentationen ska hållas uppdaterad under serverns hela livscykel. 3. Säkerhetskopiornas funktion och täckning ska testas regelbundet. 4. Säkerhetskopior ska förvaras i ett annat brandsäkert utrymme än den server från vilken kopiorna har tagits.

5 Användarrättigheternas datasäkerhet

Delområdets namn	**5.1 Administration av användarrättigheternas livscykel**
Mål	Användarrättigheternas livscykel administreras, nödvändigheten av rättigheter som beviljats användare bedöms regelbundet och onödiga rättigheter tas bort.
Krav	1. Hanteringen av användarrättigheternas livscykel (beställning, ändring, borttagning) ska i regel skötas via kyrkans gemensamma IHA[7]-system. 2. Användarrättigheterna till medlemsdatasystemet Kirjuri administreras endast via IHA-systemet. 3. Chefen är skyldig att till sina underordnade beställa nödvändiga koder och användarrättigheter till informationssystem som församlingen använder och se till att onödiga koder tas bort i tid. 4. För koder och användarrättigheter till volontärer ansvarar personen som är ansvarig för projektet/funktionen. 5. Användarna beviljas endast de rättigheter till systemen som de behöver för att utföra uppgifterna. 6. För att undvika konfliktsituationer med överlappande användarnamn ska domänernas användarnamn skapas efter gemensamma regler. Vid behandlingen av överlappningar tillämpas rekommendationen JHS-161[8]. 7. Församlingsenheterna har fungerande processer för att bedöma nödvändigheten av tidigare beviljade användarrättigheter. Onödiga användarrättigheter tas bort.

[7] IHA-systemet är ett identitetshanteringsprogram som har utvecklats inom Kyrkostyrelsens projekt TYP (Työasemien Yhteiset Palvelut).

[8] JHS-rekommendationerna godkänns av delegationen för informationsförvaltning (JUHTA) inom den offentliga förvaltningen.

Delområdets namn	**5.2 Personliga användarrättigheter**
Mål	Användarnamn och tillhörande lösenord förvaras omsorgsfullt.
Krav	1. Användarnamnen för systemen är personliga. 2. Personliga koder får inte överlåtas till andra. Man får inte ge lösenord som hör ihop med användarnamn till någon annan och inte heller förvara dem nedtecknade på sådana ställen där någon utomstående kan hitta dem. En arbetsstation och program som har startats med de egna koderna får inte lämnas över för att användas av andra. Användaren ansvarar för att det inte sker missbruk med hans eller hennes användarnamn och lösenord. 3. Lösenorden i anslutning till användarnamnen till systemen ska vara tillräckligt starka. Lösenordet ska vara minst 12 tecken långt och innehålla minst tre teckentyper (siffror, versaler, gemener och specialtecken) och det ska inte vara ett årtal, datum, ett ord i något språk eller ett namn eller en modifiering av ett ord eller namn. Församlingsenheten ansvarar för att lösenorden fyller kraven på komplexitet. 4. Lösenorden ska bytas tillräckligt ofta, domänens lösenord var sjätte månad. Lösenordshistoriken ska vara tillräckligt lång för att förhindra att samma lösenord används upprepade gånger. 5. Rättigheter till diskdelning eller disksystem ska inte ges direkt till användarnamn utan de ges till grupper.