

Økonomistyrelsen, den 25. januar 2010
Version 5.1

Vejledning om
indhold og opstilling af
sikkerhedsinstruks

Indholdsfortegnelse

0. Indledning.....	4
1. Formål.....	4
2. Ansvar for informationsbehandlingen/IT-strategi.....	4
2.1 Ledelsens ansvar	4
2.3 System- og dataejerskaber	4
2.4. Principper for Informationsikkerhed/risikovurdering.....	5
3. Dokumentationsmateriale, funktioner og opbygning.....	5
4. Fysisk sikkerhed.....	6
4.1. Serverrum	7
4.2. Brugerlokaler	7
4.3. Skadeforebyggelse.....	7
4.4. Opbevaring af datamedier og systemdokumentation	7
4.5. Virus og andre uønskede programmer.....	8
4.6. Brugernes ansvar.....	8
5. Adgangsforhold	8
5.1 Administrator konto på fysisk server/domaine.....	8
5.2 Brugeradministration vedrørende lokalnettet.....	9
5.3. Brugervedligeholdelse vedrørende Navision Stat og SQL-server	10
5.4. Brugeradministration vedrørende banksystemet	11
5.5 Brugeradgang til ØDUP-relaterede mapper	16
5.6 Interne kontrolprocedurer for brugervedligeholdelse.....	18
5.7 Eksternes adgang til institutionens systemer.....	18
6. Afvikling af driftskørsler og periodiske aktiviteter	19
6.1 Oversigt over periodiske aktiviteter.....	19
6.2 Backup/sikkerhedskopiering	19
7. Særlige driftskørsler.....	20
7.1 Opdatering med nye programversioner, servicepacks og hotfixes.	20
8. Særligt om anvendelse af eget it-anlæg med egen programmering	22
9. Særlige kontroller.....	24
9.1 Modtagelse af eBilag via OIOSI.....	24
9.2 Afsendelse af eBilag via OIOSI.....	24
9.3 Afsendelse af betalinger til Nemkonto via OIOSI og OIOSI/VANS gateway.....	25
10. Navision Stat og følsomme persondata	26
10.1 Skrivning af følsomme persondata	26
10.2 Afsendelse af elektronisk salgsbilag fra Navision Stat	26
10.3 Modtagelse af elektroniske købsbilag i Navision Stat.....	26
11. Nødplaner.....	27
12. Sikkerhedsmæssige hændelser	27

Version

Dato	Rettet af:	Versionsnr.	Ændring
27.06.2006	SKH	3.4	Ny struktur med reference til DS 484
31.08.2006	CPS/CCP	3.5	Implementering af kommentarer fra IT-enheden (Økonomistyrelsen)
15.08.2008	CPS/CCP	5.0	<ul style="list-style-type: none">• Afsnit om følsomme persondata indført.• Afsnit om JNE rettet for skift til BO• Fakturadatabase erstattet med Logging database• VANS kobling er erstattet af OIOSI• Generel gennemgang for konsekvensrettelser iht. Navision Stat 5.0• NS/ØDUP afsnittet er gennemskrevet.
05.09.2009	CPS/NAH	5.0	<ul style="list-style-type: none">• Afsnit 5.4 om Danske Bank er opdateret
25.10.2010	PGC/CPS	5.1	<ul style="list-style-type: none">• Håndtering af ØSC betjening

Dokumentet er opdateret i forhold til DS484 (jf. www.oio.dk/itsikkerhed), transportlaget samt eBilag.

Transportlaget benyttes til håndtering af elektroniske dokumenter, håndtering af betalingsfiler til og fra NemKonto systemet (NKS) samt stamdataeksport til GateTrade eProcurement (GTE) eller INDFAK, såfremt institutionen benytter GTE eller INDFAK.

Begrebet eBilag dækker over elektroniske dokumenter i form af salgs- og købsfakturaer, salgs- og købskreditnotaer, salgs- og købsrykkere, salgs- og købskontoudtog, ordre fra GTE samt betalingsdokumenter og retursvar til og fra NKS.

0. Indledning

Institutioner der anvender Navision Stat skal udarbejde en sikkerhedsinstruks, der nærmere beskriver hvorledes institutionens sikkerhedspolitik er tilrettelagt, herunder de forhold, der gør sig gældende ifbm. elektronisk fakturering samt indførelse af Nemkonto, der er affødt af bekendtgørelsens lov nr. 1203 vedtaget d. 27. december 2003. Herudover skal sikkerhedsinstruksen tage højde for de i DS484 nævnte forhold.

Denne vejledning indeholder en kort gennemgang af de punkter, der skal medtages i sikkerhedsinstruksen.

Institutioner der indgår i Økonomi Service Centret i Økonomistyrelsen, og får Navision Stat og ØS LDV hosted af KMD, CSC eller TMI via Økonomistyrelsen, skal for de områder der vedrører Navision Stat og ØS LDV, og som institutionen ikke selv har indflydelse på, henvise til Økonomistyrelsen. I vejledningen er de områder hvor der kan henvises til Økonomistyrelsen markeret.

1. Formål

Sikkerhedsinstruksen skal indledes med en kort beskrivelse af instruksens formål og tage højde for DS484, som er en fælles standard for informationssikkerhed og omhandler de basale krav en virksomhed/institution som minimum bør opfylde. Standarden fastlægger bl.a. en række krav til konkrete foranstaltninger samt overordnede krav til hvordan en institution skal styre it-sikkerhedsindsatsen. Standarden indeholder en række krav inden for områderne personalesikkerhed, fysisk sikkerhed, systemrelaterede krav og håndtering af lovbestemte og kontraktlige krav.

2. Ansvar for informationsbehandlingen/IT-strategi

I forbindelse med ansvarsfordelingen omkring informationsbehandlingen skal følgende forhold beskrives:

Ledelsens ansvar
IT-afdelingens ansvarsområde
System- og dataejerskab for institutionens it-systemer
Principper for Informationssikkerhed i institutionen

2.1 Ledelsens ansvar

Jf. DS 484, 6.1.1 (Ledelsens rolle)

2.3 System- og dataejerskaber

Jf. DS 484, 7.1.2 (Ejerskab)

Systemejerskabet for Navision Stat bør ligge hos den overordnede ansvarlige for institutionens administration. Ved ØSC medlemskab ligger systemejerskabet hos Økonomistyrelsen. Dataejerskab bør

ligge hos den ansvarlige for regnskabssystemet (f.eks. økonomi- eller regnskabschef eller funktionsansvarlig bogholder).

I den udstrækning institutionen fungerer som servicecenter for en eller flere institutioner, skal dette anføres i sikkerhedsinstruksen, ligesom det skal anføres, hvad det er for it-opgaver institutionen varetager for disse institutioner.

Transporten af eBilag, sendt og modtaget via OIOSI, foregår internt på institutionens server ved hjælp af et ”transportlag”. Transportlaget skriver data ind i en Logging database og indskriver udvalgte data i Navision Stat databasen. Transportlagets rettigheder styres af rettighederne for den tilhørende systembruger. Se nærmere herom i installationsvejledning til transportlaget på <http://www.oes.dk/sw49967.asp>

Logging database og transportlag tilføjes med angivelse af systemejer og dataejer.

