LIDINGÖ STAD
Stadsledningskontoret

Lidingö stads it-plattform 2015

(Version 5.2)

Innehållsförteckning

1 INLEDNING

En stabil och driftsäker plattform för it-system är en förutsättning för en framgångsrik it-miljö. Ett väl fungerande it-system är anpassat till verksamhetens processer, stöder användarna i deras arbete och är lätt att anpassa till nya krav. I dessa egenskaper ryms både lämplighet med avseende på funktioner, tillgänglighet och prestanda samt mindre uppenbara egenskaper som exempelvis tillförlitlighet, flexibilitet, skalbarhet och säkerhet. Brister i funktionalitet kan kompenseras i efterhand men det är betydligt svårare att sent i utvecklingen bygga in flexibilitet eller tillförlitlighet. Dessa egenskaper är resultat av tidiga val av konstruktionsprinciper och systemstruktur eller det som brukar omfattas i begreppet ”it-arkitektur”. I en byggnad är arkitekturen till stora delar synlig, det är lätt att studera andras verk eller visa sina byggnader för kunden. It-arkitekturen är däremot osynlig. Strukturen i ett system är svår att genomskåda för användaren.

It-enhetens arbete utgår från verksamhetens behov och önskemål. Beställaren har då en huvudroll i att bidra till att upprätthålla en bra struktur i it-miljön. Liksom ett hus som ska byggas efter vissa standarder för att klara byggnormer så använder även it-organisationer standarder för den tekniska strukturen. Detta kan ibland krocka med beställarens önskemål, men oftast ger det ett bättre slutresultat och högre kvalitet för användaren av systemet. Förutom bättre nytta innebär standardisering även större kostnadseffektivitet och förenklad teknisk administration. It-enheten eller en extern leverantör kan snabbare avhjälpa fel som uppstår och kan i högre grad arbeta i förebyggande syfte och åtgärda fel innan de upptäcks av användaren.

2 SYFTE

Detta dokument har tagits fram i syfte att beskriva stadens it-miljö samt de tekniska kraven och förutsättningarna för drift av verksamheternas it-stöd.

Beskrivningen ska vara vägledande för såväl beslutsfattare, upphandlingsansvariga, systemförvaltare och it-personal som för leverantörer och konsulter vid upphandling, införande, drift och avveckling av it-system.

Innehållet och bilagor ska uppdateras minst vart tredje år. Revidering ska också ske om förändringar i it-miljön inträffat som väsentligt avviker från denna beskrivning.

Kraven i detta dokument ska tillämpas i en omfattning som baseras på syftet med det system som avses och känsligheten, typen och användningen av den information som systemet innehåller.

Vid upphandling av framförallt stadens verksamhetskritiska system ska relevansen av samtliga krav som framgår i detta dokument aktivt bedömas och tas ställning till.

Avsteg från infrastrukturstandarden för ett enskilt system eller tjänst kan negativt påverka driftsituationen för andra systemlösningar och är kostnadsdrivande. Undantag kan enbart beslutas av Stadsledningskontoret.

3 TILLÄMPNING FÖR LEVERANTÖRER VID UPPHANDLING

Leverantören **ska** beskriva det offererade systemet med utgångspunkt från detta dokument inklusive bilagor.

Leverantörens beskrivning utgör underlag för Lidingö stads bedömning av systemets säkerhetslösningar och krav på driftmiljö.

Leverantören **ska** ange i vilka avseenden det offererade systemet ställer avvikande krav på it-miljön eller inte uppfyller säkerhetskraven. Samtliga delar av stadens plattform ska beaktas av leverantören och särskild uppmärksamhet ska ägnas åt rubrikerna avseende Systemdokumentation (10), Säkerhet och kvalitet hos leverantörer (16) samt Infrastrukturstandard (19). I de fall kraven på driftmiljö eller säkerhet kan anses ovidkommande bör detta anges.

Lidingö stad kommer att beräkna kostnader för eventuella anpassningar/förändringar i den befintliga miljön. Dessa kostnader vägs in i utvärderingen av anbudet.

Kostnaderna kan bestå av dels den omedelbara kostnaden för etablering av systemet och dels de långsiktiga totala kostnaderna - för såväl det aktuella systemet som för stadens befintliga system - som kan uppstå vid större eller mindre förändringar i stadens it-miljö eller som följd av eventuella säkerhetsbrister.

I utvärderingen kommer staden att ange vilka kostnader som lagts till vid utvärderingen av priset för anskaffning av systemet.

4 ÖVERGRIPANDE STYRANDE PRINCIPER FÖR DRIFT

Följande styrande principer ska tillämpas som grund i olika ställningstaganden gällande Lidingö stads it-miljö. I de fall förstahandsvalet inte är tillämpligt ska detta motiveras särskilt och dokumenteras. Skäl för avvikelse kan vara ekonomiska, säkerhetsmässiga, miljömässiga, problem med integration eller brist på lämpliga tjänstealternativ.

4.1 VAL AV DRIFTMODELL

1. Användargränssnitt ska i första hand vara webbaserade.
2. Förstahandsvalet för it-funktioner ska vara att köpa funktionen som tjänst (till exempel SaaS eller Moln-baserade tjänster) där drift, backup och delar av administration ingår.
3. I andra hand ska funktionen driftas internt (se 4.2).
4. Undantaget är infrastruktur och tekniska stödsystem som normalt ska driftas internt.

En eventuell ekonomisk vinst att köpa funktion som tjänst måste också balanseras mot ökade krav kring beställarkompetens, integrationer och andra kostnadsdrivande faktorer.

4.2 EGEN DRIFT

I de fall beslut fattas om intern drift med utgångspunkt av vad som anges under 4.1 gäller följande principer

1. Förstahandsvalet vid investering av ny infrastruktur och programvara ska baseras på Microsofts produkter och plattformar.

2. Vid införande av nya plattformar ska särskild hänsyn tas till kostnadsdrivande indirekta faktorer som till exempel uppstår med anledning av skäl som räknas upp under punkt 1.

5 UPPHANDLING OCH INKÖP

Det regelverk som gäller för upphandling generellt gäller även för it. Upphandlingsenheten ska kontaktas med avseende på gällande regler kring upphandlingshantering.

1. I samband med att en upphandling inom it-området sker måste såväl driftaspekter som rådande infrastrukturstandard omfattas. I kravspecifikationen måste det nya systemet täcka nu gällande infrastrukturstandard och även det som beskrivits som framtida standard.

2. It-relaterade krav i upphandlingen ska granskas av it-enheten och godkännas av stadsledningskontoret.

3. Avrop mot gällande avtal inom it-infrastruktur får enbart göras av utanordningsansvariga inom it-enheten, stadsledningskontoret och vissa systemägare. Alla inköp av it-relaterad utrustning och programvara ska ske via eller i samråd med it-enheten och enligt gällande ramavtal.

4. Vid systemupphandling som innehåller information som är föremål för arkivering ska stadsarkivet kontaktas. Detta för att säkerställa att kraven för arkivering tillgodoses.

Se rubrik 16 rörande krav på externa leverantörer.

6 HÄLSA OCH ARBETSMILJÖ

Förbättringar av den it-relaterade arbetsmiljön ska dels bedrivas som en naturlig del i det dagliga arbetet och dels som ett systematiskt arbete där vi regelbundet genomför och följer upp beslutade åtgärder.

Lidingö stads leverantörer av it-utrustning bör inneha certifiering enligt Arbetsmiljöverkets AFS 2009:2.

7 MILJÖPÅVERKAN OCH GRÖN IT

Verksamhetsansvariga ska tillsammans med it-enheten aktivt och långsiktigt verka för miljöanpassning av it-produkter och it-system. Detta innebär att vid varje upphandling av it-produkter om möjligt ställa större miljökrav än vad som föreskrivs i gällande lagar och förordningar samt att också noggrant beakta arbetsmiljöfrågor vid upphandling och införande av it-system.

