Landstinget i Östergötland
Lars Åke Pettersson
Personuppgiftsombud

Gallrings-/bevarandetider för loggar i landstingets IT-system

Loggtyp	Bevarandetider (avser minimitider) Informationsklassning krav på spårbarhet, säkerhetsklass: Höga krav	Normala krav
Händelseloggar (system- och transaktionsloggar) avser fel- och åtgärdshantering för upprätthållande av tillgänglighet till landstingets IT-infrastruktur och applikationer		
• Loggar över systemfel och felmeddelande/larm i IT-infrastrukturen (s k systemlogg)	3 månader	1 månad
• Spårningsloggar för analys av fel (varje aktivitet visas i loggen)	3 månader	1 månad
• Övervakningsloggar (intrångsförsök, virusangrepp etc)	3 månader	1 månad
• Loggar över händelser som rör applikations säkerhet (s k säkerhetslogg)	3 månader	1 månad
• Loggar över systemfel och felmeddelande/larm i applikationer (s k systemlogg)	6 månader	1 månad
• Loggar över genomförd transaktionshantering i applikationer (s k transaktionslogg)	1 år	3 månader
Accessloggar (säkerhetsloggar) avser det bevis landstinget behöver för att säkerställa att missbruk inte skett av IT-resurser eller brott mot sekretess, tystnadsplikt eller dataintrång		
• Loggar över internetaccesser	3 månader	1 månad
• Loggar över e-postaccesser	3 månader	1 månad
• Loggar över in – och utloggningar i AD (lyckade och misslyckade försök)	3 år	1 år
• Loggar över lösenordsbyte i AD eller i HSA-katalogen	3 år	1 år
• Loggar över åtkomst till fysisk utrustning (processorer, minnen/lagringsmedia)	3 år	1 år
• Loggar för åtkomst till patientuppgifter (applikation, operation, info. objekt)	10 år	1 år
• Loggar för åtkomst av administrativa uppgifter (personal, ekonomi etc)	5 år	5 år
• Loggar för vem som tagit del accessloggar	10 år	5 år

Lars Åke Pettersson
Personuppgiftsombud

Gallrings-/bevarandetider för loggar i landstingets IT-system

Utväxlingsloggar (juridiska loggar) avser de bevis som landstinget behöver för att styrka utförda handlingar och mottagna ärenden/meddelanden

• Loggar över avsända meddelanden (s k transaktionslogg)	10 år	1 år
• Loggar över mottagna meddelanden (s k transaktionslogg)	10 år	1 år
• Loggar över ”av mottagaren” kvitterade meddelanden (s k juridisk logg)	10 år	1 år

Särskilda förutsättningar, åtkomst och avsteg

Åtkomst till händelseloggar ges enbart den personal som deltar i systemförvaltningen eller driften av IT-infrastrukturen.

Åtkomst till säkerhets- och utväxlingsloggar sker endast till särskilt förordnade personer och baseras på att ett ärende upprättas och utreds av olika skäl.

Vill någon systemägare göra avsteg från ovanstående krav på bevarandetider för en logg får detta ske först efter samråd med landstingsarkivarien så att ett särskilt gallringsbeslut kan fattas.

BESLUT:
Ovanstående förslag om gallrings-/bevarandetider godkännes.
Enligt uppdrag

Agneta Sundstrand
Landstingsarkivarie

Gallrings-/bevarandetider för loggar i landstingets IT-system

Definitioner – ordförklaringar

Bevarandettid	avser den tid som uppgifter skall **sparas** i ”ursprungligt skick” och som sedan får gallras (förstöras/destrueras) enl. angiven gallringsfrist.
Informationsklassning *classification of data*	klassning av information utifrån systemägarens krav på tillgänglighet, riktighet, insynsskydd och spårbarhet. Systemägaren skall ta ställning (klassa) till vilka krav som skall ställas på systemet i form av säkerhetsklass.
Spårbarhet *traceability*	systemägarens krav på spårbarhet i systemets funktioner. Systemägaren skall ta ställning till vilken säkerhetsklass som skall gälla för spårbarheten på systemet.
Säkerhetsklass spårbarhet	i form av att klassa krav på spårbarheten i systemet, mycket höga krav, höga krav, normala krav eller grundkrav
Höga krav spårbarhet	Om det inte går att härleda utförda aktiviteter och/eller identifiera användare kan detta leda till **mycket allvarlig eller allvarlig skada** för verksamheten eller enskild person. Det skall vara möjligt att spåra vem som gjort vad och när det gjorts. Spårbarheten ska täcka **hela** kedjan i behandlingen.
Normala krav spårbarhet	Det skall vara möjligt att spåra vem som gjort vad och när det gjordes. Annars kan det leda till **lindrig eller försumbar skada** för verksamheten eller enskild person. Spårbarheten ska därför täcka nödvändiga delar av kedjan i behandlingen.
Logg *audit trail*	(kontinuerligt) insamlad information om de operationer som utförs i ett system Registrerade uppgifter kan utnyttjas till att i efterhand analysera vilka operationer som utförts och vilka användare som initierat dessa. Registreringen omfattar som regel tidpunkt, användar**identitet**, berörda **objekt** och övriga **resurs**er samt utförda operationer. Registreringen kan ibland vara så detaljerad att bearbetningen i detalj kan rekonstrueras, men är oftast – av utrymmesskäl – begränsad till att gälla bearbetningens huvuddrag. Jämför **säkerhetslogg** (äldre term: behandlingshistorik).
Loggning	förande av logg