2.4. Principper for Informationssikkerhed/risikovurdering

Jf. DS 484, 5.1.1 + Anneks A (Formulering af informationssikkerhedspolitik)

Jf. DS 484 5.1.2 (Løbende vedligeholdelse)

Jf. DS 484 0.4 (Opgørelse af sikkerhedsbehov)

Jf. DS 484, 4.1 (Vurdering af sikkerhedsrisici), 4.2 (Risikohåndtering), 7.2 (Klassifikation af informationer og data)

Institutionen skal være opmærksom på de manuelle rutiner, der knytter sig til brugen af it, idet Informationssikkerhed ikke kun er et spørgsmål om sikkerhed i forbindelse med lagring af oplysninger. Ved udarbejdelse og vedligeholdelse af manuelle rutiner skal der tages objektive hensyn, såsom lovkraft, men også lokale hensyn. Udførelsen af nogle manuelle rutiner kan være beskrevet i brugervejledninger m.v. Det anbefales, at man for kritiske eller komplicerede rutiner, der knytter sig til driften af it-systemet overvejer behovet for at udarbejde interne detaljerede arbejdsgangsbeskrivelser. Dette kunne eksempelvis være relevant for rutiner omkring sikkerhedskopiering, kontrol og genindlæsning af data samt destruktion af udskrifter og lagermedier med persondata i henhold til registerlovgivningen.

Mht. elektronisk fakturering skal institutionen være opmærksom på, at sikkerhedsinstruksen beskriver, at Navision ”indbakken” skal overvåges manuelt, og der skal udskrives en papirkopi til brug for sagsbehandling (godkendelse, bogføring og betaling) i det tilfælde, at godkendelsen er manuel. Hvis institutionen benytter et elektronisk fakturahåndterings- og godkendelsessystem skal instruksen beskrive dets anvendelse.

Jf. DS 484, 8.1 (Sikkerhedsprocedure før ansættelse)

Ved ØSC medlemskab henvises til Økonomistyrelsen for så vidt angår informationssikkerhed for Navision Stat.

3. Dokumentationsmateriale, funktioner og opbygning

Jf. DS 484, 7.1.1 (Fortegnelse over informationsaktiver)

Det skal endvidere være muligt at identificere det kørende system præcist ud fra angivelse af, hvor de gældende versioner af produktionssystemet er installeret. Jf. DS 484, 10.1.4 (Adskillelse mellem udvikling, test og drift)

Hvis den kørende version af Navision Stat ikke er installeret i samme bibliotek for alle arbejdspladser, skal de individuelle placeringer angives i sikkerhedsinstruksen.

Opbygningen af Payment Management funktionaliteten i Navision Stat nødvendiggør en midlertidig mellemlagring af betalingsdata i forbindelse med overførsel af data mellem Navision Stat og officebanksystemet BO. Det skal sikres, at kun bogholderimedarbejdere kan skrive data i dette mellemlager. Dette kan eksempelvis ske ved at oprette en særlig mappe på et serverdrev til formålet og kun tildele brugere med bogholderrettigheder adgang til at læse og skrive i denne mappe. Sikkerhedsinstruksen skal indeholde oplysninger om, hvordan denne sikring er foretaget.

Mhp. Elektronisk fakturering og NemKonto integrationen skal der etableres et ”transportlag” på serveren, som skal håndtere de eBilag, som udveksles med omverden, dvs. håndtere modtagelse, afsendelse og lagring af købs- og salgsdokumenter samt betalingsdokumenter. Transportlaget omfatter diverse services på serveren, Logging databasen for ind/ud dokumenter, samt en (evt. ny) systembruger, der skal læse og skrive i Logging databasen og Navision databasen, jvnf. installationsvejledningen til transportlaget.

Institutionen skal sørge for, at instruksen behandler, hvorledes det sikres, at disse services kører, og at systembrugerne har de korrekte rettigheder.

Data for originale dokumenter sendt og modtaget elektronisk lagres permanent i en Logging database hos institutionen.

I instruksen gøres tilføjelse om hvilken (hvilke) Logging database(r) der anvendes for ind og udgående fakturaer, hvor de er placeret, og hvilke regnskaber der benytter hvilke Logging databaser.

Logging databaser skal indgå i en backup rutine.

I instruksen beskrives eventuelt hvorledes Logging database (og Navision Stat database) sikres mod uautoriseret adgang, placering i forhold til firewall mv.

Ved ØSC medlemskab henvises til Økonomistyrelsen for så vidt angår dokumentationsmateriale for Navision Stat.

4. Fysisk sikkerhed

Sikkerhedsinstruksen skal beskrive hvorledes hardware, programmer og data samt sikkerhedskopier af programmer og data sikres bedst muligt i det fysiske miljø.

I den forbindelse skal beskrives hvorledes serverrum og brugerlokaler er sikret mod tyveri, brand m.v. samt anvendte foranstaltninger til skadeforebyggelse.

Ved ØSC medlemskab henvises til Økonomistyrelsen for så vidt angår fysisk sikkerhed for Navision Stat.

4.1. Serverrum

Jf. DS 484, 9.1 (Sikreområder), 9.2 (Beskyttelse af udstyr)

4.2. Brugerlokaler

Jf. DS 484, 9.1 (Sikreområder), 9.2 (Beskyttelse af udstyr)

4.3. Skadeforebyggelse

Jf. DS 484, 9.1.3 (Sikring af kontorer, lokaler og udstyr), 9.1.4 (Beskyttelse mod eksterne trusler), 9.2 (Beskyttelse af udstyr)

Brand

Brand i serverrummet vil kunne medføre tab af udstyr, programmer og data. Der bør derfor etableres foranstaltninger, der reducerer risikoen for en brands opståen og de skader, en brand vil kunne forvolde. For at forebygge brand bør der derfor ikke opbevares brandbart materiale i serverrummet. Ligeledes bør tobaksrygning være forbudt i serverrummet. Serverrummet bør være brandsikret efter forskrifter eller anvisninger fra f.eks. Brandteknisk Institut, og brandsikringsudstyr bør være placeret hensigtsmæssigt. Det bør endvidere overvejes at anvende automatiske alarmerings og brandslukningssystemer, se evt. DS 484, 9.1.4 (Beskyttelse mod eksterne trusler), 9.2.1 (Placering af udstyr)

Lynnedslag og fejlstrøm

Jf. DS 484, 9.2.2 a-c (Forsyningssikkerhed)

Vandskade

Jf. DS 484, 9.1.4 (Beskyttelse mod eksterne trusler), 9.2.1 (Placering af udstyr)

Tyveri og hærværk

For at forhindre tyveri og hærværk bør serverrummet være aflåst. Vinduer og døre i serverrum bør altid holdes aflukket og låst. For at kunne spore udstyr i forbindelse med tyveri, kan udstyrets serienumre registreres og udstyret kan mærkes, se evt. DS 484 9.1.1 (Fysisk afgrænsning)

4.4. Opbevaring af datamedier og systemdokumentation

Aktuelle datamedier, f.eks. sikkerhedskopier, programmer og systemkonfigurationer, der er nødvendige ved en eventuel retablering af edb-systemet bør opbevares i et brandsikkert skab. Instruksen skal indeholde oplysninger om skabets placering og om regulering af adgangen til skabet, se evt. DS 484, 9.2 (Beskyttelse af udstyr), 10.5.1 (Sikkerhedskopier), DS 484, 10.7.4 (Beskyttelse af systemdokumentation).

Hvis der ligeledes opbevares dokumentation vedrørende kildekode henvises til DS 484, 12.4.3 (Styring af adgang til kildekode).