Grön it är ett begrepp som omfattar kontinuerligt arbete för att minska it-infrastrukturens miljöpåverkan. Följande principer ska följas med avseende på it-relaterade produkter och tjänster inom staden.

Avsteg från dessa principer ska motiveras och dokumenteras särskilt. Lägg märke till att andra styrande dokument (t ex inom miljö och upphandling) kan ställa högre krav än vad som anges här.

7.1 MILJÖPÅVERKAN VID INKÖP OCH UPPHANDLING

1) Alla inköp i staden bör ske enligt miljöstyrningsrådets riktlinjer[1].
2) Leverantörer bör inneha miljöcertifiering enligt SS-EN ISO 14001:2004.
3) Inköp ska ske i så stora volymer som möjligt för att minska miljöpåverkan på grund av transporter.
4) Valda leverantörer bör redovisa hur de aktivt bidrar till att minska miljöpåverkan.
5) Lidingö stad ska ställa krav på emballering, t ex genom att tillämpa riktlinjer från Pappersindustrins miljöråd (PIA), RESU och Svanen-märkning.
6) Energiförbrukning på it-utrustning bör vara ett utvärderingskrav vid upphandling.
7) Miljöpåverkan från förbrukningsmaterial ska vara ett utvärderingskrav vid upphandling.

7.2 MILJÖPÅVERKAN VID FÖRVALTNING OCH AVVECKLING

1) Produktens miljöpåverkan bör ske utifrån produktens hela livscykel där miljöpåverkan under produktion, användning och avveckling vägs in.
2) E-tjänster och möjligheter till digital lagring (t ex scanna till e-post) ska prioriteras för att minska miljöpåverkan via pappershantering och utskrifter.
3) Servermiljön och infrastruktur ska i möjligaste mån virtualiseras för att minska energiförbrukning och miljöpåverkan vid avveckling
4) It-utrustning och förbrukningsmaterial (t ex toners) ska återvinnas och tas om hand på ett miljömässigt sätt. Leverantörer som sköter avveckling av stadens it-utrustning ska kunna redovisa hur de aktivt bidrar till att minska miljöpåverkan.
5) Användning av personliga skrivare ska minimeras för att minska miljöpåverkan.
6) Avveckling av äldre it-utrustning ska ske kontinuerligt också med utgångspunkt från att nyare utrustnings energiförbrukning ständigt förbättras. Hänsyn ska dock tas mot de konsekvenser som uppstår av en ökad omsättning av it-utrustning

8 FÖRVALTNING OCH ÄGANDESKAP AV IT-SYSTEM

För verksamhetskritiska system som används inom Lidingö stad ska stadens förvaltningsmodell tillämpas. Se dokumenten *”Förvaltningsmodell för it-system i Lidingö stad”* och *”Lidingö stads verksamhetskritiska system”*.

9 DRIFTSÄTTNING, FÖRÄNDRING OCH AVVECKLING

9.1 MODELLER

Leverantörer bör tillämpa en vedertagen modell för förvaltning, drift, utveckling och projektarbete. Leverantören bör redovisa vilket arbete som bedrivs för att säkerställa kvalitet och säkerhet under projektarbete och systemutveckling.

9.2 DRIFTSÄTTNING

Innan ett nytt system sätts i drift gäller följande

1) Acceptanstest, t ex via provinstallation, ska vara genomförd.

[1] http://www.kkv.se/nyheter/sammanfattning-av-riktlinjer-for-hallbar-upphandling

2) En fungerande systemförvaltning för systemet ska vara upprättad.
3) Eventuella förändringar i driftmiljön ska vara beslutade och genomförda.
4) Driftkrav, säkerhet, behörighet, systembeskrivning och beroenden till andra system ska vara dokumenterade.

9.3 FÖRÄNDRINGSHANTERING

Innan förändringar av ett system genomförs gäller följande

1) Förändringens omfattning och vem som beslutat ska dokumenteras.
2) Säkerhetskopior av systemet ska göras och en handlingsplan ska upprättas för återställning av systemet till tillståndet före förändringen.
3) Acceptanstest enligt för systemet beskrivna rutiner (testprotokoll) ska genomföras.

9.4 AVVECKLING

Vid ett systems avveckling ska systemägaren tillsammans med stadens arkivarie säkerställa att information arkiveras. Se stadens systemförvaltningsmodell för ytterligare riktlinjer om hur avveckling ska ske.

10 SYSTEMDOKUMENTATION

Systemdokumentationen ska ge en förståelse för systemets uppbyggnad och funktion. Den ska stödja och styra den löpande driften, underlätta underhåll, vidareutveckling och samordning samt underlätta kommunikationen mellan användare, systemförvaltare, leverantörer och driftpersonal. Ett enkelt språk bör genomsyra samtliga beskrivningar för att underlätta kommunikation mellan parterna. Vedertagna begrepp enligt branschpraxis ska eftersträvas för att undvika missförstånd. Dokumentationen bör kontrolleras i syfte att även en part som inte var med i processen kan förstå innehållet för att säkerställa dokumentationens långsiktiga användbarhet.

1) Det åligger leverantören, systemägaren, systemförvaltaren och den driftansvarige gemensamt att upprätta begriplig, tillförlitlig, lättillgänglig och tillräcklig systemdokumentation. Dokumentationen ska uppdateras vid förändringar i systemet

2) All dokumentation ska vara tillgänglig i eller via It-enhetens systemregister.

Dokumentationen består av systemets syfte och användningsområde, teknisk arkitektur, informationsarkitektur, rutinbeskrivningar, finansierings eller licensmodell samt tillhörande avtal och övrig dokumentation.

10.1 SYSTEMBESKRIVNING

Beskriver systemets användningsområde och verksamhetsstöd. Beskrivningen ska omfatta

a. systemets syfte och användningsområde
b. de verksamhetsprocesser systemet stödjer

10.2 INFORMATIONSARKITEKTUR

Beskriver systeminformationens uppbyggnad. Beskrivningen ska omfatta

a. informationsobjekt och relationer mellan dessa
b. in och utdata, bearbetning och presentation
c. programkomponenter och funktionen hos dessa
d. handlingsplan för informationssäkerhet
e. informationssäkerhetsklassning

10.3 TEKNISK ARKITEKTUR

Beskriver systemets tekniska konstruktion samt miljö och driftförutsättningar och ska omfatta

a. i systemet ingående hård- och programvara (server och klient) med krav på
   - processor och minne
   - disk och raidnivå
   - kommunikation (t ex bandbredd, brandväggsinställningar)
   - operativsystem och patchnivå
   - databashanterare och version
b. beroenden och samband med andra system
c. säkerhetslösningar

10.4 RUTINER OCH PROCESSER

Beskriver systemets driftrutiner. Beskrivningen ska omfatta

a. start- och stopprutiner av system och delsystem
b. normala driftåtgärder och vanliga drifttillstånd
b. instruktioner för problemlösning
c. backuprutiner
d. installations och uppgraderingsprocesser
e. plan för återställning efter eventuellt totalt haveri (Katastrofplan/Kontiuitetsplan)
f. kontaktvägar till leverantören vid olika typer av driftsituationer
g. rutiner och funktioner för import och export av data

10.5 LICENSER OCH AVTAL

Beskriver finansiering, licenser och andra avtal. Stadens mallar för avtal bör användas. Beskrivningen ska omfatta

a. Licensmodell med tydlig beskrivning om vad licenserna omfattar och vilken form av licensiering som gäller
b. Finansieringsmodell som beskriver hur betalning för användande av systemet är uppbyggt.
c. Avtal där krav på tillgänglighet, respektive parts ansvar och typ av system/tjänst tydliggörs

11 ARKIVERING OCH GALLRING

Den information som hanteras i stadens it-system utgörs till stor del av allmänna handlingar. Av detta följer att denna ska bevaras, gallras och arkiveras som all annan information enligt bestämmelserna i arkivlagen och myndigheternas dokumenthanteringsplaner. För att tillgodose allmänhetens insynsrätt och forskningens behov kan även sådan information behöva arkiveras för all framtid. Den grundläggande tanken är att endast rådata ur varje system ska bevaras, inte it-systemen i sin helhet.