Gallrings-/bevarandetider för loggar i landstingets IT-system

loggning

Systemlogg
system log
System audit trail
registrerade uppgifter om vilka systemadministrativa operationer som utförts, tidpunkten för dessa och vilka operatörer som initierat dessa

Säkerhetslogg
security audit trail
logg över **säkerhetskritiska händelser**.
Säkerhetsloggen kan exempelvis innehålla information om förändringar i behörighetsinformationen och förändringar i datorsystemets konfiguration som är kritiska ur säkerhetssynpunkt. För att säkerhetsloggen skall kunna tjäna sitt syfte är det väsentligt att den ges ett bra skydd mot obehörig påverkan. Se även **säkerhetskritisk händelse**.

Transaktionslogg
transaction audit trail
i kronologisk ordning insamlad information om genomförd transaktionshantering
Transaktionslogg kan syfta till att uppfylla spårbarhetskrav, se **spårbarhet**, men kan även utnyttjas till att återställa det tidigare innehållet i en databas, *"rollback"*, eller – t ex efter en förlust av databasen – utifrån en tidigare **säkerhetskopia** tillsammans med sedan dess genererad transaktionslogg skapa en aktuell korrekt databas, *"roll-forward"*.

Säkerhetskritisk händelse Händelse i ett system som rör säkerheten i systemet. Jämför **säkerhetslogg**.
security event **Se även** driftjournal**.**

Driftjournal
operator log
manuellt förd journal i vilken löpande införs noteringar om förändringar och störningar i driften
Normalt i huvudsak för större system, varvid förs anteckningar om viktigare händelser i systemets drift; ex operatörsbyte, byte eller förändring av systemprogram, in- och urkoppling av yttre förbindelser, olika typer av störningar etc. För varje händelse antecknas tidpunkt, bedömd orsak till störning, vidtagna åtgärder samt vem som vid tillfället var ansvarig operatör.

Utväxlingslogg logg över kvittenser på avsändningsbevis och mottagningsbevis för att kunna bevisa **oavvislighet** för avsända- och mottagna meddelanden.

Oavvislighet
Non-repudiation
princip som tillämpas vid överföring av meddelanden vari dessas avsändande och/eller mottagande ej i efterhand skall kunna förnekas.

Benämnes ibland även ickeförnekbarhet. Se även avsändningsbevis, mottagningsbevis.

Avsändningsbevis
repudiation origin
till ett meddelande fogat ursprungsbevis som styrker avsändarens identitet och det faktum att denne *non-*verkligen avsänt meddelandet.
Avsändaren skall senare inte kunna förneka att han sänt det. Jämför **oavvislighet** och **mottagningsbevis**.

Mottagningsbevis
non-*repudiation delivery*
till ett meddelande relaterat bevis som styrker identiteten hos den som mottagit meddelandet och styrker att meddelandet faktiskt har tagits emot.
Mottagaren skall inte senare kunna förneka att han tagit emot meddelandet. Jämför **oavvislighet** och **avsändningsbevis**.

Behörighetskontroll
authorisation control
administrativa och tekniska åtgärder för kontroll av användares identitet, styrning av användares behörighet att använda systemet och dess resurser samt för registrering av denna användning.
Åtgärderna kan inkludera tillträdeskontroll och administration av behörighetsprofiler. I system med flera **användare** vilka har olika behörighet finns denna funktion som regel inbyggd i systemet (jämför **behörighetskontrollsystem**). Se även **åtkomstkontroll** samt **logg**.

Behörighetskontrollsystem; BKS
access control system
säkerhetsfunktioner som tillsammans utför **behörighetskontroll** i ett system.
BKS omfattar alla erforderliga säkerhetsfunktioner i ett **IT-system**. Säkerhetsfunktionerna skall tillsammans tillse att verksamhetens **säkerhetsregler** (kontinuerligt) uppfylles; som regel ingår som ett minimum följande typer av funktioner:

a) **identifiering** av användaren och **verifiering** av den föregivna identiteten (se identitet samt autenticiering)
b) reglering av **åtkomsträttigheter**
c) registrering av användarens aktiviteter i systemet (se **logg** och **accesslogg**)