4.5. Virus og andre uønskede programmer

Jf. DS 484, 10.4 (Skadevoldende programmer og mobil kode)

Uvedkommende indtrængen på netværk

Jf. DS 484, 11.4 (Styring af netværksadgang)

4.6. Brugernes ansvar

Jf. DS 484, 8.1.1 (Opgaver og ansvar), 11.3 (Brugernes ansvar)

5. Adgangsforhold

Adgangsforhold til institutionens it-systemer skal være beskrevet i institutionens sikkerhedsinstruks. Beskrivelsen i instruksen skal som minimum omfatte følgende forhold:

- Brugeradministration vedrørende lokalnettet
- Brugeradministration vedrørende Navision Stat/SQL
- Brugeradministration vedr. banksystemet
- Interne kontrolprocedurer for brugervedligeholdelse
- Eksternes adgang til institutionens systemer
- Retningslinier for anvendelse af remote support program

Ved ØSC medlemskab henvises til Økonomistyrelsen for så vidt angår adgangsforhold for Navision Stat.

5.1 Administrator konto på fysisk server/domaine

Der bør oprettes en unik administrator-konto (herefter benævnt **Admin_Account**) til de driftsansvarlige i institutionens IT-afdeling. Navngivningen af disse konti kunne evt. være admin_ efterfulgt af brugerens initialer. Det vil således være muligt at logge, hvem der har lavet hvad og hvornår. Der bør ligeledes oprettes en navngiven konto til eksterne konsulenter, som efterfølgende bliver disabledt når konsulenten forlader institutionen.

Auditing af serveren

Efter behov anbefales det at overvåge visse handlinger på serveren ved at slå auditing til. Der er en række muligheder for hvilke typer begivenheder, der skal logges og hovedregelen er, at det kun er det mest relevante, der skal slås til. Dels har det indflydelse på performance og dels kan det let resultere i en lang række logninger.

I et windows 2000-domæne kan auditing defineres på en række niveauer: Site, domæne, organisatorisk enhed eller lokalt på den enkelte computer. Det bør defineres på et så højt niveau som muligt, men dette afhænger af det konkrete setup og her beskrives udelukkende, hvordan dette gøres lokalt på serveren. For mere information refereres i øvrigt til Dokumentationen for Windows 2000 server og følgende artikler uddyber dette:

HOW TO: Enable and Apply Security Auditing in Windows 2000

<http://support.microsoft.com/default.aspx?kbid=300549>

og for mere generel information henvises til:

Securing Windows 2000 Server – Patterns and Practices

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/scwin2k/>

5.2 Brugeradministration vedrørende lokalnettet

For at få adgang til Navision Stat skal en bruger være oprettet på lokalnettet og dermed have adgang til visse af lokalnettets ressourcer (printere, program- og databiblioteker mv.).

For at få adgang til lokalnettet skal brugeren tildeles et password. Der gælder følgende minimumskrav for tildeling af password:

Passwords er personlige og fortrolige og består af mindst 6 tegn, og de skal udskiftes mindst hver 3. måned. Password skal endvidere udskiftes, hvis det er – eller der er mistanke om, at det er – kommet til andres kendskab. Hvis der forgæves forsøges login til et brugernavn mere end 3 gange i træk, skal brugerens adgang til systemet automatisk lukkes. Indtastning af password skal ske i et ikke læsbart felt.

En del af Navision Stats sikkerhedsforanstaltninger bygger på funktioner i arbejdspladsens operativsystem (Windows NT/98 og nyere). For at disse foranstaltninger (håndhævelse af passwordpolitik, skærmlås m.v.) kan fungere, kræves det, at en bruger skal være oprettet under samme brugernavn på lokalnettet, på SQL-serveren og i Navision Stat. Endvidere skal Navision Stat og SQL-serveren være konfigureret til at benytte NT-authentication.

I forbindelse med udarbejdelsen af institutionens sikkerhedsinstruks skal institutionen overveje om ovennævnte minimumskrav for passwordpolitik er tilstrækkelige i forhold til det sikkerhedsniveau, som institutionen ønsker.

Transportlaget skal i forbindelse med modtagelse og afsendelse af elektroniske fakturaer samt udveksling af NemKonto data foretage læsning og skrivning i Logging databasen og Navision databasen.

Der skal derfor benyttes en systembruger til transportlaget, med de korrekte tilstrækkelige rettigheder. Se installationsvejledning til transportlaget for krav til rettighederne.

Denne bruger skal have rettighed til at:

afvikle de nødvendige services/ stored procedures på serveren
skrive til Navision databasens tabel 'NS TS Udveksling'
læse fra Navision databasens tabeller: 'NS TS Integrationsopsætning' og 'NS TS Dokument Type'.

Der kan benyttes en eksisterende systembruger, hvis denne ikke har for store rettigheder.

Alternativt kan oprettes en særlig systembruger med tilpassede rettigheder.

Denne systembruger skal oprettes som windowsbruger/domæne-bruger i Navisions brugeradministration. Dennes rettigheder tildeles direkte på serveren og ikke fra Navisions brugeradministration.

Den anvendte systembruger for transportlaget skal være omfattet af institutionens beskrivelse af brugeradministration og vedligehold.

5.3. Brugervedligeholdelse vedrørende Navision Stat og SQL-server

Brugere skal foruden at være oprettet på lokalnettet også være oprettet i Navision Stat og i SQL-serveren for at kunne benytte systemet, og de skal være tildelt autorisationer, der matcher deres funktioner i organisationen.

Hver bruger af Navision Stat skal være oprettet med eget brugernavn og et tilhørende password. Kravet om password gælder også Navision-sikkerhedsadministrator.

For en nærmere beskrivelse af brugerprofiler i Navision Stat henvises til Økonomistyrelsens afsnit 4 i 'Generel beskrivelse af Navision Stat'.

Sikkerhedsinstruksen skal beskrive, hvordan den overordnede brugeradministration i Navision Stat foretages, og hvem der udfylder rollen som Navision Stat sikkerhedsadministrator. Ved overordnet brugeradministration forstås større omlægninger af rettighedstildelinger eller rettighedsgrupper samt tildeling af nye rettigheder til de funktionsansvarlige, der varetager den daglige brugeradministration.

Navision sikkerhedsadministratoren skal være særligt sikret mod misbrug, og opgaven må ikke varetages af en person, som har almindelig brugeradgang til systemet. I praksis kan det være svært at tildele denne rolle til én person, og den kan derfor i praksis være tildelt funktionsansvarlig bogholder og funktionsansvarlig kasserer i fællesskab.

Brugervedligeholdelse og tildeling af brugerrettigheder skal foregå efter en fast procedure. Proceduren skal sikre, at ingen enkeltperson kan få fuld kontrol over regnskabssystemet. Dette sikres ved personmæssig adskillelse af visse funktioner.

Proceduren skal endvidere sikre, at det kan kontrolleres, hvilke rettigheder hver enkelt bruger har, og hvilke oplysninger personale, der udfører brugervedligeholdelse, har registreret i adgangskontrolsystemet i det lokale regnskabssystem.

Såfremt institutionen har behov for at definere egne rettighedsgrupper, skal dette ske under hensyntagen til de sikkerhedsbestemmelser og krav om adskillelse af funktioner, som er beskrevet i institutionsinstruksen. Oprettelse af egne rettighedsgrupper må kun ske med dataejerens skriftlige godkendelse. I det omfang institutionen selv har defineret rettighedsgrupper, som ligger ud over systemets standardgrupper, skal disse beskrives nærmere i sikkerhedsinstruksen.

MS SQL Server

Som udgangspunkt bør der kun benyttes Windows login på SQL Serveren, og der bør benyttes de administrator- konti som blev oprettet under afsnit 5.1, således at det er muligt at logge/trace de handlinger der foregår i SQL Serveren med unik bruger-id.

SA brugeren bør kun benyttes i særlige tilfælde. SA password'et bør deles mellem 2 personer, og efterfølgende gemmes i et brandsikkert skab og i hver sin forseglede kuvert.