Nedan följer några riktlinjer för hur detta ska kunna bli möjligt från ett arkiv och gallringsperspektiv.

11.1 SYSTEMUPPHANDLING

Vid upphandling av nya it-system och förändringar av befintliga system ska krav på långtidsarkivering av informationen i systemen beaktas. Möjligheten att göra uttag av rådata ur systemet för arkivering enligt varje myndighets dokumenthanteringsplan ska utredas. Uttagen ska kunna göras i format som är godkända enligt Riksarkivets tekniska krav på elektroniska handlingar[2].

11.2 ANSVARSFÖRDELNING VAD GÄLLER ARKIVERING

Nämnder och kommunala bolag

- levererar digital information till stadsarkivet enligt fastställda riktlinjer.
- tillhandahåller digital information så länge den finns tillgänglig i system eller på myndigheten
- tillgodoser kraven på arkivering vid systemupphandling.

Arkivmyndigheten

- fastställer riktlinjer för digital arkivering
- ger råd och anvisningar om digital arkivering (filformat, lagringsmedia, standarder)
- tar emot digital information för arkivering
- tillgängliggör arkiverad digital information
- bevakar den tekniska utvecklingen inom området

11.3 ARKIVERING OCH GALLRING

För varje system ska arkiverings- och gallringsrutiner fastställas. Rutiner för gallring av dokument, e-postlistor, loggar, cookie- eller andra historik-filer för internetsökning ska följa stadens övergripande dokumenthanteringsplan.

Dessa rutiner utgör också underlag för upprättandet av myndighetens dokumenthanteringsplan samt förteckningen av personuppgifter enligt PUL.

11.4 ARKIVBESTÄNDIGHET

Vid upphandling av skrivare ska hänsyn tas till möjligheten att få arkivbeständiga utskrifter. Skrivare ska vara upptagna i Sveriges Provnings- och forskningsinstituts förteckning över certifierad skrivmateriel.

---

[2] Riksarkivets föreskrifter om elektroniska handlingar http://riksarkivet.se/rafs?item=106

12 EXTERN ÅTKOMST TILL STADENS SYSTEM I UNDERHÅLLSSYFTE

Systemunderhåll ska ske efter överenskommelse med systemförvaltning och it-enheten. Underhållet ska vara aviserat och planerat. Underhåll får endast ske då alla tre parter (systemförvaltning, it-enhetens driftansvarig och leverantören) är informerade och godkänt underhållstillfället.

Åtkomst till system eller tjänster som staden köper upp ska vara tillgängliga med webbaserat interface som nås via en publik internetadress. Tjänsten måste använda sig av en krypterad anslutning via HTTPS om användaruppgifter eller känsliga uppgifter hanteras av systemet och bör även annars göra det.

Undantag kan göras under begränsade perioder med t.ex. VPN-uppkopplingar mot externa system men staden vill hålla sådana länkar till ett minimum. Staden stödjer som lägsta nivå IPSec med AES (128/192/256bit) och autentisering via SHA (384/512).

De möjligheter som staden erbjuder externa leverantörer är i prioriteringsordning följande

1. Fjärrstyrning av klientdator via produkten Teamviewer
2. Direktaccess via ett delat och dedikerat nät (Extranet, DMZ)
3. Lån av Lidingö stad dator samt distansarbetsplatslösning

Driftansvarig på It-enheten ska kontaktas vid varje åtkomsttillfälle för att tilldela extern part åtkomst samt för att medverka i arbetet. Driftansvarig ansvarar också för att arbetet följer regler och riktlinjer för it-användning i staden.

Leverantörens primära kontaktyta gentemot staden är respektive systems systemförvaltare. Systemförvaltaren ansvarar för dialog och planering med driftansvarig på it-enheten.

System inom stadens nät där extern part svarar för driften ska ligga i separat nät, isolerat på ett sådant sätt att stadens driftnät skyddas på jämförbart sätt med skyddet från Internet. Verksamheten ansvarar i dessa fall för hur supportarbetet utförs och att stadens regler och riktlinjer för it-system efterlevs. Särskild leveransöverenskommelse som reglerar roller och ansvar mellan it-enheten och verksamheten ska finnas. Accessen kan vara tillfällig eller permanent och ska ske i första hand genom upprättande av en VPN-tunnel.

Lån av Lidingö stad dator med funktioner för distansarbete bör bara användas i undantagsfall och under mycket begränsad tid. Systemförvaltningen tar ansvar för att dessa användare följer stadens regler och riktlinjer kring it-användning, samt att de har nödvändig kompetens.

Oavsett anslutningsmetod ska alla användare använda sig av individuella konton och lösenord.

13 GENERELLA KRAV PÅ PRESTANDA

För att systemet ska uppnå rimlig användbarhet bör följande generella krav på prestanda iakttas

Tillgänglighet mäts av Lidingö stad vid en anslutningspunkt innanför Lidingö stads brandvägg på en dator där systemet används och som uppfyller systemkraven samt är uppkopplad mot nätverkets centrala delar med minst 10 Mbit/s. Tillgänglighet kan mätas under förutsättning att Internetleverantören levererar fullgod prestanda.

Systemet bör vara dimensionerat för att uppnå följande svarstider.

1. Under 1,5 sekunder från Enter tryckning till svar för minst 90% av normalt arbete i systemets olika moduler.
2. Under 4 sekunder från Enter tryckning till svar för rapportering där kontroll, beräkningar eller databasläsning krävs.
3. Under 10 sekunder från Enter tryckning till svar för rapportering där komplex kontroll, beräkningar eller databasläsning krävs.
4. Under 5 sekunder från Enter tryckning till svar för sammansatta aktiviteter där flera personers uppgifter är inblandade och det sker kontroll, beräkningar eller databasläsning krävs.
5. Under 5 sekunder från Enter tryckning till standardrapport.
6. Ingen garanterad svarstid
    a. I samband med utskrift av rapporter
    b. För rapporter som inte är standardrapporter
    c. För stora beräkningar, t.ex. resursjämförelser
    d. För start av Systemet

14 SYSTEM FÖR TEST

Testsystem används i framförallt två huvudsyften;

1. En utvecklingsmiljö som används innan systemet ska tas i drift. Denna avvecklas normalt i samband med att systemet tas i produktion.
2. En test och eventuell utbildningsmiljö som används parallellt med system som används i produktion

Beställning av system för drift i testmiljö ska göras av systemägaren. I beställningen ska tydligt framgå vad som omfattas och vad syftet är inklusive krav på tillgänglighet, säkerhet och behörighet. Dessa krav ska vara tydligt dokumenterade och överenskomna. Testmiljöer är aldrig att anse som verksamhetskritiska och ska beskrivas utifrån det.

1. Systemägare och driftansvarig ska vara utsedda och systemet ska vara dokumenterat och registrerat på motsvarande sätt som produktionssystem. Om inte detta gjorts följer ansvaret för testsystemet samma modell som för produktionssystemet. Normalt ska även systemförvaltare vara utsedd. Systemförvaltaren är testansvarig. Om inte en systemförvaltare är utsedd är systemägaren testansvarig.

