Region Midtjylland

Informationssikkerhedshåndbog

Retningslinjer

Region Midtjyllands regler for informationssikkerhed

1.0

11-03-2013

Indholdsfortegnelse

Retningslinjer

1 Indledning

Informationssikkerhedshåndbogen og Informationssikkerhedspolitikken udgør tilsammen de overordnede informationssikkerhedsmæssige rammer for Region Midtjylland. Informationssikkerhedspolitikken fastlægger det overordnede sikkerhedsniveau for Region Midtjylland. Informationssikkerhedshåndbogen beskriver og samler de retningslinjer, som Region Midtjylland skal følge for at sikre, at det ønskede sikkerhedsniveau kan efterleves.

Informationssikkerhedshåndbogen skal betragtes som et opslagsværk over de mest alment anerkendte it-sikkerhedsområder, som det er nødvendigetat forholde sig til for at kunne opnå et passende informationssikkerhedsniveau. Håndbogen følger ISO 27002, som er en international standard for informationssikkerhed, som Region Midtjylland har besluttet at følge ligesom Staten og mange andre danske offentlige organisationer og private virksomheder.

-

2 Termer og definitioner

I det følgende beskrives begreber som anvendes i Informationssikkerhedshåndbogen. Definitionerne er i videst mulig omfang hentet fra standard definitioner, men tilpasset Region Midtjylland hvor det er fundet nødvendigt og relevant.

Begreb	Definition/beskrivelse
Autenticitet	(Ægthed) dækker over det at noget (f.eks. en identitet eller en ressource) er det, som det giver sig ud for at være.
Autentifikation	Fastlæggelse af en autensitet. At man tjekker, at en person (eller en ressource) er den, som vedkommende hævder at være.
Autorisation	En (formel) tilladelse til at anvende programmer og/eller systemer med mere.
Beredskabsplaner	En beredskabsplan er et konkret plan, som kan anvendes operationelt af ledelse og medarbejder, hvis en ekstraordinær hændelse indtræffer og skal håndteres.
Databehandler	Den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert organ, der behandler oplysninger på den dataansvarliges vegne (fra Datatilsynets ordbog)

Dataejer	Dataejer har det grundlæggende ansvar for, at anvendelsen af en bestemt samling data sker i overenstemmelse med Informationssikkerhedspolitikken. Ofte vil systemejer være identisk med dataejer, men ikke i alle tilfælde. (jf. "Notat om Dataejer" - behandles på Informationssikkerhedsudvalgsmøde marts 2013)
Dataansvarlig	Den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af oplysninger (fra Datatilsynets ordbog)
Eksterne samarbejdspartnere	Defineres som alle typer af samarbejdspartnere som ligger uden for Region Midtjylland. Det kan f.eks. være kommuner og andre offentlige myndigheder, praktiserende læger, hosting firmaer, konsulent- og rådgivningsvirksomheder, outsourcing partnere m.v.
Fjernarbejdsplads	Fjernarbejdspladser dækker først og fremmest over arbejde, der sker fra medarbejderens hjem, men omfatter også arbejde, der foregår uden for Region Midtjyllands lokationer.
Fortrolighed	Fortrolighed vil sige, at følsom information ikke komme uvedkommende i hænde
Information Security Management System - ISMS	Det organisatoriske styringssystem. Tager sig af udarbejdelse af informationssikkerhedspolitik og retningslinjer samt gennemførelse af risikovurderinger og løbende opfølgning på informationssikkerhedsarbejdet. (Notat: Etablering af styringsmodel for informationssikkerhed")
Informationsaktiver	Informationsaktiver er de informationsbehandlingssystemer, data og procedure for behandling af data, som har væsentlig betydning for Region Midtjylland økonomisk, juridisk eller i anden forstand.
Informationssikkerhed	De samlede foranstaltninger til at sikre fortrolighed, tilgængelighed og integritet af regionens samlede informationsstrøm.

Informationssikkerhedsfunktionen	Informationssikkerhedsfunktionen har til opgave at overvåge, at informationssikkerhedspolitikken overholdes og at udarbejde de overordnede retningslinjer i overenstemmelse med informationssikkerhedspolitikken. Opgaverne løftes i fællesskab af Regionssekretariatet og It, hvor Regionssekretariatet varetager den organisatoriske del, mens It varetager den tekniske del.
Informationssikkerhedsudvalg	Udgør det taktiske og strategiske niveau for arbejdet med informationssikkerhed. Udvalget træffer de overordnede beslutninger vedrørende informationssikkerhed i Region Midtjylland
Integritet	Integritet vil sige, at data er korrekte og dermed ikke bliver ændret utilsigtet
It-sikkerhed	It-sikkerhed defineres som alle foranstaltninger til at sikre regionens it-systemer og elektroniske data.
It-sikkerhedschefen	Har ansvaret for at sikre at it-sikkerhedsniveauet er i overensstemmelse med det overordnede besluttede informationssikkerhedsniveau i Region Midtjylland. It-sikkerhedschefen har desuden ansvaret for at følge op på indrapporterede sikkerhedshændelser og for den daglige ledelse af it-sikkerhedsfunktionen.
It-sikkerhedsfunktion	It-sikkerhedsfunktionen er forankret i Ledelsessekretariatet i It-stab under it-sikkerhedschefen med direkte kontakt til It-chefgruppen og Informationssikkerhedsudvalget (ISU). Det er it-sikkerhedsfunktionens opgave at være konsulenter og rådgivere inden for it-sikkerhedsområdet samt udvikle it-sikkerhedsretningslinjer, udføre review og auditering af it-sikkerhed. Funktionen er samtidig it-afdelingens ambassadør for it-sikkerheden i Region Midt.
Konsekvensanalyse (samme som konsekvensvurdering)	Ved en konsekvensanalyse evalueres, hvilke forretningsmæssige konsekvenser det har for et informationssystem, hvis der sker brug på de tre effektområder inden for informationssikkerhed: tilgængelighed, fortrolighed og integritet

Kryptering	Processen at tage en besked og kode eller sløre, den, så den er ulæselig for uvedkommende, kaldes at *Kryptere.* At afkode en krypteret besked kaldes at *dekryptere.* Man skal have en "nøgle" for at kunne åbne og aflæse den oprindelige tekst.
Kryptografi	Læren om hemmeligholdelse af informationer. Se også Kryptering.
Mobil kode	Mobil kode er programmering, som angiver, hvordan programmer udveksler informationer. Typisk brugt af webudviklere, men også til skadelige formål. Programmerne er selvstartende og kan bruges til at overføre data fra en computer til en anden. Typiske mobile koder er Java applets, QR-tags, Active-X, Makroer, Scripts af forskellig art, Quick-time, JRE med mere.
Mobilt udstyr	Med mobilt udstyr menes bærbare pcere, smartphones og andet udstyr, der kan flyttes.
Personfølsomme oplysninger	Se under Personoplysninger.
Personhenførbareoplysninger	Se under Personoplysninger.
Personoplysninger	"Enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede) " jf. "Lov om behandling af personoplysninger" (Persondataloven) kapitel 2.
Privacy	Retten til privatliv og personlig frihed.
Procedure	En formaliseret arbejdsgang som kan være en proces eller en instruks.
Retningslinje	En udmøntning af Informationssikkerhedspolitikken der anviser, hvordan man skal forholde sig til et givent område.
Risikoanalyse	En risikoanalyse er en mere detaljeret analyse end en risikovurdering og gennemføres i en række sammenhænge som en naturlig del af det almindelige sikkerhedsarbejde, og når den overordnede risikovurdering begrunder det. Det kan være i forhold til et specifikt informationssystem, systemkomponent eller -ydelse (Vejledning om Risikovurdering fra It og Telestyrelsen 2007)