5.4. Brugeraadministration vedrørende banksystemet

Adgang til institutionens officebanksystem, Business Online, reguleres i forbindelse med institutionens tilslutning til Statens KoncernBetalingsystem (SKB) og installering af Business Online (BO) hos institutionen i henhold til aftale mellem Danske Bank og institutionen.

Institutionen anmoder Økonomistyrelsen om at blive etableret som kontohaver i SKB, jf. den procedure, der på Økonomistyrelsens hjemmeside under SKB/OBS er beskrevet herfor.
<http://www.oes.dk/sw54056.asp>.

Anmodningen skal underskrives af institutionen og vedlægges tegningsberettigedes underskrift i kopi i henhold til regnskabsinstruks.

Sammen med anmodningen udfylder og indsender institutionen de krævede oplysninger, således som disse fremgår af Skema 1 for statsinstitutioner, respektive Skema 2 for selvejende institutioner, under staten til omtalte anmodning.

Økonomistyrelsen behandler anmodningen om etablering af nye kontohaverforhold i SKB og videresender den godkendte anmodning til Danske Bank til effektivering.

Ved Økonomistyrelsens imødekommelse af anmodningen gives institutionen fuldmagt til at disponere over de konti, der i henhold til beskrivelse oprettes i SKB - herunder bemyndigelse til at give fuldmagt og prokura til brugere i BO udvalgt efter institutionens ønske.

Brugerfuldmagt i Business Online

Kontohaver skal udstede en fuldmagt til brugeren, før denne kan foretage transaktioner i Business Online på vegne af kontohaver eller en tredjemand. Brugerfuldmagten oprettes via Business Online. Fuldmagten til en bruger vedrørende tilmeldte konti oprettes via bankens brugerfuldmagt i Business Online.

Hvis en tredjemand har underskrevet ”Tredjemands fuldmagt til Virksomheder, der selvadministrerer ”brugere”, kan kontohaver videregive denne fuldmagt til en bruger. Det sker ved hjælp af brugerfuldmagten i Business Online.

Forinden oprettelse af en brugerfuldmagt skal Kontohaver indhente brugers samtykke til, at brugers CPR-nr. må videregives til banken.

Administration af brugere

Ved oprettelse af en bruger skal Kontohaver tage stilling til om bruger skal tildeles administrationsrettigheder. Følgende administrationsrettigheder kan tildeles:

- Aftleadministration
- Brugeradministration
- Aftaleinformation
- Pinkode og spærring
- Konti og Kort
- Udbetalingsmaksimum og lånerammer

Hvis bruger tildeles rettighederne Aftale- og Brugeradministration, skal Kontohaver tage stilling til, hvilken af følgende fuldmagtstyper, brugeren skal tildeles i hvert enkelt tilfælde:

- Alene fuldmagt
- To i forening (A-fuldmagt).

Hvis brugeren tildeles rettigheden Udbetalingsmaksimum, vil brugeren kunne tildeles:

- Alene fuldmagt
- To i forening (A-fuldmagt)
- To i forening (B-fuldmagt)
- To i forening (C-fuldmagt)
- Aftleadministration

Hvis Kontohaver tildeler bruger rettigheden Aftleadministration bemyndiges bruger til på Kontohavers vegne:

- at anmode om tildeling af rettigheden Aftleadministration til brugere, herunder anmode om at ændre rettigheden Aftleadministration under eksisterende brugere,
- at slette brugeres aftleadministrationsrettigheder,
- at oprette, rette og slette brugeres brugeradministrationsrettigheder ,
- at oprette og slette brugeres aftaleinformationsrettigheder,
- at oprette og slette brugeres rettigheder vedrørende pinkode og spærring,
- at oprette og slette brugeres rettigheder vedrørende Konti og Kort
- at oprette, rette og slette brugeres rettigheder vedrørende Udbetalingsmaksimum.

Aftleadministrator kan tildele sig selv og andre brugere disse rettigheder. Tildeling af aftleadministrationsrettigheder skal altid godkendes af ledelsen hos Kontohaver.

Når en bruger med rettigheden Aftleadministration har anmodet om oprettelse eller rettelse af en brugerfuldmagt med aftleadministrationsrettigheder, vil der blive genereret en brugerfuldmagt med underskriftfelt i eArkiv. Brugerfuldmagten vil være tilgængelig for brugere med rettigheden Aftaleinformation.

Brugerfuldmagten skal underskrives af ledelsen hos Kontohaver (tegningsberettigede) og sendes til banken, som herefter igangsætter ændringen.

Med sin underskrift anerkender ledelsen hos Kontohaver at de kortbetingelserne, som er tilgængelige på www.danskebank/skbobs under menuen Business Online/Betingelser gælder for kortaftaler der indgås på baggrund af administrators tildeling af rettigheden konti og kort til brugere.

I øvrige tilfælde godkender og underskriver bruger med sin digitale signatur. Brugere med rettigheden Aftleadministration skal også være tildelt rettigheden Brugeradministration.

Brugeradministration

Hvis Kontohaver tildeler bruger rettigheden Brugeradministration, bemyndiges brugeren til på Kontohavers vegne:

- at oprette og rette Kontohavers almindelige brugere, herunder give brugeren adgang til de ønskede moduler, konti, fuldmagts- og transaktionstyper,
- at oprette og rette en brugers stamoplysninger,
- at slette alt på en bruger, herunder stamoplysningsdata.

Brugeradministrator kan tildele sig selv og andre brugere disse rettigheder.

Aftaleinformation

Med rettigheden Aftaleinformation får bruger - via en brugeroversigt - adgang til at søge på aftalens bruger samt få listet brugerens individuelle adgange (stamoplysninger, moduler, administrationsrettigheder, adgange til konti og betalinger). Herudover får bruger adgang til alle de dokumenter, der er lagret i eArkiv (ex. de af Kontohaver udstedte brugerfuldmagter).

Fuldmagtstyper

Med typen af fuldmagt kan Kontohaver bestemme, hvilke brugere der sammen eller alene må godkende en betaling eller en ordre. I banken findes der følgende fuldmagtstyper:

- Alene fuldmagt
- To i forening (A-fuldmagt)
- To i forening (B-fuldmagt)
- To i forening (C-fuldmagt)

Alene fuldmagt

Når en ordre er lagt ind af en bruger med denne fuldmagt, betragtes ordren automatisk for godkendt af denne. Brugere med denne fuldmagt kan også godkende ordrer, der er lagt ind af brugere med alle andre fuldmagtstyper. Administratorer må ikke oprette brugere med alene fuldmagt til betalinger.

To i forening (A fuldmagt)

Brugere med A-fuldmagt er sideordnede, og godkendelsesrækkefølgen er derfor underordnet, når to fuldmægtige godkender en betaling eller en ordre. Når en ordre eller en betaling er lagt ind af en bruger med A-fuldmagt, er den automatisk godkendt af denne (1. godkendelse). Betalingen kræver endnu en godkendelse (2. godkendelse) af en bruger med enten alene fuldmagt, A-, B- eller C-fuldmagt

To i forening (B-fuldmagt)

Når en betaling er lagt ind af en bruger med B-fuldmagt er betalingen automatisk godkendt af denne (1. godkendelse). Betalingen skal herefter godkendes (2. godkendelse) af en bruger med enten alene, A- eller C-fuldmagt. To brugere med B-fuldmagt kan ikke godkende en betaling sammen.