2. Avvecklingsdatum ska vara fastställt innan driftsättning av systemet i testmiljön får ske.

3. Systemet får inte användas ens delvis i produktion.

4. Utvärderingen av testdriften ska dokumenteras av testansvarig

5. System som ska övergå i produktion ska avvecklas från testmiljön och därefter installeras i produktionsmiljön efter beställning från systemägaren.

6. Miljöer uppsatta permanent för kontinuerliga tester av funktioner, nya versioner, utbildning och liknande betraktas som produktionsmiljöer. Tester i sådana miljöer ska likväl hanteras på ovanstående sätt.

15 IT-SÄKERHET

Säkerhetslösningar, rutiner och funktioner i stadens it-system ska säkerställa verksamheternas krav på tillgänglighet, spårbarhet, riktighet och sekretess i enlighet med stadens styrande dokument avseende informationssäkerhet.

15.1 ANSVARSINDELNINGEN RÖRANDE IT-SÄKERHET

1. *Säkerhetschef:* Är överordnat ansvarig för stadens säkerhet.
2. *It-strateg:* Assisterar säkerhetschefen inom IT-området samt ansvarar för informationsäkerhet
3. *Systemägare:* Ansvarar för specificering av säkerhet för sitt system.
4. *Systemförvaltare:* Etablerar och underhåller de säkerhetskrav som ägaren ställer på systemet.
5. *Driftsansvarig:* Upprätthåller säkerhetsnivån preciserad i driftkraven för systemet.
6. *Användare:* Följer säkerhetskraven

15.2 ANVÄNDAR-ID I SYSTEM

1. Användare som kan påverka informationen (lägga till, ändra, ta bort) i stadens it-system ska vara personligt identifierade.

2. Användare som kan ta del av informationen (läsa, kopiera, skriva ut) i stadens it-system bör vara personligt identifierade.

3. Åtkomst till internet via stadens nät ska vara personligt identifierade.

4. Användar-id i verksamhetssystem ska vara detsamma som används i AD för nätåtkomst och genereras med tre till fem tecken tagna ur för och efternamn och vid behov en eller flera mellaninitialer. Alternativt ska användarens e-post adress användas som användarnamn.

5. Personnummer ska användas som nyckel för integration mellan system samt för att säkra personposter.

6. Användar-id för elever genereras med sju tecken bestående av de två sista siffrorna i födelseåret samt fem tecken tagna ur för och efternamn.

7. I externa system med självregistrering bör om möjligt e-postadressen användas som användar-id.

8. Integration av behörighetshantering med stadens gemensamma system för användarbehörigheter (Microsoft Active Directory) ska iakttas och eftersträvas.

9. Kontakta Krav på informationssystem som innehåller

15.3 INFORMATIONSSYSTEM MED SKYDDADE PERSONUPPGIFTER

Kontakta stadens PUL ombud vad gäller krav på informationssystem som innehåller skyddade personuppgifter eller krav på sekretess. Grunden för denna hantering utgörs av Skatteverkets vägledning för hantering av sekretessmarkerade personuppgifter enligt följande;

1. Ansvaret för att informera om skyddade personuppgifter ligger på den enskilde själv
2. Skyddade uppgifter ska sekretessmarkeras
3. Rutiner för att hantera sekretessmarkerade uppgifter ska finnas
4. Hanteringen av sekretessmarkerade uppgifter ska beaktas vid utveckling av it-stöd. Det bör finnas en tydlig markering som visas på skärmen och markeringarna bör se likadana i alla system
5. Sekretessmarkerade uppgifter får inte flyttas till system som saknar funktioner och rutiner för sekretessmarkering
6. Behörighet till sekretessmarkerade uppgifter ska tilldelas restriktivt och särskilt motiveras
7. Loggning av vem som tagit del av uppgifterna bör finnas
8. Sekretessmarkerade uppgifter får inte sändas med e-post
9. Personal som hanterar sekretessmarkerade personuppgifter ska ha kunskap om rutiner, regler och riktlinjer för detta

15.4 LÖSENORD OCH LÖSENORDSHANTERING

1. System bör vara uppsatta så att krav på lösenordsbyte sker minst var 180:e dag.
2. System ska stödja påtvingat lösenordsbyte med för systemadministratören valfritt intervall. Detta för att användare lättare ska kunna synkronisera sina lösenordsbyten.
3. Lösenord bör vara minst 8 tecken, varav krav på små och stora tecken samt kombination med siffror är att föredra.
4. System bör stödja påtvingat lösenordsbyte vid första inloggningen.
5. Vid användning av Single-Sign-On (SSO) lösningar ska autentisering ske mot stadens Microsoft Active Directory (AD).
6. Vid delgivning av nytt lösenord ska detta ske efter identifiering och i följande prioritetsordning;
    a. Via stadens tjänst för lösenordsbyte (SelfService)
    b. Direkt till personen i fråga muntligen eller via e-post
    c. Till närmaste chef muntligen eller via e-post
7. Där identifiering av användare kan ske via tvåfaktorsinloggning ska en pinkod baserad på fyra tecken användas. I dessa fall behöver inte heller lösenord bytas regelbundet.

15.5 STARK AUTENTICERING

Utifrån bland annat informationssäkerhetsklassning av system kan krav på två-faktors autenticering föreligga. Lidingö stad stöder autenticering via två-faktor enligt följande principer;

1. SAMLv2 ska användas för attributhantering
2. Inloggningsförfarandens som stöds är
    a. Användarnamn ochLösenord i kombination med SMS
    b. BankID
    c. Mobilt BankID

15.6 ANSLUTNING AV DATORER TILL STADENS NÄT

Stadens it-utrustning som också används i andra nät får anslutas på följande villkor.

1. It-utrustningen ska anslutas till stadens nät minst två gånger per månad för uppdatering av virusskydd och annan säkerhetsrelaterad programvara.
2. Brandväggen ska vara aktiverad.

3. För webbåtkomst ska stadens proxy användas.
4. DHCP ska användas

Till stadens trådlösa nät får också privata datorer och annan utrustning anslutas. Användare ska göras uppmärksamma på följande villkor.

1. Anslutning sker endast via stadens publika nät (öppet nät).
2. Den lokala brandväggen bör vara aktiverad.
3. Uppdaterat och aktivt virusskydd ska finnas.
4. Lidingö stad tar inte ansvar om datorn utsätts för intrång eller skada på grund av virus.
5. Staden lämnar inte någon form av support på privata datorer.

15.7 BACKUP RUTINER

1. Säkerhetskopia av information i verksamhetssystem eller dokument som lagras på grupp- eller hemkataloger sparas i 180 dagar.
2. Säkerhetskopiering görs varje natt av all data lagrad på centrala gemensamma system.
3. För backup av data användaren lagrat på lokala diskar på datorn, eller andra icke nätverksanslutna system, svarar användaren eller systemförvaltaren.
4. Backupband med säkerhetkopior äldre än en månad ska lagras i brandsäkert skåp och i brandrisk- och stöldhänseende väl åtskilda från servrar med originaldata. Full backup ska tas minst en gång per vecka och inkrementell backup dagligen.

15.8 STRÖMFÖRSÖRJNING, BRANDSKYDD OCH KYLSYSTEM

1. Servrar och central kommunikationsutrustning ska strömförsörjas med avbrottsfri kraft (UPS).
2. Servrar med verksamhetsdata ska stå i brandskyddade serverhallar.
3. Temperaturen i serverhallar ska regleras med kylsystem och får inte överstiga 25 grader under längre period än 24 timmar och 30 grader under max 4 timmar. Driftsättning av nödkyla eller stängning av systemen är därefter ett krav. Plan för prioritetsordning för eventuell nödstängning ska finnas.

16 SÄKERHET OCH KVALITET HOS LEVERANTÖRER

16.1 INFORMATIONSSÄKERHET

16.1.1 ANVÄNDNING AV UNDERLEVERANTÖR FÖR DRIFT OCH UTVECKLING AV SYSTEM

Leverantörer ska redovisa om underleverantör används samt om avtal med underleverantör omfattar informationssäkerhet.