Risikovurdering	Risikovurdering er en systematisk måde at identificere, prioritere og styre ricisi relateret til anvendelse af alle typer informationssystemer.
Sikringsforanstaltninger	Sikringsforanstaltninger er alle de bestræbelser, forholdsregler og foranstaltninger, der gøres for at modvirke fejl (såvel tilsigtede som utilsigtede), tab og misbrug af data samt sikre, at data er tilgængelige for de personer, som skal anvende dem.
Systemadministrator	En person der har adgang til at rette i systemets opsætning m.m.
Systemejer	I Region Midtjylland repræsenterer systemejer det overordnede forretningsmæssige ansvar for det system, som vedkommende er systemejer for. (jf. "Notat om systemejers ansvar")
Sårbarhedsvurdering	Gennem en sårbarhedsvurdering får man overblik over, hvor godt Region Midtjylland er beskyttet over for hændelser gennem sikringsforanstaltninger, som Region Midtjylland allerede har. Det vil sige sandsynligheden for, at en hændelse indtræffer med de nuværende sikringsforanstaltninger.
Tilgængelighed	Tilgængelighed betyder, at data kan tilgås af de personer og systemer, der har behov for det, når de har behov for det.
Tredje part	Se under "eksterne samarbejdspartnere"
Trussel	En trussel er en potientiel årsag til en uønsket hændelse, der kan volde skade på Region Midtjylland.
Validering	Datavalidering er en sikring af, at medarbejder, kun indtaster defineret gyldige data i specifikke felter.

-

3 Håndbogens opbygning

Informationssikkerhedshåndbogen er opbygget efter ISO 27002 standarden, som er en international anerkendt standard for informationssikkerhed.

Afsnit 2 omfatter en ordliste over begreber, som anvendes i håndbogen i relation til informationssikkerhed.

Afsnit 4-15 rummer de sikringsområder regionen i henhold til god praksis og ifølge ISO 27002, standarden skal forholde sig til. Hvert afsnit kan rumme en eller flere sikringsforanstaltninger og er skrevet i så generelle termer som muligt. Under de enkelte afsnit henvises til relevante, uddybende retningslinjer, hvori det konkret beskrives, hvordan de sikkerhedsmæssige forhold skal efterleves.

Langt de fleste afsnit rummer emner med relevans for alle ledere og brugere af regionens It-systemer, dog kan der være afsnit, som primært er målrettet it medarbejdere og it-ledelse.

Retningslinjer, som er angivet i informationssikkerhedshåndbogen, skal vurderes i forhold til relevante forhold i Region Midtjylland, og fravigelser fra retningslinjerne kræver en dispensation.

-

4 Risikovurdering og -håndtering

Risikovurdering er en overordnet afvejning af de ricisi, Region Midtjylland kan være udsat for, når den benytter sig af informationsteknologi. Det kan f.eks. være tab af data, fejl i data eller at data kan tilgås af personer, som ikke har ret til at se data. Resultatet af vurderingen danner grundlag for beslutning om hvilke sikringsforanstaltninger, der skal gøres for at nedbringe risici på et for Region Midtjylland acceptabelt niveau.

Sikringsforanstaltninger er alle de bestræbelser, forholdsregler og foranstaltninger, der gøres for at modvirke fejl (såvel tilsigtede som utilsigtede), tab og misbrug af data. Det er også at sikre, at data er tilgængelige for de personer, som skal anvende dem.

Risikovurderingen lægger ikke op til, at der skal være informationssikkerhedsforanstaltninger for enhver pris. Den sikkerhed, ledelsen beslutter sig for, er en afvejning af mulige trusler op imod sandsynlighed og konsekvens af eventuel kompromittering sammenholdt med, hvor kritisk it-systemet er for organisationen

4.1 Vurdering af sikkerhedsrisici

På baggrund af risikovurderingen udarbejdes en handlingsplan som identificerer de områder, der skal have særlig opmærksomhed i forhold til at opretteholde det aftalte sikkerhedsniveau.

Overordnet risikovurdering	Der udføres en overordnet risikovurdering mhp. fastlæggelse af et acceptabelt risikoniveau i Region Midtjylland. Risikovurderingen opdateres mindst en gang om året. Risikovurderingen omfatter alle forretningskritiske it-systemer. Forretningskritiske it-systemer i Region Midtjylland vil sige it-systemer, som har stor udbredelse i organisation, og som vil medføre store produktionstab ved f.eks. et nedbrud. For alle øvrige it-systemer er systemejer ansvarlig for at tage stilling til, om der er behov for at foretage en risikovurdering. Ved udarbejdelse af risikovurdering anvendes standardiseret metode, der omfatter konsekvensanalyse, vurdering af trusler samt en sårbarhedsvurdering.

5 Overordnede retningslinjer

5.1 Informationssikkerhedsstrategi

Der arbejdes systematisk med informationssikkerhed i Region Midtjylland. Regionsrådet udstikker rammen for informationssikkerhed gennem den til enhver tid vedtagne informationssikkerhedspolitik. Informationssikkerhedsudvalget har ved den årlige risikovurdering ansvaret for udarbejdelse af en handlingsplan for arbejdet med informationssikkerhed. På operationelt niveau følger ansvar for sikkerhed linjeledelsen, der løbende er forpligtet til at støtte op om informationssikkerhedspolitikken og den overordnede handlingsplan samt prioritere ressourcer til arbejdet med informationssikkerhed i Region Midtjylland.

5.1.1 Formulering af informationssikkerhedspolitik

Informationssikkerhedspolitikken fastlægger det overordnede sikkerhedsniveau for Region Midtjylland. Derudover rummer den en beskrivelse af omfang, organisering og ansvarsplacering, sikkerhedsbevidsthed og beskrivelse af konsekvenser, hvis der sker brud på informationssikkerheden.

Der henvises til:

"Informationsikkerhedspolitik for Region Midtjylland"

Definition på informationssikkerhed	Informationssikkerhed defineres som de samlede foranstaltninger til at sikre fortrolighed, tilgængelighed og integritet af regionens samlede informationsstrøm. Fortrolighed vil sige, at følsom information ikke må komme uvedkommende i hænde. Tilgængelighed betyder, at data kan tilgås af de personer og systemer, der har behov for det, når de har behov for det. Integritet vil sige, at data er korrekte og dermed ikke bliver ændret utilsigtet It-sikkerhed defineres som værende alle foranstaltninger til at sikre regionens it-systemer og elektroniske data

Udarbejdelse af Informationssikkerhedspolitik	Informationssikkerhedsudvalget har ansvaret for at udarbejde Region Midtjyllands Informationssikkerhedspolitik og retningslinjer
Godkendelse af sikkerhedspolitik	Informationssikkerhedspolitikken godkendes af Regionsrådet
Dispensation fra informationssikkerhedspolitikken	It sikkerhedsfunktionen er bemyndiget til at træffe beslutning om midlertidige dispensationer fra informationssikkerhedspolitikken. Ansøgning om permanent dispensation fra informationssikkerhedspolitikken forelægges Informationssikkerhedsudvalget til afgørelse. (Kilde: ref. af Informationssikkerhedsudvalgsmøde okt. 2011)

5.1.2 Løbende vedligeholdelse

Informationssikkerhedspolitikken og tilhørende retningslinjer skal løbende vedligeholdes og opdateres.