To i forening (C-fuldmagt)

Når en betaling er lagt ind af en bruger med C-fuldmagt, er betalingen automatisk godkendt af denne (1. godkendelse). Betalingen skal herefter godkendes (2. godkendelse) af en bruger med enten alene, A- eller B-fuldmagt. To brugere med C-fuldmagt kan ikke godkende en betaling sammen.

Nemkonto

I forlængelse af ovenstående er det også muligt fra Navision at sende betalinger til Danske Bank via NKS (Nemkonto Systemet), hvor det er muligt at håndtere komplette såvel som ukomplette betalinger. Alle relevante brugere af NKS skal i relation til ovenstående have tildelt de rolleprofiler, som de har brug for i NKS.

I forbindelse med myndighedens tilslutning til NKS skal myndigheden udfylde en massetilslutningsaftale til NKS, hvor der kan oprettes op til 5 brugere.

Der kan indgås en tillægsaftale hvis myndigheden ønsker at KMD skal oprette flere brugere, end de brugere, der er oprettet ifm. massetilslutningsaftalen. Der er mulighed for at tildele rolleprofiler på flg. 2 niveauer:

Rolleprofiler på myndighedsniveau:

Rolleprofilerne giver brugeren adgang til at udføre opgaven for hele myndigheden.

Rolleprofiler	NKS-KTOVIS	NKS-KTOADM	NKS-YDEADM	NKS-SØGBET	NKS-SØGBUN
Skal tildeles brugeren (marker med X, hvilke rolleprofiler brugeren skal have tilknyttet)					

Rolleprofiler på LOS-enhedsniveau (bogf.kreds):

Rolleprofilerne giver brugeren adgang til at udføre opgaven for den enkelte LOS-enhed (bogføringskreds).

Rolleprofiler	NKS-VISLØN + NKS-VISKRP	NKS-VISLEV	NKS-BETSTA	NKS-BUNSTA
Skal tildeles brugeren på følgende LOS-enheder (anfør hvilke bogf.kredse, brugeren skal have tildelt de forskellige rolleprofiler til)				

Der er i det efterfølgende angivet, hvilke rettigheder de enkelte rolleprofiler dækker over.

Tildeles på myndighedsniveau

Rolleprofil	Beskrivelse/bemærkning
NKS-KTOVIS	Adgang til at vise NemKonti og Specifikke konti
NKS-KTOADM	Adgang til at vise, oprette, rette og slette Nemkonti og specifikke konti.
NKS-YDEADM	Adgang til at vise, oprette, rette og slette ydelsesarter for en given offentlig myndighed
NKS-SØGBET	Adgang til Betalingsmenu og søgebillede for enkeltbetalinger
NKS-SØGBUN	Adgang til betalingsmenu og søgebillede for bundter

Tildeles på LOS-enhedsniveau (bogf.kreds)

Rolleprofil	Beskrivelse/bemærkning
NKS-VISLØN + NKS-VISKRP	Adgang til at se betalinger tilknyttet ydelsesarten *LØN (Løn, honorarer og tjenestemandspension), samt ydelsesarten *KRP (Kapital-ratepensionsindbetaling)
NKS-VISLEV	Adgang til at se betalinger med ydelsesarten *LEV tilknyttet. (Leverandørudbetalinger)
NKS-BETSTA	Adgang til standsning af enkelt betalinger. Tildeles med administrativ enhed som dataudsnit. Sagsbehandleren, der har adgang til at standse betalinger, kan standse alle de betalinger, vedkommende har autorisation til at se
NKS-BUNSTA	Adgang til at standse et bundt af betalinger. Tildeles med administrativ enhed som dataudsnit. Sagsbehandleren, der har adgang til at standse betalinger, kan via standsningen standse betalinger, som vedkommende ikke har autorisation til at se, da autorisationen går på HELE bundtet

Forinden brugerne kan tildeles de relevante rolleprofiler i NKS, skal medarbejderne oprettes som autoriserede brugere med digitale signaturer.

I forbindelse med udsøgning af betalinger til NKS, sker prokurahåndteringen i Navision.

Der skal oprettes prokuragrupper (eksempelvis Bogholdere og Kasserer) og prokurabrugere i Navision, hvorefter der opsættes, hvilken prokurabrunder der første godkender og tilsvarende hvem der anden godkender betalingen. Jf. 'Generel beskrivelse af Navision Stat', afsnit 5.5.

5.5 Brugergang til ØDUP-relaterede mapper

NS/ØDUP er den integrationskomponent, der udveksler data mellem Økonomistyrelsens Dataudvekslingspunkt (ØDUP) og institutionens server. Det program der varetager dataudvekslingen hedder ØDUP-Invokeren.

ØDUP-invokeren bør afvikles af en systembruger, som netop har de rettigheder den skal bruge.

Økonomistyrelsen anbefaler at oprette systembrugeren som et medlem af 'Users' gruppen, dvs. en almindelig bruger uden administrator-rettigheder. Denne bruger har som udgangspunkt kun få rettigheder i serverens filsystem og ingen rettigheder til de relevante databaser.

Ved ØSC medlemskab henvises til Økonomistyrelsen for så vidt angår ØDUP integrationen til Navision Stat.

Oprettelse af brugeren i SQL Server og tildeling af DB rettigheder

Systembrugeren skal derudover have tildelt de nødvendige rettigheder til serverens filsystem og til relevante "objekter" i de databaser som anvendes af ØDUP-Invokeren.

Økonomistyrelsens leverer et rettighedsscript til en systembruger med de nødvendige rettigheder. Rettigheds-scriptet hedder 'SecuritySettings_5_00.sql.'

Systembrugeren kan oprettes som lokal Windowsbruger som medlem af gruppen "Users", hvis ØDUP-invokeren, Navision databasen og evt. ØS LDV ligger på samme server.

Hvis ØDUP-invokeren ligger på en server og Navision Stat ligger på en anden server, skal systembrugeren oprettes som domænebruger som medlem af gruppen 'Domain Users'.

Rettigheder til filsystem

En bruger som er medlem af "Users" gruppen har kun læse- og afviklingsrettigheder i filsystemet. Da OedupInvokeren danner en logfil samt flytter datastrømsfiler, skal brugeren tildeles skrive- og modificeringsrettigheder til de mapper, som OedupInvokeren er installeret i, og underliggende mapper.

Auditing af serveren

Efter behov anbefales det at overvåge visse handlinger på serveren ved at slå auditing til. Der er en række muligheder for hvilke typer begivenheder, der skal logges og hovedregelen er, at det kun er det mest relevante, der skal slås til. Dels har det indflydelse på performance og dels kan det let resultere i en lang række logninger.

Auditing defineres på en række niveauer: Site, domæne, organisatorisk enhed eller lokalt på den enkelte computer. Det bør defineres på et så højt niveau som muligt, men dette afhænger af det konkrete setup og her beskrives udelukkende, hvordan dette gøres lokalt på serveren.

Indstillinger og minimumsanbefaling kan kort skitseres som følger, men afhænger meget af det lokale behov.

Policy	Beskrivelse	Anbefalet minimumsindstilling
Audit account logon events	Lokale logon til serveren	Success + Failure
Audit account management	Logger oprettelse, ændring og sletning af konti på serveren	Failure
Audit directory service access	Adgang til	Failure
Audit logon events	Alle logins til serveren logges, både interaktivt eller via netværk	Success + Failure
Audit object access	Logger fejlet adgang til objekter filer. For filer og mappers vedkommende, bliver der kun logget, såfremt auditing er defineret for de pågældende mapper/filer og aktuel bruger. Bemærk at dette genererer mange logninger.	No auditing
Audit privilege use	Dette logger ethvert succesfuldt eller fejlet forsøg på at anvende en brugers rettigheder på serveren. Dette genererer ligeledes mange hits på serveren	No auditing
Audit policy change	Ændringer af policy indstillinger, tilføjelse/sletning af bruger mm.	No auditing
Audit process tracking	Logger alle start og stop af processer	Failure
Audit system events	Genstart af serveren og sletning af event logs	Success + Failure

Uanset niveau af logning, anbefales det at ændre den maksimale størrelse på security-eventloggen samt ændre håndtering af fuld log. Som udgangspunkt overskrives ældste events og er der forsøg på eller sket sikkerhedsbrud, er dette gerne det mest relevante.