I det fall Leverantörer nyttjar underleverantör för utveckling bör ett samarbetsavtal som reglerar både affärsmässighet och säkerhet finnas. Följande punkter bör beaktas avseende informationssäkerhet:

1. hur de rättsliga kraven ska uppfyllas, exempelvis rörande lagstiftning för sekretess och personuppgifter,

2. vilka åtgärder som ska vidtas för att säkerställa att alla berörda parter, inklusive underleverantörer, är medvetna om sitt säkerhetsansvar, licensieringsarrangemang, äganderätt till koden och upphovsrätt,

3. säkerställande av utfört arbetes kvalitet och noggrannhet; depositionsarrangemang för programkod om inte underleverantör kan fullgöra sin uppgift.

Leverantörer bör redovisa hur säkerhet beaktats i avtalsrelationen, exempelvis avseende hantering av personuppgifter.

16.1.2 STANDARD FÖR INFORMATIONSSÄKERHET

Leverantörer bör följa ISO/IEC 27001, ISO/IEC 17799 eller motsvarande för ledning av arbete med informationssäkerhet. Leverantörer ska kunna redogöra för hur arbete med informationssäkerhet och IT-säkerhet bedrivs i verksamheten.

16.1.3 KVALITETSSÄKRING AV SYSTEM

Leverantören bör kunna redovisa vilka aktiviteter som utförs för att löpande hantera vanligt förekommande säkerhetsbrister.

16.2 EFTERLEVNAD OCH KONTROLL

16.2.1 SÄKERHETSTESTNING AV APPLIKATION OCH SYSTEMKOMPONENTER

Lidingö stad kan komma att utföra kvalitets och säkerhetsrevisioner av systemet/tjänsten. Säkerhetstesterna kan komma att utföras med hjälp av tredje part anlitad av Lidingö stad. Leverantörer ska godkänna att dessa tester genomförs samt bistå Lidingö stad och eventuell tredje part med den information och resurser som krävs för genomförandet.

Om det efterfrågade systemet eller tjänsten genomgår, eller har tidigare genomgått säkerhetstestning av tredje part bör leverantören tillhandahålla resultaten av dessa säkerhetstester, information om hur testerna genomfördes, omfattning av testerna samt vem som var utförare.

16.2.2 REVISIONER

Leverantörer bör möjliggöra att Lidingö stad på egen hand eller med hjälp av revisor eller annan person/er granskar Leverantörens tillhandahållande av tjänsten. Leverantören ska lämna skäligt biträde, inklusive tillgång till Leverantörens lokaler där tjänsten levereras i syfte att kontroller att tjänsten utförs enligt Leverantörens gällande säkerhetsföreskrifter. Granskning får också omfatta riktigheten i Leverantörens debiteringar och att tjänsten levereras i enlighet med avtal. Leverantören har rätt att närvara vid revisionen, vilken ska utföras under normal arbetstid.

16.2.3 ÅTGÄRD AV SÄKERHETSBRISTER

Leverantörer ska inom skälig tid åtgärda säkerhetsbrister som Lidingö stad identifierar i samband med revision eller acceptanstest. Skälig tid ska ställas i relation till säkerhetsbristens omfattning, risk och konsekvens.

Säkerhetsbrister som kan orsaka skada för tredje part (t ex medborgare eller företag) ska åtgärdas omedelbart. Likaså ska brister åtgärdas omedelbart som inte är i enlighet med gällande lagstiftning, kan ha en omfattande påverkan på Lidingö stads anseende eller leder till omfattande indirekta kostnader för Lidingö stad. Leverantörens åtgärdsarbete ska inte medföra merkostnader för Lidingö stad.

Leverantörer ska redovisa för Lidingö stad genomförda åtgärder av säkerhetsbrister och sårbarheter som identifierats vid säkerhetstester eller revisioner.

16.3 INDATAVALIDERING, SESSIONSHANTERING

16.3.1 INFORMATIONSLÄCKAGE

Vid fel bör systemkomponenter eller applikationer ej lämna detaljerade felmeddelanden som kan användas för att kartlägga systemets uppbyggnad eller ingående komponenter.

16.3.2 SESSIONSIDENTITETER

Sessionsidentiteter för användare anslutning till system och applikationer bör genereras på ett sätt så att det inte är möjligt att enkelt och olovligen rekonstruera eller utnyttja giltiga sessionsidentiteter.

16.4 ÅTKOMSTSTYRNING OCH BEHÖRIGHETSHANTERING

16.4.1 LAGRING AV BEHÖRIGHETSINFORMATION

Känslig information som till exempel lösenord ska lagras på ett sätt som skyddar dem mot obehörig användning.

16.4.2 BEHÖRIGHETSSYSTEM

Behörighetssystem bör tillåta att behörigheter kan tilldelas både på grupp, roll och individnivå.

16.4.3 ANVÄNDARIDENTITETER

Användare och administratörer ska kunna tilldelas unika användaridentiteter. Integration av behörighetshantering med stadens gemensamma system för användarbehörigheter (Microsoft Active Directory) ska iakttas och eftersträvas. Användar-id i verksamhetssystem ska vara detsamma som används i AD för nätåtkomst och genereras med tre till fem tecken tagna ur för och efternamn, användar-id för elever genereras med sju tecken bestående av de två sista siffrorna i födelseåret samt fem tecken tagna ur för och efternamn. I externa system med självregistrering bör om möjligt e-postadressen användas som användar-id.

16.4.4 LÖSENORDSSKYDD

Åtkomst till system som ställer krav på reglerad åtkomst till information i systemet ska kunna skyddas med lösenord eller motsvarande. Detta gäller såväl för behöriga användare som administratörer. Utifrån informationsinnehållet bör systemet stödja två-faktorsinloggning och SAMLv2 för de användare som ska komma åt informationen.

16.4.5 KONTROLL AV LÖSENORDSKVALITET

Där lösenord tillämpas för åtkomstskydd bör kontroller av lösenordskvalitet finnas. Kontroller för lösenordskvalitet bör medge möjlighet att specificera minimilängd för lösenord, intervall för återanvändning av lösenord samt komplexitetskrav. Dessa kontroller bör standardmässigt vara aktiverade. Lidingö stad bör ha möjlighet att ange vilken policy som ska gälla för lösenord och lösenordskontroller. Om inte annat överenskommits gäller de villkor som anges under rubrik 15.4.

16.4.6 BEHÖRIGHETER FÖR INTERNA SYSTEMKONTON

Behörigheter för interna systemkonton bör vara utformade enligt principen där minsta möjliga behörighet tilldelas. Med systemkonton avses behörigheter som används vid kommunikation mellan interna systemkomponenter, exempelvis mellan applikation och databas.

16.4.7 TILLDELNING AV ANVÄNDARBEHÖRIGHETER

Användarbehörigheter bör tilldelas enligt principen där minsta möjliga behörighet tilldelas.

16.4.8 STYRNING AV ÅTKOMST TILL FUNKTIONER

De delar av applikationer som skyddas av behörighets- eller åtkomstkontroller bör ej vara direkt adresserbara för obehöriga användare.

16.4.9 RENSNING AV BEHÖRIGHETS- OCH SESSIONSINFORMATION

Behörighetsinformation som lagras i temporära filer i användarens arbetsstation bör vara skyddad mot avläsning. Informationen får ej lagras i klartext.

Vid utloggning bör samtliga behörighets- och sessionsinformation som lagras i temporära filer i användarens dator rensas.

16.4.10 KOMMUNIKATION AV BEHÖRIGHETSINFORMATION

Behörighetsinformation bör ej sändas i klartext mellan användarens arbetsstation och applikationsserver. De kommunikationskanaler som används för behörighetsinformation bör vara skyddade mot insyn med exempelvis kryptering.