Revision af sikkerhedspolitik	Informationssikkerhedsudvalget tager på grundlag af den løbende overvågning og rapportering fra it-sikkerhedsfunktionen Informationssikkerhedspolitikken op til revurdering en gang om året.

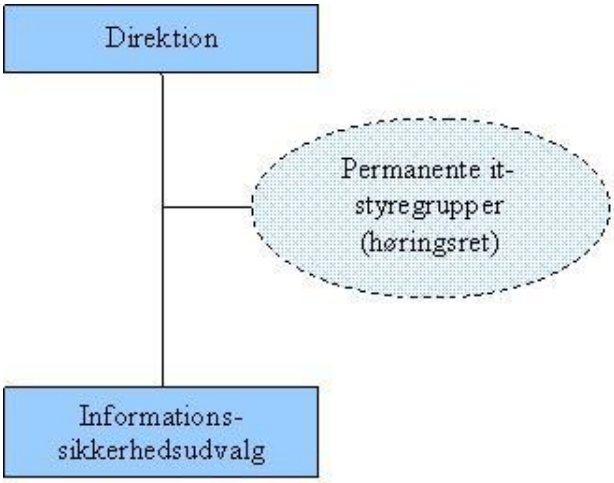
6 Organisering af informationssikkerhed

Entydig ansvarsplacering er vitalt for at sikre den fornødne opmærksomhed på informationssikkerhed. I det følgende beskrives det ledelsessystem, som er etableret i Region Midtjylland, ansvarsplacering samt krav til samarbejde med eksterne samarbejdspartnere.

6.1 Interne organisatoriske forhold

Det overordnede ansvar for informationssikkerheden i Region Midtjylland påhviler Direktionen. Der er derudover nedsat et informationssikkerhedsudvalg, der udgør det taktiske og strategiske niveau for arbejdet med informationssikkerhed. Udvalget træffer de overordnede beslutninger vedrørende informationssikkerhed i Region Midtjylland.

Beslutningsstruktur:



Der henvises i øvrigt til følgende, der ligger på Koncern Intra under Organisation og Informationssikkerhed:

"Styringsmodel for informationssikkerhed"

"Kommisorium for Informationssikkerhedsudvalget"

"Informationsikkerhedspolitik for Region Midtjylland"

"Systemejers ansvarsområde"

6.1.1 Ledelsens rolle

Ledelsens rolle	Det er ledelsens ansvar på alle organisatoriske niveauer i Region Midtjylland at implementere og understøtte Informationssikkerhedspolitikken og medvirke til at højne sikkerhedsbevidstheden og fastholde denne blandt Region Midtjyllands ansatte. Det er således ledelsens ansvar, at informationssikkerhedspolitikken overholdes. Det er ledelsens ansvar at vurdere, om der lokalt skal være et skærpet sikkerhedsniveau ift. den fælles informationssikkerhedspolitik (Kilde: Informationssikkerhedspolitikken)
Systemejers rolle	Systemejer repræsenterer det overordnede forretningsmæssige ansvar for et eller flere it-systemer og skal sikre, at håndtering af det pågældende it-system varetages i overenstemmelse med de gældende retningslinjer og informationssikkerhedspolitikken. Systemejers opgaver er beskrevet i notat "Systemejers ansvarsområder"

6.1.2 Koordinering af informationssikkerhed

Organiseringen af arbejdet med informationssikkerhed i Region Midtjylland kan opdeles i beslutningsstruktur og operationel struktur.

Sikkerhedsorganisation	Der er nedsat et Informationssikkerhedsudvalg bestående af den samlede Direktion, én ledelsesrepræsentant fra hhv. sundhedsområdet, psykiatri og socialområdet, administrationen, it-chefen og sekretariatschefen. Informationssikkerhedsudvalget udgør det taktiske og strategiske niveau for arbejdet med Informationssikkerheden. Udvalget træffer de overordnede beslutninger vedrørende Informationssikkerheden i Region Midtjylland Informationssikkerhedsudvalget har ansvaret for at informationssikkerhedspolitikken realiseres. På operationelt plan er der etableret en informationssikkerhedsfunktion i Region Midtjylland. Informationssikkerhedsfunktionens vigtigste opgave er at overvåge, at informationsikkerhedspolitikken overholdes og at udarbejde overordnede retningslinjer i overensstemmelse med informationssikkerhedspolitikken.
Koordination af informationssikkerheden	Informationssikkerhedsfunktionen varetages i fællesskab af Regionssekretariatet og It-sikkerhedsfunktionen, hvor Regionssekretariatet varetager den organisatoriske del, mens It-sikkerhedsfunktionen varetager den tekniske del. Regionssekretariatet koordinerer informationssikkerhedsindsatsen på overordnet niveau. I praksis sker styring i tæt samarbejde med It-sikkerhedsfunktionen.

6.1.3 Ansvarsplacering

Direktionen har det overordnede ansvar for informationssikkerheden i Region Midtjylland. Det er Informationssikkerhedsudvalgets ansvar at sikre, at informationssikkerhedsarbejdet forankres i organisationen. Den besluttede struktur for informationssikkerhed indebærer, at det operationelle ansvar for informationssikkerheden følger den almindelige ledelsesstruktur.

Det er linjeledelsens ansvar, at det løbende sikres, at de procedurer, standarder, retningslinjer og foranstaltningerm, der er beskrevet i Informationssikkerhedshåndbogen, gennemføres og efterleves.

Sikkerhedsansvar for informationsaktiver	Se afsnit 7.1

6.1.4 Godkendelsesprocedure ved anskaffelser

Der henvises til

"Indkøbspolitik for Region Midtjylland"

Anskaffelser	Anskaffelser skal følge Region Midtjyllands indkøbspolitik.

Anskaffelsesprocedurer	Anskaffelser må ikke give anledning til forøget risiko for sikkerhedshændelser, medmindre ledelsen accepterer den øgede risiko. Anskaffelse af it-systemer og services skal være i overensstemmelse med Informationssikkerhedspolitikken. Systemejer skal vurdere, om der bør foretages en risikovurdering inden anskaffelse for at sikre at politikken bliver overholdt.
Specifikation af sikkerhedskrav	Ved anskaffelse af nye it-systemer skal det være dokumenteret, at systemet lever op til Region Midtjyllands sikkerhedskrav. Anskaffelse sker iht. It's anskaffelsesprocedure. Systemet skal være vurderet af såvel Arkitektur og Design som sikkerhedsfunktionen.
Installation af programmer på arbejdsstationer	Kun udstyr og software, der er godkendt af It, supporteres af It. Privat udstyr supporteres ikke med mindre der foreligger en dispensation fra it-chefen

6.1.5 Tavshedserklæringer

Alle, der virker inden for det offentlige, hvad enten man er ansat eller på anden måde tilknyttet det offentlige, er underlagt krav om tavshedspligt jf. Forvaltningsloven kap. 8.