NTFS-rettigheder¹

Den følgende tabel lister dels anbefalinger vedr. NTFS-rettigheder til relevante mapper dels minimumskravene for at synkroniseringen fungerer.

Mappe	Rettighed
Ødup-katalog med underliggende partneraftaler, eks. C:\OedupNs	System – modify Service_Account - modify Admin_Account – modify

¹ New Technology File System

Som udgangspunkt anbefales det, at følgende NTFS rettigheder er sat på mappen OedupNS samt underliggende mapper:

Følgende brugere skal have rettighed til mapperne:

Domain Admins har:	Modify
Service har:	Modify
System har:	Modify

Derudover skal der sættes hak i 'Reset permissions on all child and enable propagation of inheritable permissions', under 'Advanced'. Bemærk, at hvis alt kører på en enkelt server, skal den lokale administrator gruppe have Modify rettigheder.

Bemærk, at alle datastrømme i forbindelse med import og eksport på et tidspunkt vil befinde sig i en af undermapperne til ØDUP/NS. Derfor anbefales det, at disse datastrømme bliver beskyttet af de ovennævnte sikkerhedsforanstaltninger.

5.6 Interne kontrolprocedurer for brugervedligeholdelse

Det skal til en hver tid være klart defineret, hvem der har adgang til regnskabssystemet og tilknyttede databaser, og brugere af systemet skal være tildelt de rettigheder, der er nødvendige og tilstrækkelige, for at de kan udføre deres opgaver. Brugernes rettigheder skal være tildelt/rekvireret af en person, der er bemyndiget hertil. Der skal føres kontrol med, at disse regler er opfyldt.

Sikkerhedsinstruksen skal indeholde en beskrivelse af kontrolprocedurer.

5.7 Eksternes adgang til institutionens systemer

Institutionen skal fastsætte regler for, hvilke eksterne personer, der kan få adgang til institutionens systemer, hvilke systemer og data der kan være tale om, hvilke betingelser det kan ske på, og hvor længe adgang tillades.

Som eksempler på eksterne personer, der kan få adgang til institutionens systemer, kan nævnes revisorer, konsulenter og supportmedarbejdere i Økonomistyrelsen.

Sikkerhedsinstruksen skal indeholde en oversigt over eksterne adgang til institutionens systemer.

6. Afvikling af driftskørsler og periodiske aktiviteter

6.1 Oversigt over periodiske aktiviteter

Sikkerhedsinstruksen skal indeholde en oversigt over periodiske aktiviteter og driftskørsler i forhold til institutionens regnskabssystem.

Ved ØSC medlemskab henvises til Økonomistyrelsen for så vidt angår periodiske aktiviteter for Navision Stat.

6.2 Backup/sikkerhedskopiering

Formålet med backup/sikkerhedskopieringen er at kunne retablere et kørende regnskabssystem efter hændelser, der har medført tab af data.

Institutionens forretningsgange og procedurer vedrørende sikkerhedskopieringen skal som minimum opfylde de krav der er beskrevet nedenfor omkring opbevaring af sikkerhedskopier og kontrol af den daglige driftsafvikling.

Som følge af elektronisk fakturering skal Logging databasen, der indeholder de modtagne originale XML dokumenter inkl. et eventuelt TIFF billede af den skannede faktura/kreditnota, samt den filmappe (jævnfør installationsvejledningen for transportlaget) de elektroniske dokumenter bliver gemt i, indgå i den backup rutine, som institutionen har vedtaget for driftsmiljøet. Kravene til Logging databasens sikkerhed er mindst på samme niveau som kravene til Navision databasen.

I samme Logging database lagres endvidere kopi af de afsendte originale OIO xml dokumenter. Indholdet i Logging databasen udgør de originale dokumenter, som modsvarer arkiveringen af de hidtil modtagne papirfakturaer hhv. kopier af afsendte papirfakturaer.

Økonomistyrelsens vejledning (Microsoft SQL server installationsvejledning) indeholder standardopsætninger for SQL-serverens automatiske sikkerhedskopieringsfunktioner. Hvis disse er anvendt, skal institutionens sikkerhedsinstruks referere til disse. Hvis andre indstillinger er anvendt, skal sikkerhedsinstruksen indeholde en beskrivelse af baggrunden for de valgte indstillinger.

Ved ØSC medlemskab henvises til Økonomistyrelsen for så vidt angår backup, sikkerhedskopier, driftsovervågning mv. for Navision Stat.

Opbevaring af sikkerhedskopier

Nedenstående retningslinier for opbevaring af sikkerhedskopier omhandler alene opbevaring af sikkerhedskopier og opbevaring af regnskabsmateriale på maskinlæsbare medier (edb-medier, f.eks. magnetbånd, cd-rom'er o.lign.). Regnskabsmateriale på andre medier (papir, mikrofilm mv.) behandles og arkiveres efter de i regnskabsinstruksen beskrevne regler.

Der skal til enhver tid opbevares mindst 10 generationer af daglige kopier svarende til alle hverdage i mindst to uger, mindst 3 generationer af månedskopier samt minimum årskopier for de forudgående 5 år.

Daglige kopier kan anbringes på internt arkiv. Uge-, måneds- og årskopier skal anbringes på eksternt arkiv.

Sikkerhedskopier skal opbevares på en sikker måde, så de er beskyttet mod fysisk skade og tab. Sikkerhedskopier skal endvidere opbevares fysisk adskilt fra it-udstyret.

Proceduren for drift af it-systemet, samt arkivering og fremfinding af sikkerhedskopier skal sikre, at ingen person har adgang til it-systemet og samtlige sikkerhedskopier på en gang, således at personen har mulighed for ved et uheld eller i ond mening at ødelægge eller fjerne alle systemets data og samtlige eksisterende sikkerhedskopier.

Det skal fremgå af sikkerhedsinstruksen, hvilken medarbejder, der anbringer sikkerhedskopier på eksternt arkiv. Det skal endvidere af sikkerhedsinstruksen fremgå, hvor det interne og det eksterne arkiv for sikkerhedskopier findes. Se evt. DS 484, 10.5 (Sikkerhedskopiering).

Kontrol af den daglige driftsafvikling

Kontrol af den daglige driftsafvikling skal omfatte en kontrol af, at sikkerhedskopiering er foretaget, og at sikkerhedskopierne er anvendelige.

Det skal fremgå af institutionens sikkerhedsinstruks, hvem der foretager, og hvornår der foretages kontrol af den daglige driftsafvikling

Dokumentation af kontrollen skal fremgå af institutionens backup-kalender/driftlog, som forsynes med dato, underskrift samt eventuelle bemærkninger vedrørende driftsafviklingen/kontrollen.

Institutionens sikkerhedsinstruks skal desuden omfatte en nærmere beskrivelse af proceduren vedrørende kontrol af den daglige driftsafvikling. Sikkerhedsinstruksen skal tillige beskrive institutionens kontrol af retableringsprocedure med henblik på at kontrollere, at retablering kan foretages på grundlag af de eksisterende sikkerhedskopier.