16.4.11 SKYDD AV ADMINISTRATIVA GRÄNSSNITT

Samtliga administrativa gränssnitt för system och tjänster, såväl gränssnitt som används av Lidingö stads personal som leverantörers personal, ska skyddas. Leverantörer ska kunna redovisa vilka administrationsgränssnitt som finns samt hur dessa skyddas.

16.4.12 NÄTVERKSMÄSSIG ÅTKOMSTKONTROLL

Mekanismer för styrning av nätverksmässig åtkomst, exempelvis brandväggar, ska finnas aktiverade som skydd för komponenter som hanterar system, applikationer eller tjänster som används av Lidingö stad.

Operativsystemets inbyggda brandvägg bör kunna vara aktiverad för såväl arbetsstationer som serversystem.

Uppgift om vilken nätverkstrafik som krävs för både in och utgående trafik ska finnas.

16.5 INCIDENTHANTERING

16.5.1 RAPPORTERING OCH UTVÄRDERING AV SÄKERHETSINCIDENTER

Leverantörer ska ha tydliga och dokumenterade rutiner för hantering, utvärdering och uppföljning av säkerhetsrelaterade incidenter.

16.5.2 RAPPORTERING AV SÄKERHETSINCIDENTER

Leverantörer ska omgående rapportera alla säkerhetsincidenter till Lidingö stad. Detta omfattar incidenter i miljö och system där Leverantören hanterar Lidingö stads system och tjänster samt närliggande driftmiljö där en incident kan påverka Lidingö stads informationssäkerhet.

16.5.3 LAGKRAV

Det bör finnas dokumenterade rutiner för hantering av incidenter som kan leda till rättsliga efterspel. Rutinerna ska omfatta säkerställande av bevismaterial. Leverantörer ska kunna redogöra dessa rutiner.

16.6 LOGGNING OCH ÖVERVAKNING

16.6.1 LOGGNINGSFUNKTIONER

Loggningsfunktioner och historik bör finnas för användares in- och utloggningar i applikationer och system samt även felaktiga/misslyckade inloggningar och övriga säkerhetsrelaterade händelser. Dessa loggar bör vara skyddade för obehörig manipulering. Loggning ska vara maximalt aktiverad om inga väsentliga prestandamässiga hinder finns.

16.6.2 ÖVERVAKNING

Övervakning av säkerhetsrelaterade händelser ska vara möjlig i system och tjänster som innehåller känslig information. Övervakningsrutiner ska medge att statistik kan sammanställas och redovisas för Lidingö stad.

16.7 SÄKERHET I DRIFTMILJÖ

16.7.1 SKYDD MOT SKADLIG PROGRAMKOD

Samtliga komponenter i driftmiljön ska ha skydd mot skadlig programkod/virus. Rutiner ska finnas för rensning/återställning av systemmiljön efter ett angrepp av skadlig programkod. Rutiner ska finnas för kontinuerlig uppdatering av virusskydd. Leverantörer bör redovisa vilket skydd som finns mot skadlig programkod/virus för de plattformar som kommer att utgöra det efterfrågade systemet eller tjänsten.

16.7.2 ANVÄNDNING AV LÖSENORD

Rutiner ska finnas för hantering av behörigheter, exempelvis lösenord. Rutinerna ska regelbundet följas upp.

16.7.3 SEPARATION AV KUNDINFORMATION

I det fall Lidingö stads information ska hanteras i system där andra organisationer/företags information hanteras ska kontroller finnas för att säkerställa separation av informationen. Leverantörer bör redogöra för hur separation säkerställs.

16.7.4 HANTERING AV SÄKERHETSUPPDATERINGAR

Leverantörer ska redogöra för ansvar, riskhantering och rutiner som säkerställer att driftmiljö uppdateras för att minimera riskerna samt även hur samspelet med Lidingö stad i dessa frågor kommer att hanteras.

16.7.5 TEST- OCH UTVECKLINGSDATA I PRODUKTIONSMILJÖ

Dokumenterade rutiner ska tillämpas för att styra överföring från utveckling och test till produktion samt säkerställa att information och programversioner inte blandas.

16.8 FYSISK SÄKERHET

16.8.1 FYSISK SÄKERHET OCH SKYDD AV LOKALER

Servrar med verksamhetsdata ska stå i brandskyddade serverhallar. Skalskydd ska finnas för att skydda utrymmen där den systemmiljö som hanterar Lidingö stads IT-system och tjänster är fysiskt placerad. Vid utformning av skydd mot externa och miljörelaterade hot ska hänsyn tas till omgivningarna i närheten av lokalerna. Leverantörer ska redogöra för ansvar och rutiner samt hur fysiskt skalskydd är utformat.

16.8.2 ÅTKOMST TILL UTRYMMEN

Endast behörig personal ska ha tillträde till de utrymmen där systemmiljöer som hanterar Lidingö stads IT-system och tjänster är fysiskt placerade. Leverantören ska på begäran kunna redogöra för vilka som har tillträde till dessa utrymmen.

16.8.3 ELFÖRSÖRJNING, KYLA

Servrar och central kommunikationsutrustning ska strömförsörjas med avbrottsfri kraft (UPS). Temperaturen i serverhallar ska regleras med kylsystem och får inte överstiga 25 grader under längre period än 24 timmar och 30 grader under max 4 timmar. Driftsättning av nödkyla eller stängning av systemen är därefter ett krav. Plan för prioritetsordning för eventuell nödstängning ska finnas.

16.9 KONTINUITETSPLANERING OCH SÄKERHETSKOPIERING

16.9.1 KONTINUITETSPLANERING

Kontinuitetsplaner ska finnas för att Lidingö stads verksamhet i IT-system kan återupptas inom erforderlig tid efter ett avbrott eller fel i kritiska rutiner. Dessa planer ska vara dokumenterade, kommunicerade och testade. Leverantörer bör redogöra för ansvar och rutiner för att säkerställa att Lidingö stads verksamhet kan återupptas enligt avtalade tillgänglighetskrav.

16.9.2 RUTINER FÖR SÄKERHETSKOPIERING

Säkerhetskopiering ska utföras. Arbetet med säkerhetskopiering ska utgå från dokumenterade rutiner. Säkerhetskopia ska sparas i 180 dagar inte annat överenskommes. Leverantörer ska redovisa hur säkerhetskopiering kommer att hanteras, hur rutiner är utformade samt hur de tillämpas på alla efterfrågade system och tjänster.

16.9.3 FÖRVARING AV BACKUPMEDIA

Säkerhetskopior ska förvaras väl åtskilt från produktionsmiljö och på ett sådant sätt att det ej påverkas av katastrof som drabbar ordinarie produktionsplats.

16.9.4 ÅTERLÄSNINGSTESTER OCH ÅTERSTÄLLNINGSTESTER

Återläsnings- och återställningstester ska genomföras som kontrollerar datakvalitet på säkerhetskopior och att återställning kan utföras i enlighet med avtalade tillgänglighetskrav. Tester ska utföras minst årligen. Resultatet av tester som utförs av Leverantörer ska på begäran redovisas för Lidingö stad.

16.10 PRINCIPER FÖR NAMNGIVNING AV ORGANISATION I IT-SYSTEM

Syftet med en enhetlig och konsekvent namnstandard är att it-system med automatik ska kunna bestämma en användares organisatoriska tillhörighet. Till exempel behöver intranätet identifiera användares grupptillhörighet för personalisering av hemsidan.