Der henvises til:

"Fortrolighedserklæring for eksterne samarbejdspartnere" på Koncern Intra
"Erklæring vedrørende tavshedspligt" på HRs hjemmeside

Medarbejdernes forpligtigelse i forhold til tavshedspligt	Alle medarbejdere i Region Midtjylland er underlagt Forvaltningslovens og Straffelovens bestemmelser vedrørende tavshedspligt. Det gælder såvel fastansatte og personer, som midlertidigt arbejder for Region Midtjylland, uanset om disse modtager vederlag herfor eller ej. Tavshedspligten ophører ikke ved fratræden.
Fortrolighedserklæring for eksterne samarbejdspartnere	Alle eksterne samarbejdspartnere (det kan f.eks. være leverandører, rådgivnings- og konsulentfirmaer), der har brug for at få adgang til Region Midtjyllands it-systemer og/eller data med henblik på at kunne udføre bestemte opgaver, skal underskrive en fortrolighedserklæring.
Indhold af fortrolighedserklæringerne	Fortrolighedserklæringen skal afgrænse, hvem der skal have adgang, samt hvilke it-systemer, der gives adgang til. Indholdet af fortrolighedserklæringen iøvrigt fastlægges af informationssikkerhedsfunktionen

6.1.6 Kontakt med myndigheder

Myndigheder skal i denne sammenhæng forstås som andre offentlige instanser. Ved brud eller mistanke om brud på sikkerheden skal man følge procedure for håndtering af bevismateriale og kontakt med politi og/eller relevante samarbejdspartnere.

I Region Midtjylland er det den nærmeste leder, som har ansvaret for, at medarbejderne overholder informationssikkerhedspolitikken og retningslinjerne herunder.

Der henvises til:

"Vejledning om bevissikring" (DI og DI ITEKs vejledning) på Dansk Industries hjemmeside og Its intranet.

Kontakt med relevante myndigheder	Kontakt til andre relevante myndigheder ved brud eller mistanke om brud på sikkerheden koordineres af It, Regionssekretariatet, HR eller den lokale linieledelse afhængig af situationen.

6.1.7 Fagligt samarbejde med grupper og organisationer

Samarbejde med relevante interne og eksterne interessegrupper og sikkerhedsorganisationer er nødvendig i forhold til at kunne sikre relevant videns- og erfaringsudveksling.

Information om nye trusler, virus og sårbarheder	It skal holde sig orienteret om eventuelle trusler mod de benyttede it-platforme og netværk. It er ansvarlig for eksternt samarbejde med de fornødne informationskanaler herunder samarbejde omkring it-sikkerhed med relevante eksterne interessegrupper og sikkerhedsorganisationer. It skal etablere en proces for identifikation af nye sårbarheder. Der skal udpeges en ansvarlig person eller gruppe for dette. It skal informere relevante personer i ledelsen om nye trusler, som potentielt kan berøre de pågældende forretningsenheder. It er ansvarlig for etablering af interne og eksterne netværk til sikring af fornøden information og vidensdeling samt opkvalificering af specifikke vidensområder.

6.1.8 Periodisk opfølgning

Det er vigtigt løbende at følge op på og sikre, at informationssikkerhedspolitik og retningslinjer overholdes, ligesom det kan være nødvendigt med faste intervaller til at opdatere politikken og retningslinjerne, såfremt vilkår eller trusselsbilledet ændrer sig.

Periodisk opfølgning	Informationssikkerhedsfunktionen sikrer, at der sker en periodisk opfølgning af informationssikkerhedspolitikken og retningslinjerne.

6.2 Eksterne samarbejdspartnere

Det udgør en risiko at give en samarbejdspartner adgang til Region Midtjyllands interne faciliteter (lokaler, serverrum, driftscentre etc.) og/eller informationssystemer. For at fastholde Region Midtjyllands sikkerhedsniveau skal alle former for samarbejde med eksterne samarbejdspartnere være baseret på en formel aftale.

Ved forretningskritiske it-systemer, herunder systemer der har særlig betydning for regionens økonomi eller som indeholder personfølsomme oplysninger, skal der desuden laves en risikovurdering. Ledelsen i den enhed, som indgår aftalen med eksterne samarbejdsparter, har ansvaret for at sikre, at de formelle sikkerhedskrav til samarbejdet er opfyldt.
Der henvises til

"It-sikkerhedsfunktionens overordnede principper for eksterne leverandørs remote support adgang til Region Midtjylland"
"Vejledning til adgang til Region Midts netværk og systemer"
"Retningslinje for eksternt samarbejde" (ultimo 2013)

6.2.1 Identifikation af risici i forbindelse med eksternt samarbejde

Ved samarbejde med andre parter, der har adgang til Region Midtjyllands informationsaktiver, skal der gennemføres en sikkerhedsvurdering, og relevante sikringsforanstaltninger skal identificeres og implementeres.

Der henvises til:

"Retningslinje for identifikation af risici i forbindelse med eksternt samarbejde" (ultimo 2013)

Eksterne samarbejdspartnere	Ved samarbejde med eksterne parter, som skal have adgang til Region Midtjyllands ressourcer, skal der gennemføres en risikovurdering og passende sikkerhedsforanstaltninger skal adresseres. Eksterne parter skal altid udfylde fortrolighedserklæringer enten som enkelt personer eller ved forud aftalt firmaerklæring. Sikkerhedsniveauet hos alle eksterne samarbejdspartnere skal som minimum leve op til Region Midtjyllands Informationssikkerhedspolitik
Outsourcing	Ved outsourcing af systemer til tredjepart skal der foreligge aftaler såsom SLA, Databehandleraftaler og evt. revisionserklæring, som kan dokumentere sikkerhedsniveau og -foranstaltninger samt dokumenterer, at Region Midtjylland lever op til sin tilsynspligt i overensstemmelse med bestemmelserne i Persondataloven. Systemejer for systemer, der er ekstern hostet, skal vurdere behovet for en revisionerklæring. Ved systemer, der hostes eksternt, og som har betydning for regionens økonomi og/eller indeholder personfølsomme data, skal leverandøren årligt leverer en revisionserklæring. Evt. fravalg af revisionerklæring for sådanne systemer skal godkendes af informationsikkerhedsudvalget. (Kilde: ISU ref. okt. 2011)

6.2.2 Sikkerhedsforhold i relation til borgere

For at Region Midtjylland kan give borgere adgang til Region Midtjyllands systemer og services, skal der foretages en risikovurdering. Det er linjeledelsens og projektlederens ansvar, at der er foretaget en sikkerhedsvurderingen af borgernes adgang til Region Midtjyllands systemer og services inden implementeringen.

Nedenstående opmærksomhedspunkter skal vurderes inden implementering.

Vejledning til adgang til Region Midts netværk og systemer skal følges ved adgang til Region Midtjyllands systemer og services, hvor det måtte være relevant i forhold til borgeradgang.

Når borgere får adgang skal man være opmærksom på:	Formålet med adgangen. Hvilke serviceydelser borgeren får adgang til. Region Midtjyllands ret til at overvåge og afbryde den aftalte serviceydelse. Henholdsvis Region Midtjyllands og borgerens ansvar. Tilstrækkelig beskyttelse af systemerne herunder af personoplysninger. Sikring af aftalt tilgængelighed for systemer og services. Adgangskontrolforanstaltninger skal som minimum følge Region Midtjyllands generelle retningslinjer for adgang til systemer. Adgang til systemer som indeholder personoplysninger skal ske på et sikkerhedsniveau, der svarer til en 2-faktor autentifikation.