7. Særlige driftskørsler

7.1 Opdatering med nye programversioner, servicepacks og hotfixes.

Ved ØSC medlemskab henvises til Økonomistyrelsen for så vidt angår nye programversioner, servicepacks og hotfixes til Navision Stat.

Økonomistyrelsen distribuerer med mellemrum programopdateringer til Navision Stat-institutionerne, der hentes via ØS's hjemmeside <http://www.oes.dk/sw1178.asp> (Der udsendes Navision Stat nyhed).

En programopdatering kan bestå af følgende:

Opdatering af Navision Stat-databasen

Opdatering af relaterede systemer til Navision Stat (f.eks. Transportlaget eller ØDUP-integrationen)

Opdatering af de relaterede systemer kan indeholde forskellige komponenter afhængigt af system og løsning.

En Navision Stat opdatering består normalt af en fob-fil med et antal nye og/eller ændrede objekter. Derudover vil der lidt afhængigt af releases karakter være vedlagt følgende:

- Inf- filer, der bruges i forbindelse med det lokale versionstyringssystem.
- Kon-filer, der anvendes i forbindelse med datakonvertering.
- Hjælpefiler til Payment Management, Navision Stat og Navision Standard.
- dll-filer for programudvidelse.
- Stored procedures.
- Data-filer.
- Diverse komponent filer.

Institutionen er forpligtet til at indlæse obligatoriske og nye opdateringer og servicepacks i produktions-databasen inden for 90 kalenderdage, efter at denne er modtaget. Hotfixes, der indeholder kritiske fejlrettelser, indlæses indenfor 5 arbejdsdage. Tidsfristerne er fastsat i de idriftsættelsesaftaler/leveringsaftaler, der indgås mellem institutionerne og Økonomistyrelsen.

Vedlagt programopdateringen er en kort beskrivelse af, hvilke områder og moduler er blevet ændret, og hvilke nye eller ændrede funktionaliteter, institutionen skal forberede sig på at bruge – og evt. teste i eget testmiljø (Her kan institutionen eventuelt vedlægge Systeminfo'en udgivet af ØS - denne beskriver netop rettelserne).

Indlæsning af alle objektændringer i Navision Stat produktions-databasen skal foretages af Netværks-sikkerhedsadministratoren eventuelt i samarbejde med institutionens underleverandør. En anden medarbejder skal foretage kontrol af, at nyeste programversion er indlæst. Proceduren for programoverførsel, inkl. evt. installation i et test-miljø, skal være beskrevet nærmere i institutionens sikkerhedsinstruks.

Når indlæsningen er foretaget og efterfølgende kontrolleret, skal institutionen give besked til Økonomistyrelsen via VMS's (versionsstyringsmodul i Navision Stat) automatiske e-mail og kvitteringsfunktion og ellers blot via mail.

Der skal føres log over programopdateringer og den efterfølgende kontrol heraf. Sikkerhedsinstruksen skal indeholde en nærmere beskrivelse af denne log og adgangene til den.

Fremgangsmåden ved indlæsning og kontrol af nye programopdateringer er beskrevet i brugervejledning til Lokal versionsstyring (VMS), samt i den til releasen medfølgende SystemInfo.

Alle objekter i Navision Stat er entydigt identificeret ved en objekttype og et objektnummer. Adgangen til at modificere objekter styres dels gennem overordnet tildeling af rettigheder til at modificere objekter dels gennem begrænsninger i den type licens, der er erhvervet. Adgangen til at modificere objekter fremgår af nedenstående tabel.

Objektinterval	Beskrivelse	Kan oprettes af	Kan ændres af	Må afvikles af
----------------	-------------	-----------------	---------------	----------------

[1 ; 49.999] [99.000.750 ; -]	Navision Attain	Microsoft Danmark	Forhandlere/ udviklere med AL-nøgle	Brugere i henhold til tildelte rettigheder (og erhvervet licens)
[50.000; 99.999]	Forhandler- område	Forhandlere/ udviklere med AL-nøgle		
[6.016.800; 6.017.206]	Payment Management	Celenia Software		
[6.006.850; 6.007.849]	Navision Stat	Økonomi- styrelsen		

Institutionen skal etablere faste procedurer omkring opdatering af Navision Stat og relaterede systemer. Disse procedurer skal sikre, at den kørende version af regnskabssystemet er i overensstemmelse med den af ledelsen og systemejer godkendte. Der skal foretages sikkerhedskopiering umiddelbart før opdatering. Denne kopi skal ligesom tilhørende relevant systemdokumentation arkiveres, da der til stadighed skal kunne redegøres for og fremfindes tidligere versioner i fornødent omfang. Dette vil i praksis sige i fem år efter et finansårs afslutning.

Økonomistyrelsen anbefaler at der etableres et testmiljø, hvor en kopi af den aktuelle produktionsdatabase til Navision Stat er indlæst. Her kan brugerne frit eksperimentere med de forskellige funktionaliteter i systemet, uden at det påvirker de rigtige regnskabsdata. Brugere har således en periode til at blive fortrolige med nye eller ændrede funktionaliteter i nye Navision Stat versioner, inden de indlæses i produktionsdatabasen.

For ØSC institutioner på Navision Stat 5.0 eller nyere, varetages særlige driftskørsler af Økonomistyrelsen.

8. Særligt om anvendelse af eget it-anlæg med egen programmering

Beslutning om ændringer i regnskabssystemet samt rekvisition af systemudvikling og tilpasninger varetages for de fælles statslige dele af systemet af Økonomistyrelsen.

For så vidt angår lokale tilpasninger varetages disse opgaver af systemejer, der også godkender programopdateringer, før de sættes i drift.

Såfremt institutionen selv foretager programmering, foretager specialtilpasninger eller får sådanne opgaver udført af en ekstern leverandør, skal sikkerhedsinstruksen indeholde en nærmere beskrivelse af, hvem der rekvirerer og foretager systemudvikling, tilpasning og programmering samt nærmere retningslinier for dokumentation af evt. ændringer/tilføjelser. Opgavefordeling skal ske under hensyn til en hensigtsmæssig personmæssig adskillelse.

Instruksen skal endvidere indeholde en oversigt over, hvem der udfører systemopgaver. Disse opgaver er:

- overførsel af nye versioner til drift
- driftsafvikling

- kontrol af driftsafvikling
- anbringelse og afhentning af sikkerhedskopier på eksternt arkiv
- brugeradministration på lokalnettet og SQL-serveren

Medarbejdere, der udfører ovenstående opgaver må ikke varetage opgaver i bogholderi eller kasse eller have ansvaret for beholdninger af varer m.v.

Ved ØSC medlemskab er det alene Økonomistyrelsen der står for udvikling af Navision Stat.

9. Særlige kontroller

Kravet om en personmæssig adskillelse mellem driftsafvikling (IT-afdelingen) og institutionens regnskabsopgaver kan være vanskelig at tilgodese for mindre institutioner med få administrative medarbejdere. Hvis denne adskillelse ikke er mulig, skal der efter samråd med institutionens departement eller hermed ligestillet myndighed og Rigsrevisionen i fornødent omfang etableres særlige kontrolforanstaltninger.

Med indførelse af elektroniske fakturering og NemKonto er løsningen udbygget med en Logging database og et transportlag som begge ligger udenfor Navision Stat databasen. Såvel transportlag som Logging database samvirker med Navision Stat databasen. Navision brugerens eneste adgang til Logging databasen er via link i Navision databasen, som automatisk indlægges af transportlaget ved indskrivning af et (modtaget eller sendt) eBilag i Logging databasen.