Organisationen ska namnges i följande form:

Nivå1/Nivå2/...../NivåX

1. En organisationsenhet ska tillhöra och ingå i enheten på överliggande nivå
2. Antal nivåer är valfritt

3. Nivåerna bör separeras med antingen ”/” (slash) eller ”.” (punkt)
4. Nivå1 är den högsta nivån och ska vara förvaltningsnamn eller motsvarande
5. NivåX är den lägsta nivån och utgörs av organisationsenheten där första linjens chef finns
6. Eventuella nivåer lägre än NivåX utelämnas
7. Namnen ska vara korta och beskrivande och får endast innehålla alfanumeriska tecken samt tecknet & (dvs A-Ö, a-ö, 0-9, &)

Exempel
Uf.Förskola.Tuppen
Uf.Grundskola. Högsätra skola 6-9
Osf.Utföraravdelningen.OSS.Ögruppen1

17 LAGRING AV DOKUMENT, FILER OCH DATA

Användardata bör lagras på personliga hemkataloger eller gemensamma gruppkataloger. Verksamhetskritiska dokument data ska lagras på gemensamma lagringsutrymmen.

1. Endast användaren är behörig till data i personlig hemkatalog
2. Behörighet till gruppkataloger beslutas av ägaren
3. Om särskilda krav föreligger kring tillgång till enskilds e-post eller lagrade dokument ska detta godkännas skriftligt av förvaltningschef och stadens personalchef innan så sker.

18 FILFORMAT

1. Väletablerade filformat för datalagring bör användas och väljas med hänsyn till läsbarhet under lång tid och vara oberoende av viss leverantör eller programvara.
2. System bör innehålla funktioner för export av data till standardiserat filformat både med hänsyn till behovet av arkivering och eventuellt byte av system eller integration med andra system.
3. Databaser bör vara beskrivna så att export av data till andra system kan ske på enklast möjliga sätt.
4. I systemdokumentation ska tydligt framgå vilka filformat systemet använder.

19 INFRASTRUKTURSTANDARD

Beslut om förändringar i standardplattformen kan endast göras av stadsledningskontoret. Gällande standard är beskriven men uppdateringar och uppgraderingar är något som görs kontinuerligt

Vid en upphandling av nytt system gäller följande:

1) Nulägesstandarden bör omfattas.
2) Framtida standard bör stödjas.
3) Standard under avveckling bör uteslutas.
4) KSL:s principer från 2013 kring säkerhet och samverkan beskrivna i bilaga 1 ska efterlevas.
5) Avvikelser från dessa standarder ska redovisas och kostnadsberäknas av it-enheten samt utgöra en del av den ekonomiska bedömningen av systemet.

19.1 KOMMUNIKATION

Kommunikationen är baserad på Ethernet och TCP/IP-v4 i fiberstamnät med 1000 Mbps och i spridningsnät 100 Mbps. Samtliga större anläggningar med 10 eller fler användare har fiberkommunikation och ingen förbindelse är under 10 Mbps.

Två brandväggar skiljer Internet från Lidingös lokala nätverk. Användare mot Internet använder en och samma ip-adress (NAT). Användare på Internet får full nåtåtkomst via VPN. Vissa system är undantagna från access via VPN.

Lidingö Stad förbehåller sig rätten att i brandväggen bryta krypterade kommunikationsströmmar för inspektion.

I nuläget finns tre användarnät, administrativt, pedagogiskt och publikt nät som ansluter mot Internet på tre olika ip-adresser. Det finns även tre servernät och tre systemspecifika nät för olika driftjänster (tex fastighetsövervakning och teknisk övervakning).

Trådlös krypterad kommunikation för bärbara pc är spritt över stadens verksamheter.

1) Till stadens nät får endast anslutas utrustning och system som uppfyller kraven i detta dokument samt är godkänd och upphandlad via it-enheten

2) Vid anslutning till verksamhetssystem från internet/öppna nät ska säker krypterad kommunikation (motsvarande HTTPS) användas.

3) Systemägaren beslutar om från vilket eller vilka nät ett system ska vara åtkomligt. Om beslutet påverkar andra system avgör påverkade systems ägare gemensamt.

4) Generella säkerhetsnivåer för åtkomst beslutas av stadsledningskontoret.

19.2 E-POST

1. E-postadresser ska ha formatet *fornamn.[mellaninitial].efternamn@lidingo.se*
2. Åtkomst till e-post från oskyddade nät ska ske via https
3. Maximal storlek på inkommande e-postmeddelanden är 100 MB. Maximal på utgående e-postmeddelanden är 100 MB. För användare av Office365 är begränsningen 25 MB. Normal extern standard är 25 MB vilket givetvis också påverkar vad vi kan skicka.
4. Varje användarkonto förfogar som standard 1 GB lagringsutrymme.

19.3 SERVERPLATTFORMEN

Plattformen för serverdrift är baserad på Microsoftprodukter med Active Directory som katalogtjänst och Windows Server som operativsystem. En miljö för virtuell serverdrift baserad på VMware utgör basplattformen och förstahandsvalet för all serverdrift. Nya system bör om inga särskilda skäl finns vara anpassade för virtuell serverdrift.

Som databashanterare bör i första hand MS SQL Server väljas. Andra databashanterare får användas endast om synnerliga skäl finns.

Delsystem	Standard nuläge	Framtid

	Lägst	*Högst*	
Operativsystem			
VMware vSphere 5	5.5		
Microsoft Windows Server	2008R2	-	
Microsoft IIS webserver	7.5		
Apache webserver	2.0	-	
PHP	5	-	
Net.Framework	3.0		
Virtuell server			
Processor XEON E5530	1 st		
Minne	1 GB		
Disk	20 GB		
Fysisk server			Avvecklas

19.3.1 DATABASHANTERARE

Programnamn	**Standard nuläge**		**Framtid**
	Lägsta	***Högsta***	
Microsoft SQL Server	2008R2		
Oracle	10.g		Avvecklas

19.4 PC HÅRDVARA

Klientmiljön är standardiserad kring ett så fåtal olika modeller som möjligt. Kringutrustning ska vara godkänd av it-enheten.

Hårdvara stationär PC	**Standard nuläge**		**Framtid**
	Lägst	***Högst***	
Processor	2,33 GHz dualcore	-	-
Minne	4GB	-	-
Disk	80 GB	-	-
Bildskärm	22” CRT	-	-
Nätverkskort trådbundet	1000 Mbps	-	-
USB	2 st USB2.0	-	-

Hårdvara bärbar PC	**Standard nuläge**		**Framtid**
	Lägst	***Högst***	
Processor	2,33 GHz dualcore	-	-
Minne	2GB	-	-
Disk	120 GB	-	-
Bildskärm	12”	-	-
Nätverkskort trådbundet	1000 Mbps	-	-
Nätverkskort trådlöst	802.11g	-	-
USB	2 st USB2.0	-	-

Mobila enheter	**Standard nuläge**	**Framtid**

	Lägst	***Högst (2015)***	
Smartphone iOS	iPhone 5	-	
Smartphone Android	Samsung Galaxy S	-	
Smartphone Microsoft	-	-	
Surfplatta iOS	iPad	-	
Surfplatta Android	Samsung Galaxy Tab 10	-	

19.5 UTSKRIFTSYSTEM

Skrivare kan vara direkt- eller nätanslutna. För nätanslutna skrivare används Microsoft Printservices och drivrutiner distribueras automatisk. Behörigheter till skrivare och utskriftsköer hanteras i AD. Standarden bygger på skrivare från HP, Lexmark och Canon.

Användning av nätanslutna skrivare ska prioriteras.