6.2.3 Samarbejdsaftaler

Ethvert samarbejde skal være baseret på en formel aftale.
Der henvises til

"Fortrolighedserklæring for eksterne samarbejdspartnere" på Koncern Intra.
"Retningslinje for samarbejdsaftaler" (ultimo 2013)

Fortrolighedserklæring for eksterne samarbejdspartnere	Alle eksterne samarbejdspartnere (det kan f.eks. være leverandører, rådgivnings- og konsulentfirmaer), der har brug for at få adgang til Region Midtjyllands it-systemer og/eller data med henblik på at kunne udføre bestemte opgaver, skal underskrive en fortrolighedserklæring.
Tilgængelighedshændelser	Hændelser, der har indflydelse på tilgængelighed, skal afklares i henhold til gældende driftsaftaler (SLA). Driftshændelser, der ikke kan afklares inden for aftalt tid, skal udløse procedurer for hændelseshåndtering. De ramte brugere og systemejere skal informeres.

Samarbejdsaftaler med eksterne serviceleverandører	Ethvert samarbejde med en ekstern serviceleverandør skal formaliseres og være baseret på en samarbejdsaftale herunder udfærdigelse af SLA, fortrolighedserklæring og eventuel ekstern adgang til Region Midtjyllands netværk. Samarbejdsaftaler skal følge de retningslinjer, som er angivet i afsnit 6.2.1.

7 Styring af informationsrelaterede aktiver

Informationsaktiver er de informationsbehandlingssystemer, data og procedurer for behandling af data, som har væsentlig betydning for Region Midtjylland økonomisk, juridisk eller i anden forstand.

7.1 Identifikation af og ansvar for informationsrelaterede aktiver

Kritiske og væsentlige it-systemer skal dokumenteres, således at tilstrækkelige sikkerhedsforanstaltninger kan vurderes og iværksættes.

Der henvises til

"Systemejers ansvarsområde"

7.1.1 Fortegnelse over informationsaktiver

Der skal forefindes en fortegnelse over alle Region Midtjyllands forretningskritiske funktioner og processer. Ligeledes skal der forefindes en opdateret fortegnelse over Region Midtjyllands kritiske systemer og services.

Registrering af it-udstyr	Der skal vedligeholdes en liste over relevant udstyr, som er kritisk eller vitalt for Region Midtjyllands it-infrastruktur
Administration af internet-domænenavne	Der skal forefindes en liste over Region Midtjyllands registrerede domænenavne, status for brug, betalingsoplysninger og dato for fornyelse. Ansvaret for registrering af domænenavne ligger hos It.

7.1.2 Systemejer

I Region Midtjylland skal alle kritiske systemer have en systemejer. Systemejer repræsenterer det overordnede forretningsmæssige ansvar vedrørende it-systemer. Systemejer skal anlægge et helhedsorienteret perspektiv, der sikrer, at det pågældende it-system håndteres ud fra et koncernperspektiv og en helhedsbetragtning, således at håndtering af systemet varetages i overensstemmelse med overordnede politikker og strategier, koordineres ift. andre systemer og projekter, og at de relevante fora inddrages i henhold til den til enhver tid gældende beslutningsstruktur for it-området.

Systemejer skal være bekendt med notatet

"Systemejers ansvarsområde"

Ejerskab	Alle væsentlige eller kritiske it-systemer skal have udpeget en systemejer.
Sikkerhedsansvar for it-funktioner	Systemejer for forretningskritiske systemer skal identificeres og gøres opmærksom på sikkerhedsansvaret. Disse ejere skal have ansvar og beføjelser til at sikre tilstrækkelig beskyttelse.
Ansvar for adgangsrettigheder	Systemejer har ansvaret for at fastlægge og løbende revurdere adgangs- og brugsrettigheder.

7.1.3 Accepteret brug af aktiver

Accepteret brug af Region Midtjyllands aktiver har til formål at skitsere hvilke punkter, brugeren skal være opmærksom på ved anvendelsen af Region Midtjyllands it-systemer og netværk.

Kontrol af antivirus på arbejdsstationer	It skal sikre, at der er installeret antivirus på managed enheder. Medarbejdere skal løbende kontrollere, at antivirusprogrammet er aktivt og opdateret på deres enhed.
Mail indeholdende personoplysninger	Hvis man har behov for at sende personoplysninger elektronisk, skal det som udgangspunkt ske enten via Digital Post eller som en krypteret e-mail. Der findes dog en række undtagelser, hvor man kan sende direkte til modtageren, fordi krypteringen sker automatisk.

Hensigtsmæssig anvendelse af it-udstyr og data

Ved forsendelse af personoplysninger eller informationer, som anses for at være fortrolige, skal den enkelte medarbejder være opmærksom på eventuelle krypteringskrav.

I Region Midtjylland kan forsendelse af personoplysninger og informationer, der anses som fortrolige, sendes sikkert og beskyttet på flere forskellige måder.

Ved anvendelse af kommunikation over det åbne internet som for eksempel Messenger, Skype, Facebook eller lignende services skal deltagerne være opmærksomme på hvilke informationer, der udveksles under hvilke aftaler. Der må ikke udveksles personoplysninger på nogen former for sociale medier.

Brugerne skal generelt være opmærksomme på deres udstyr herunder hvorvidt udstyret fungerer hensigtsmæssigt. Eventuelle sikkerhedshændelser skal indberettes til Region Midtjyllands servicedesk.

Brugernavn og password er personlige og skal beskyttes, således at det ikke kommer andre i hænde. Hvis password er kommet andre i hænde eller er blevet misbrugt, skal adgangen lukkes straks, og passwordet efterfølgende ændres.

Ved driftsarbejde kan it-ansatte have behov for at tilgå brugerfiler og data i forbindelse med systemvedligeholdelse, undersøgelse eller revision. Det kan for eksempel være i forbindelse med undersøgelse af it-systemer, logfiler for fejl, netværksovervågning, undersøgelse af e-post der ikke er leveret, e-post som indeholder personoplysninger og ikke er beskyttet tilstrækkeligt, håndtering af virus- og spamfiltre, afklaring af ressourcebegrænsninger. Medarbejdernes private informationer skal behandles i overensstemmelse med persondataloven.

En brugers adgang til it-systemer skal løbende revideres i overensstemmelse med brugerens behov for adgang til respektive it-systemer. Det er linjeledelsens ansvar at sikre at It modtager relevante oplysninger om ændringer i ansattes ansættelsesmæssige og arbejdsmæssige forhold.