Da sende- og modtage-funktionen er afhængig af, at disse installationer på serveren kører, og da Navision brugeren ikke har adgang til at overvåge eller betjene servermiljøet, bør der etableres et formaliseret samarbejde mellem Navision brugere og IT afdelingen om overvågning af dokumenttransporten ind og ud af Navision.

Instruksen bør beskrive, hvorledes institutionen foretager overvågning af, at transporten af eBilag ind og ud fra serveren kører, således at det opdages hvis transport servicen ”går i stå” eller giver fejl.

Ved ØSC medlemskab henvises til Økonomistyrelsen for så vidt angår driftsafvikling af Navision Stat.

9.1 Modtagelse af eBilag via OIOSI

Der kan ikke på forhånd vides noget om hvornår elektroniske dokumenter ankommer. Institutionen er umiddelbart forpligtet til at have et system der løbende kan modtage elektroniske dokumenter. Institutionens tilmelding på OIO UDDI kombineret med OIO RASP dataudveksling via internettet sikrer dette.

De services der skal sørge for at institutionens regnskabssystem kan modtage dokumenter via OIOSI, skal være aktive. Institutionen bør overvåge at services er aktive således at der kan iværksættes procedure for genstart/fejlahjælpning.

Instruksen bør beskrive hvorledes institutionen sikrer sig mod tab af data som følge af at eBilag ikke kan modtages.

En medarbejder (Navision bruger) der har det som opgave, overvåger med passende interval Navision indbakke tabellerne for modtagne dokumenter og foretager nødvendig sagsbehandling. Denne manuelle overvågning kan ikke erstatte en systemunderstøttet overvågning.

Ved ØSC medlemskab henvises til Økonomistyrelsen for så vidt angår eBilag til Navision Stat.

9.2 Afsendelse af eBilag via OIOSI

Når en Navision bruger bogfører/usteder et salgsbilag, der skal sendes som eBilag, sender Navision Stat efter opslag på OIO UDDI direkte til modtager eller indirekte med OIO RASP protokollen via en OIOSI/VANS gateway til modtager.

I Navision Stat kan brugeren se om et givet afsendt eBilag er modtaget via en statusmarkering på det bogførte eller udstedte salgsbilag.

Hvis et dokument forbliver usendt, kan det skyldes, at den webservice, der skal foretage afsendelsen, ikke kører eller mangler rettigheder. Servicen bør overvåges og genstartes, hvis den er gået i stå. Dokumenter med status usendt vil blive sendt automatisk når servicen (gen)etableres.

Hvis dokumenter mislykkes i forsøg på afsendelse, kan det have flere årsager. Uanset årsagen kan den præcise årsag ses fra Navision.

Fejl der er relateret til serveropsætningen vil endvidere fremgå af event loggen. Der bør derfor etableres overvågning af de fejlhændelser, som servicen skriver i event loggen, når dokumenter får status mislykket. Dokumenter der er mislykket skal gensesendes af en Navision bruger, når fejlen er afhjulpet.

Instruksen bør indeholde en beskrivelse af, hvorledes institutionen sikrer sig at blive advaret, hvis data der er beregnet for afsendelse som eBilag 'strander' og ikke bliver afsendt.

Ved ØSC medlemskab henvises til Økonomistyrelsen for så vidt angår eBilag til Navision Stat.

9.3 Afsendelse af betalinger til Nemkonto via OIOSI og OIOSI/VANS gateway

Når et betalingsforslag i udbetalingskladden bliver godkendt og sendt i henhold til prokuraopsætningen, dannes der en betalingsordre i form af en xml-fil, der sendes til NKS via OIOSI. Transportlaget danner betalingsfilen på baggrund af data fra betalingsjournal- og betalingsposttabellen.

Navision-brugeren kan følge betalingens status via udbetalingskladden, menuen "Betalingsjournaler" og betalingsposttabellen i Økonomistyringsmodulet.

Betalingsstatus vil fremgå af felterne "NKS Journalstatus" og "NKS Fejlbeskrivelse" uanset om den er gået på fejl eller ej.

En medarbejder (Navision bruger) der har det som opgave, overvåger med passende interval betalingspost- og betalingsjournaltabellerne for modtagne retursvar og foretager nødvendig sagsbehandling. Denne manuelle overvågning kan ikke erstatte en systemunderstøttet overvågning.

De særregler, der aftales, skal fremgå af sikkerhedsinstruktionen.

Ved ØSC medlemskab henvises til Økonomistyrelsen for så vidt angår Afsendelse af betalinger til Nemkonto via OIOSI og OIOSI/VANS gateway til Navision Stat.

10. Navision Stat og følsomme persondata

Navision Stat indeholder ikke felter for en indeholdelse af følsomme persondata jvf. § 6, § 7 og § 8 i Lov om behandling af personoplysninger (Persondataloven). Institutioner, der ikke indgår i Økonomi Service Centret i Økonomistyrelsen, har dog mulighed for på egen hånd at bygge en betryggende logningsfunktionalitet, hvis eksisterende felter eller ny funktionalitet anvendes til den nye type data. I den forbindelse skal institutionerne indføre beskrivelser af nedenstående emner i sikkerhedsinstruksen.

10.1 Skrivning af følsomme persondata

Hvis der skrives følsomme persondata (jf. Persondataloven) i felter beregnet til andre formål, fx beskrivelses- og bemærkningslinje felterne, er det institutionens eget ansvar at bygge den nødvendige funktionalitet for begrænsning af adgang og tilhørende logning samt sørge for den korrekte anmeldelse til datatilsynet. I den forbindelse skal institutionerne være opmærksomme på følgende krav i DS 484: Kapitel 12 (Anskaffelse, udvikling og vedligeholdelse), kapitel 11 (Adgangsstyring), afsnit 10.10 (Logning) og afsnit 15.1.4 (Beskyttelse af personoplysninger).

Desuden skal institutionerne være opmærksomme på kravene i DS 484 afsnit 8.1.1 (Opgaver og ansvar) og 8.2.2 (Uddannelse, træning og oplysning om informationssikkerhed). Disse omhandler brugernes roller og ansvar og den løbende awareness.

10.2 Afsendelse af elektronisk salgsbilag fra Navision Stat

Såfremt en institution vælger at sende elektroniske salgsdokumenter indeholdende følsomme persondata, med udgangspunkt i lokal funktionalitet eller alternativ udfyldelse af standardfelter beregnet til andet formål, skal institutionen ligeledes sørge for at markere det sendte bilag med sikkerhedsniveau 2 eller 3, jvf. mulighederne i OIOUBL2.01 (Se også DS 484, 7.2.2 (Mærkning og håndtering af informationer og data)). Dette gælder hvad enten disse data fremgår direkte af selve salgsbilaget (faktura, kreditnota, rykker, kontoudtog eller applikation response) eller af eventuelle vedlagte bilag.

10.3 Modtagelse af elektroniske købsbilag i Navision Stat

Såfremt der modtages et eBilag med OIOUBL2.01 formatet, der er markeret som indeholdende følsomme persondata, fjernes disse oplysninger ved indlæsningen i Navision Stat, og adgangen til visningen af originalbilaget i Logging databasen begrænses. Samtidigt logges alle forsøg på adgang til originalbilag indeholdende følsomme persondata - autoriserede såvel som uautoriserede.

11. Nødplaner

Jf. DS 484, Kap. 4 (Risikovurdering- og håndtering) + 14 (Beredskabsstyring)

12. Sikkerhedsmæssige hændelser

Jf. DS 10.10 + evt. kapitel 13 (Styring af sikkerhedshændelser)