19.6 OPERATIVSYSTEM OCH PROGRAMVAROR

1. Virusskydd ska finnas på samtliga pc och ska uppdateras senast en vecka efter att uppdateringar är tillgängliga.
2. Windows inbyggda brandvägg bör vara aktiverad. Uppgift om portar bör därför finnas för all klientprogramvara.
3. Distributionen av programvaror sker genom Microsoft SCCM. Applikationerna är MSI-paketerade eller MSI-”wrappade”. Som MSI-paketeringsverktyg nyttjas Wise Package Studio. Rutiner för all installation av programvara tas fram av it-enheten.
4. Programvaror som inte längre stöds av leverantören ska avvecklas snarast möjligt.
5. Nya applikationer ska levereras MSI-paketerade med möjlighet till anpassning (MST) eller med dokumenterad möjlighet till ”MSI-wrappning”.
6. Program ska av slutanvändaren kunna köras med operativsystemets grundläggande användarbehörigheter ("user").

Klientprogramvaran indelas i följande kategorier:

1) *Operativsystem:* Operativsystem med servicepaket och säkerhetsuppdateringar.
2) *Grundfunktioner:* Komponenter som ingår i operativsystemet men med separat versionshantering.
3) *Nätberoende:* Programvara som är beroende av nätoperativsystemet.
4) *Standardapplikationer:* Applikationer som finns på samtliga pc
5) *Tilläggsapplikationer:* Valbar programvara för standardfunktioner.
6) *Databasklienter:* Klientprogramvara för databasåtkomst.

Kategori	**Programnamn**	**Standard nuläge**		**Standard framtid**
		Lägsta	*Högsta*	
Operativsystem	Windows 7 32-bitars	SP1		
	Windows 7 64-bitars	SP1		

Grundfunktion	Internet Explorer	9.0	11.0	
	Microsoft NET Framework	4.5		
Standardappl.	System Center Endpoint Protection	4.7		
	Microsoft Office 2010	SP2		Office 2013 pro plus/ Office 365
	Adobe Acrobat Reader	11.0		
	Quicktime	7.7.1		
	Adobe Flash Player	autouppdateras		
	Java Runtime	7.51		
Bastilläggappl.	Adobe Acrobat Standard	10.0		
	Adobe Acrobat Pro	10.0		
	Citrix Web Client	12.1		
Databasklient	Oracle	10		
	Microsoft Access 2002 Runtime			Avvecklas

20 NYCKELTAL FÖR LIDINGÖ STADS IT-MILJÖ

Användare		
	Administrativ personal	1900
	Pedagogisk personal	1300
	Elever	5600
	Summa	*8800*
PC		
	För administrativt bruk	920
	För administrativt bruk i pedagogisk verksamhet	920
	För elever	1300
	För allmänheten	50
	Summa	*3190*
Servrar		
	Fysiska	10
	Virtuella	90
System		
	Färre än 10 användare	250

	10- 100 användare	150
	100 – 500 användare	70
	Fler än 500 användare	30
	Summa	*500*
Kommunikation		
	Fiber 1000 Mbps	29
	Ethernet över Internet 10 Mbps	70
	Internetaccess 500 Mbps	1
	Mobilt bredband 3G	200
	VPN-användare	740
Anläggningar med datakommunikation		
Färre än 5 användare		15
	5 - 10 användare	25
	10 - 20 användare	20
	20 - 50 användare	10
	Fler än 50 användare	20
Central datalagring		
	Användardata GB	5000
	Systemdata GB	3000

21 TERMER OCH FÖRKORTNINGAR

SMS Microsoft Systems Management Server. Tillhandahåller distribution av programvara, inventering, uppgraderingar, programändringar, licenshantering samt patch- och säkerhetshantering för servrar och klienter.

NAT Network Address Translation eller nätadressöversättning. En funktion i brandväggen mellan det lokala nätet och Internet och som översätter de lokala ip-adresserna till en och samma gemensam publik ip-address. Vid svar från den anropade datorn översätts ip-addressen tillbaka till den lokala adressen så att datapaketet hittar till rätt dator på det lokala nätet.

MSI Microsoft Installer. Ett standardiserat sätt att paketera och installera program i Windows.

DHCP Dynamic Host Configuration Protocol. Automatisk tilldelning av ip-addresser och vissa andra nätverksrelaterade parametrar.

MST MSI-paket med möjlighet till anpassning

UPS Avbrottsfri kraft

SDSL Symmetric Digital Subscriber Line. Dataförbindelse över telefonledning med upp till 2,3 Mbps

TCP/IP Transmission Control Protocol / Internet Protocol. Ett protokoll för datakommunikation över nätverk.

AD Active Directory

HTTPS HTTP Secure. Ett protokoll för krypterad transport av data via http-protokollet

22 BILAGOR

– Bilaga 1. KSL/IT-forums principer för regional samverkan version 2013.

23 DOKUMENTINFORMATION

Översikt
Detta dokument beskriver den it-plattform som används inom Lidingö stad.

Information	
Område	It-enheten, Konsult och service kontoret
Version / Status	5.2
Relaterade dokument	”Förvaltningsmodell för Lidingö stads it-miljö” ”Basnivå för IT-säkerhet (BITS)” ISO 2700x Bilaga 1- KSL/IT-forums principer för regional samverkan II v 2013

Godkännande			
Roll	**Namn**	**Signatur**	**Datum**
Godkänd	Björn Söderlund, it-strateg		
Godkänd	Birgitta Berglund, it-chef		
Skapad	Lars Håkansson, it-arkitekt		
Uppdaterad	Björn Söderlund, it-strateg		Maj 2012

Historik				
Version	**Status**	**Datum**	**Författare**	**Ändringssammanfattning**
0.1	Utkast	2007-10-01	Lars Håkansson	Nytt dokument
0.2	Utkast	2007-10-15	Lars Håkansson	Genomgång med Björn Söderlund
0.7	Utkast	2007-11-07	Lars Håkansson	Remitterad till It-enheten
1.0	Färdigt	2007-12-20	Lars Håkansson	Genomgång med Björn Söderlund
1.1	Uppdaterad	2009-04-20	Lars Håkansson	Justerad tillsammans med Björn Söderlund. Uppdaterat regler kring fjärranslutning samt testmiljöer.
1.23	Uppdaterad	2009-10-01	Björn Söderlund Alireza Amini Per-Johan Gelotte	Förtydligat miljö och arbetsmiljöavsnitt. Lagt till styrande principer kring driftsalternativ. Justerat texter kring miljö, drift och nuvarande miljö. Reducerat uppdateringsfrekvens av dokument. Uppdaterat version och plattform
2.0	Uppdaterad	2010-10-19	Björn Söderlund Inspect IT	Lagt till bilaga och justerat formuleringar kring kravställning av säkerhet.

2.01	Uppdaterad	2010-02-01	Björn Söderlund	Lagt till KSL/IT forums principer för samverkan. Stavningskontroll.
2.011	Uppdaterad	2010-04-11	Lars Håkansson	Uppdaterat avsnitt 13 och 15 samt kompletterat med tabell över serverplattform.
2.5	Uppdaterad	2010-05-14	Björn Söderlund, Lars Håkansson	Lagt in krav på prestanda. Bytt punkter till numrering för att underlätta hänvisning Arbetat in och arbetat om Bilaga 1 med säkerhetskrav som därmed utgår.
3.0	Uppdaterad	2010-06-11	Björn Söderlund, Lars Håkansson	Omgrupperat struktur. Redigerat och rensat bland texter
3.01	Uppdaterad	2010-06-18	Björn Söderlund, Lars Håkansson	Uppdaterat att plattformen även stöder Apache och PHP.
4.0	Uppdaterad	2012-05-22	Björn Söderlund¨ Ulrica Norgren Bo Tyrevall Lars Håkansson Per-Johan Gelotte	Uppdatering och genomgång.
5.2	Uppdaterad	2015-07-15	Björn Söderlund¨ Kenneth Winberg Andreas Liljestad Lotta Stegrell Daniel Lundh	Uppdatering och genomgång. Justerat villkor för lösenord, förvaltning mm. Ändrat referens till ny bilaga (2013) samt uppdaterat tabeller