Uacceptabel brug af it-udstyr, it-systemer og data	Brud på acceptabel anvendelse er typisk brug, der negativt påvirker it-driften, arbejdsgangen, services eller administrative mål for Region Midtjylland og kan for eksempel være: Anvende en anden brugers bruger-id. Søge uautoriseret adgang til informationer om personer, brugerid, password, data eller lignende. Udfører aktiviteter som ikke overholder gældende lov og regulativer, herunder uautoriseret kopiering af ophavsretsligt materiale, brug af retsbeskyttet software uden licens eller formidling af uautoriserede kopier af retsbeskyttet software til andre. Bevidst forsøge at omgås it-sikkerhedsmetoder og operativsystemer eller undersøge sårbarheder i andre it-systemer eller på netværk. Anvende Region Midtjyllands it-systemer til privat, kommerciel brug. Det kan fx være reklame eller massedistribution af e-post, jf. ”Regler for brug af elektronisk post i Region Midtjylland”. I tilfælde hvor der kan konstateres en overtrædelse af Region Midtjyllands informationssikkerhedspolitik, eller hvor der er en begrundet mistanke om overtrædelse af Region Midtjyllands informationssikkerhedspolitik, skal linjeledelsen, servicedesk eller it-sikkerhedsfunktionen kontaktes.

7.2 Klassifikation af informationer og data

Aktiver i Region Midtjylland skal have et tilstrækkeligt beskyttelsesniveau for at sikre fortrolighed, integritet og tilgængelighed i henhold til klassifikation.

7.2.1 Klassifikation

Informationer i Region Midtjylland skal klassificeres, hvor det vurderes at være nødvendigt og relevant. Man skal være særlig opmærksom i forbindelse med håndtering af personoplysninger. Andre oplysninger end personoplysninger kan klassificeres som enten offentlige eller interne.

Informationer og data skal klassificeres som følger:	Offentligt: Materiale/data der altid frit må udleveres til offentligheden. Personoplysninger (følsomme oplysninger): Materiale/data som er relateret til et individ f.eks. en kunde, en borger, en patient eller en medarbejder. Internt: Materiale der anvendes til at løse arbejdsopgaver. Udlevering til andre interne eller eksterne parter beror i hvert tilfælde på en vurdering af, om vedkommende har ret til at se materialet. Det er ikke alle interne materialer/data, som er tilgængelige for alle medarbejdere.

7.2.2 Mærkning og håndtering af informationer og data

For at tydeliggøre klassifikationen af informationer skal de mærkes hvorvidt de er personoplysninger, følsomme eller offentlige.

Der henvises til følgende materialer, der findes på Koncern Intra:

"Beskyttelse af sager og dokumenter"
"Tjekliste ved journalisering"
"Sikkerhedspolitik for mobile it-enheder i Region Midtjylland"

Klassifikationsmærkning	Det skal i hvert enkelt tilfælde vurderes, om et informationsbærende medium, der indeholder personoplysninger (f.eks. dokumenter, papirudskrifter, billeder, filer m.v.), bør klassificeres og markeres f.eks. med en label (vandmærke el. lignende) (jf. afsnit 7.2.1).
Fortrolige data på mobile enheder	I Region Midtjylland skal alle smartphones og tablets, som anvendes i arbejdssammenhæng, registreres på et service- og sikkerhedsniveau. Personoplysninger eller interne data, som vurderes værende fortrolige, og som ønskes opbevaret på mobile enheder, skal beskyttes tilstrækkeligt ved kryptering.

8 Medarbejdersikkerhed

Medarbejderen udgør den vigtigste ressource for Region Midtjylland. Informationssikkerheden afhænger i høj grad af medarbejdernes viden om og engagement i forhold til sikkerhed før, under og efter, ansættelsesforholdet er ophørt.

8.1 Sikkerhedsprocedure før ansættelse

8.1.1 Opgaver og ansvar

Alle medarbejdere skal kende til og bidrage til, at Region Midtjyllands informationssikkerhedspolitik bliver overholdt.

Aftale om ansættelse	I forbindelse med aftale om ansættelse skal medarbejderen gøres bekendt med Region Midtjyllands informationssikkerhedspolitik og retningslinjer ved henvisning til Region Midtjyllands information på hjemmeside og intranet.

Medarbejderens ansvar	Medarbejderen skal kende til og bidrage til at overholde Region Midtjyllands retningslinjer og informationssikkerhedspolitik. Medarbejderen skal være opmærksom på at dele viden, skabe information og sikre, at information er tilgængelig uden at dette kompromitterer personfølsomme eller fortrolige oplysninger. (Kilde: IS politikken) Medarbejderen er ansvarlig for at rapportere sikkerhedshændelser og trusler, hvis der er mistanke om sådanne, til linjeledelsen, service eller til It-sikkerhedsfunktionen.
Samarbejdsaftaler med eksterne serviceleverandører	Ethvert samarbejde med en ekstern serviceleverandør skal formaliseres og være baseret på en samarbejdsaftale herunder udfærdigelse af SLA, fortrolighedserklæring og eventuel ekstern adgang til Region Midtjyllands netværk. Samarbejdsaftaler skal følge de retningslinjer, som er angivet i afsnit 6.2.1.

8.1.2 Efterprøvning

Umiddelbart før ansættelse af en medarbejder skal det sikres, at en række faktuelle forhold er i orden. Der foretages efterprøvning/screening af den kommende medarbejder i overenstemmelse med gældende lovgivning og regler. Det omfatter såvel fastansatte som midlertidigt ansatte medarbejdere.

I Region Midtjylland er det et krav, at der altid indhentes referencer, inden der træffes endelig beslutning om ansættelse. Det gælder også, når ansøgeren i forvejen er ansat indenfor samme arbejdsplads, men med en anden leder - eller i regionen i øvrigt. Der må kun tages reference, hvis ansøgeren har givet udtrykkeligt samtykke hertil.

Der henvises til Koncern HRs hjemmeside:
"Referencer - en vejledning til lederen"
"Retningslinje for indhentning af børne- og straffeattest"

Efterprøvning af medarbejdere kan omfatte	En personlig reference. Ansøgerens curriculum vitæ. Uddannelser og professionelle kvalifikationer. Korrekt autorisation (lovgivningskrav) I særlige tilfælde opholds- og arbejdstilladelse I forbindelse med ansættelser på institutioner og hospitaler skal der for en række personalegrupper indhentes børne- og/eller straffeattest
Verifikation af referencer	Region Midtjylland forbeholder sig ret til at verificere udvalgte referencer eller eksamensbeviser for betroede medarbejdere.

Baggrundstjek af konsulenter	Hvor konsulenter og vikarer tilknyttes gennem et bureau, skal der i kontrakten med bureauet være tydelige regler for bureauets forpligtelser i forbindelse med efterprøvning. Der skal være beskrevet regler for, hvorledes bureauet informerer Region Midtjylland, hvis der ved en efterprøvning findes oplysninger, der kan give anledning til bekymring.

8.1.3 Aftale om ansættelse

Den ansatte skal i forbindelse med ansættelsen eller hurtigst muligt efter opstart oplyses om sit ansvar og sine forpligtigelser i forhold til informationssikkerhed i henhold til gældende lovgivning, informationssikkerhedspolitikken, generelle og eventuelt lokale retningslinjer.

Rettigheder og ansvar afhænger af den enkeltes ansættelsessted, funktion og opgaver.

Der henvises til:

"Informationssikkerhedspolitik for Region Midtjylland"
Se iøvrigt på Koncern Intra om informationssikkerhed, retningslinjer og procedurer.

Medarbejdernes forpligtigelse i forhold til tavshedspligt	Alle medarbejdere i Region Midtjylland er underlagt Forvaltningslovens og Straffelovens bestemmelser vedrørende tavshedspligt. Det gælder såvel fastansatte og personer, som midlertidigt arbejder for Region Midtjylland, uanset om disse modtager vederlag herfor eller ej. Tavshedspligten ophører ikke ved fratræden.
Aftale om ansættelse	I forbindelse med aftale om ansættelse skal medarbejderen gøres bekendt med Region Midtjyllands informationssikkerhedspolitik og retningslinjer ved henvisning til Region Midtjyllands information på hjemmeside og intranet.
Ansættelsesaftalen skal indeholde:	Ansættelsesaftalen skal indeholde oplysninger om Region Midtjyllands behandling af personoplysninger om den ansatte jf. persondatalovens kapitel 8. Medarbejderens ansvar i forhold til overholdelse af tavshedspligt.

8.2 Ansættelsesforholdet

Det er vigtigt for Region Midtjyllands informationssikkerhed, at alle ansatte løbende er opmærksomme på eventuelle sikkerhedstrusler eller sårbarheder. Medarbejdere skal derfor oplyses om og i relevant omfang have uddannelse i informationsikkerhedsmæssige problemstillinger.

Når en medarbejder forfremmes eller får nye opgaver og derigennem kan få adgang til yderligere informationer eller systemer, skal der foretages en efterprøvning jf. afsnit 8.1.2.

8.2.1 Ledelsens ansvar

Ledelsens ansvar	Det er ledelsens ansvar, at alle medarbejdere er tilstrækkeligt informeret om deres roller og ansvar i forbindelse med sikkerhed, før de tildeles adgang til Region Midtjyllands systemer og data. At medarbejderen er gjort bekendt med nødvendige retningslinier, således at de kan leve op til Region Midtjyllands informationssikkerhedspolitik. At alle medarbejdere har et opmærksomhedsniveau i spørgsmål vedrørende informationssikkerhed, der er i overensstemmelse med deres roller og ansvar i Region Midtjylland. At alle medarbejdere holder sig inden for de retningslinier og bestemmelser, der er for ansættelsen, inkl. Region Midtjyllands informationssikkerhedspolitik og konkrete arbejdsmetoder.

8.2.2 Uddannelse og information

Alle ansatte i Region Midtjylland skal kende til og løbende informeres om informationssikkerhedspolitikken og gældende retningslinjer og procedurer.

Det sker bl.a. gennem informationssikkerhedskampagner, introduktionsforløb og i relevante uddannelsesforløb.

Uddannelse i sikkerhedspolitikken	Alle medarbejdere har adgang til relevant information om regionens Informationssikkerhedspolitik og fælles retningslinjer. Den lokale ledelse har ansvar for at sikre, at medarbejderne har det tilstrækkelige vidensniveau i forhold til informationssikkerhed. Træning af medarbejderne i Region Midtjyllands informationssikkerhedspolitik kan foregå ved inddragelse af forskellige formidlingsmetoder, eksempelvis ved hjælp af e-mail, plakater, rundskrivelser, møder eller kampagner.

8.2.3 Sanktioner

Brud på informationssikkerheden kan få ansættelsesretlige konsekvenser. Ved brud på informationssikkerheden anvendes reglerne for sanktioner i henhold til gældende lovgivning. Sanktioner vurderes altid udfra en konkret vurdering af hver enkelt sag.

Overtrædelse af sikkerhedsretningslinierne	Medarbejdere, som bevidst bryder informationssikkerhedspolitikken eller deraf afledte retningslinjer, vil kunne blive udsat for disciplinære forholdsregler i overensstemmelse med gældende regler og personalepolitik i Region Midtjylland.

8.3 Ansættelsens ophør

Det er vigtigt, at proces omkring ophør eller ændring af et ansættelsesforhold foregår både korrekt og betryggende for alle parter. Ansvar for proceduren ved medarbejderens fratrædelse skal være klart defineret og placeret. Det skal samtidig sikres, at alt udlånt udstyr returneres, og at den fratrådtes adgangsrettigheder ophører.

8.3.1 Ansvar ved ansættelsens ophør

Fratrædelse	Ved fratrædelse er det linjeledelsens ansvar at informere relevante instanser, herunder HR og It, om ansættelsens ophør, således at de almindelige procedurer i forbindelse med fratrædelsen kan foretages. Lederen har desuden ansvar for returnering af udleveret udstyr.

8.3.2 Returnering af aktiver

Medarbejderen skal aflevere alt udleveret udstyr ved samarbejdets ophør. Med aktiver menes alt, der har økonomisk værdi for Region Midtjylland - såvel materielt udstyr som immaterielle værdier.

Det er vigtigt, at relevant og vigtig viden, som den fratrådte medarbejder besidder, er dokumenteret og videregivet.

Aflevering af aktiver ved ansættelsens ophør	Ved fratrædelse skal medarbejderen aflevere alt, der tilhører Region Midtjylland. Nøglekort og evt. nøgler m.m., der giver fysisk adgang til lokaler i Region Midtjylland Dokumenter og andet materiale, der indeholder personfølsomme eller oplysninger, som må anses at være fortrolige. Pc'ere, telefoner, USB-nøgler og evt. andet udstyr, som tilhører Region Midtjylland.

8.3.3 Inddragelse af rettigheder

Adgangsrettigheder skal inddrages, når en medarbejder er fratrådt. Det er den nærmeste leders ansvar at sikre, at HR og It modtager relevante oplysninger om ændringer i ansættelses- og arbejdsmæssige forhold.

Der henvises til:
''**Retningslinje for elektronisk post, kalender og internet" på Koncern Intranet**
"Sikkerhedspolitik for mobile it-enheder" på Koncern Intranet

Inddragelse af rettigheder ved ansættelsens ophør	Adgangsrettigheder skal efter en nærmere angiven periode inddrages i forbindelse med en medarbejders opsigelse, dog senest ved fratrædelse (den sidste løndag). I særlige tilfælde kan it-sikkerhedschefen give dispensation. Ved fratrædelse skal alle brugerprofiler og systemrettigheder for brugeren øjeblikkeligt nedlægges. Ved fratrædelse eller længerevarende fravær skal lederen sørge for, at relevant information overdrages eller gøres tilgængeligt for andre, således at arbejdspladsen har adgang til information og data, der kan være nødvendige for at løse arbejdsopgaverne. Region Midtjylland forbeholder sig ret til at nulstille private mobilenheder ved samarbejdets ophør.

9 Fysisk sikkerhed

Fysisk sikkerhed og adgangsregler for gæster er naturlige elementer i Region Midtjyllands sikkerhedspolitik. Fysisk sikkerhed omfatter blandt andet døre, vinduer, alarmer samt tyverisikring af virksomhedens fysiske aktiver, eksempelvis it-udstyr. Systemer til adgangskontrol er ligeledes et element af fysisk sikkerhed, der sikrer, at kun personer med legalt ærinde får adgang til regionens område.

9.1 Sikre områder

Sikre områder vil sige områder eller lokaler i Region Midtjylland, hvor der er behov for etablering af fysisk/mekanisk sikring for at beskytte vigtige informationsbehandlingssystemer og lagringsmedier som f.eks. driftscentre, datafaciliteter og lign. Det er et ledelsesansvar at sørge for, at der etableres de nødvendige fysiske sikkerhedsforanstaltninger.

9.1.1 Fysisk afgrænsning

Døre til sikrede områder skal være aflåste.

Aflåsning af lokaler og bygninger	Alle døre til sikrede områder skal være aflåst.
Indbrudsalarmer	Der skal anvendes passende alarmsystem i alle lokaler med it-udstyr, der indeholder personoplysninger eller informationer, der vurderes at være fortrolige.
Distribueret it-udstyr	Driftscentre, serverrum, krydsfelter eller lignende faciliteter med delt it-udstyr skal aflåses for at hindre uautoriseret adgang.

9.1.2 Fysisk adgangskontrol

Fysisk adgangskontrol har til hensigt at sikre, at kun personer der har ret til det færdes på områder, hvor der ikke er offentlig adgang, har adgang. Region Midtjyllands driftscenter og datafaciliteter er underlagt specifikke retningslinjer.

Der henvises til:

"Retningslinje for adgangsforhold til Region Midtjyllands driftscenter og datafaciliteter" (april 2013)

Udlån af adgangskort	Håndværkere, teknikere og andet teknisk personale kan få udleveret adgangskort til udlån ved passende dokumentation.
Registrering af gæster	Gæster skal generelt ikke registreres i reception og lignende. Undtaget er driftscentre, serverrum og lignende faciliteter, hvor gæster skal registreres i overensstemmelse med gældende retningslinjer.
Gæsters adgang	Værten har ansvaret for gæsters færden.
Adgang for serviceleverandører	Serviceleverandører må i fornødent omfang få adgang til Region Midtjyllands it-ressourcer. Adgang skal dokumenteres og være tidsbegrænset. Eventuel dispensation kan gives af Region Midtjyllands it-sikkerhedschef.

9.1.3 Sikring af kontorer, lokaler og udstyr

Kontorer og andre lokaler, hvor der opbevares personfølsomme oplysninger eller informationer, der vurderes at være fortrolige, skal sikres mod uautoriseret adgang.

Sikring af kontorer, lokaler og udstyr	Kontorer og andre lokaler, hvor der opbevares personfølsomme oplysninger eller informationer, der vurderes at være fortrolige, skal sikres mod uautoriseret adgang f. eks. ved aflåsning, rydning af skrivebord og/eller fjernelse af fortrolige og følsomme informationer.

9.1.4 Beskyttelse mod eksterne trusler

Beskyttelse mod eksterne trusler har til formål at sikre Region Midtjyllands ressourcer på en hensigtsmæssig måde, således at data i tilfælde af utilgængelighed kan reetableres.

Der henvises til:

"Standard backup politik for Region Midtjylland"

Opbevaring af sikkerhedskopier på ekstern lokation	Der skal forefindes eksternt opbevaringssted for datamedier til retablering af forretningskritiske systemer. Eksternt opbevaringssted skal være i sikker afstand fra primært anlæg.

Fysisk sikring	Passende fysisk sikring herunder brandsikring skal forefindes.

9.1.5 Arbejdsmæssige forhold i sikre områder

Oplysninger om sikre områder	Informationer om sikre områder og deres funktion må alene videregives ud fra et arbejdsbetinget behov.
Overvågning i sikre områder	It skal sikre, at arbejde i sikre områder så vidt muligt overvåges.
Ubenyttede lokaler i sikre områder	Linjeledelsen har ansvaret for, at ubenyttede lokaler i sikrede områder er aflåste og inspiceres jævnligt .
Optageudstyr i sikre områder	Uautoriseret optageudstyr er ikke tilladt i sikre områder.

9.1.6 Områder til af- og pålæsning med offentlig adgang

Af- og pålæsningsområder samt andre områder, hvor offentligheden kan få adgang, skal vurderes i forhold til overvågning.

Af- og pålæsningsområder	Ved af- og pålæsningsområder samt andre områder, hvor offentligheden kan få adgang, skal det vurderes, om området er af en sådan karakter, at det skal være overvåget.

9.2 Beskyttelse af udstyr

It udstyr eller andet udstyr, hvorpå der behandles personfølsomme eller kritiske informationer, skal placeres eller beskyttes, så risikoen for skader og uautoristeret adgang minimeres.

Der henvises generelt til:

"Retningslinje for adgangsforhold til Region Midtjyllands driftscentre og datafaciliteter" (april 2013)

"Retningslinje for adgang til personfølsomme data"

"Retningslinje for nødprocedurer"

"Retningslinje for anvendelse af datamedier i Region Midtjylland"

9.2.1 Placering af udstyr

Det er vigtigt at overveje placering af udstyr for at undgå tab, ødelæggelse, tyveri eller kompromittering af Region Midtjyllands værdier eller forstyrrelse af Region Midtjyllands aktiviteter.

Der henvises generelt til:

"Retningslinje for adgang til Region Midtjyllands driftscentre og datafaciliteter" (april 2013)

"Retningslinje for adgang til personfølsomme data"

Miljømæssig sikring af driftscentre	Driftscentre, serverrum, krydsfelter og tilsvarende områder skal på forsvarlig vis sikres mod miljømæssige hændelser som brand, vand, eksplosion og tilsvarende påvirkninger.
Køling	Driftscentre og serverrum skal sikres med veldimensionerede airconditionanlæg.
Placering af udstyr	Udstyr skal placeres eller beskyttes, så risikoen for skader og uautoriseret adgang minimeres. Udstyr, der benyttes til at behandle kritiske/følsomme informationer, skal placeres, så informationerne ikke kan ses af uvedkommende. It skal begrænse fysisk adgang til gateways og trådløse adgangspunkter.
Beskyttelse mod udstråling	Udstyr, der benyttes til behandling af følsomme informationer, skal beskyttes mod udstråling for at undgå kompromittering.
Spisning og rygning i nærheden af udstyr	Der må ikke spises, drikkes eller ryges i nærheden af kritisk udstyr.

9.2.2 Forsyningssikkerhed

Alle forretningskritiske systemer skal beskyttes tilstrækkeligt, således at reetablering kan ske.

Der henvises til:

"Retningslinje for nødprocedurer"

Nødstrømsanlæg	Alle forretningskritiske systemer skal beskyttes med nødstrømsanlæg til at sikre hurtig og korrekt system-nedlukning i tilfælde af strømudfald.
Forsyningssikkerhed	Data-og telekommunikationsforbindelser skal etableres via minimum to adgangsveje for forretningskritiske systemer. It har ansvaret for, at alle forsyninger som elektricitet, vand, kloak, varme og ventilation har den fornødne kapacitet og løbende inspiceres for at forebygge uheld, der kan have indflydelse på centrale it-installationer.

9.2.3 Sikring af kabler

Kabler til datakommunikation skal beskyttes mod uautoriserede indgreb og skader.

Aflåsning af hovedkrydsfelter og lignende teknikrum	Alle krydsfelter og andre teknikrum skal være aflåste.
Sikring af kabler	Kabler til datakommunikation skal beskyttes mod uautoriserede indgreb og skader. Faste kabler og udstyr skal mærkes klart og entydigt. Dokumentation skal opdateres, når den faste kabelføring ændres.

9.2.4 Udstyrs og anlægs vedligeholdelse

Udstyr skal vedligeholdes for at sikre dets tilgængelighed og integritet.

Vedligeholdelse af udstyr og anlæg	Systemejer skal sikre, at udstyr bliver vedligeholdt efter leverandørens anvisninger. Region Midtjylland skal overholde fornødne sikkerhedskrav, hvis udstyr repareres eller vedligeholdes uden for Region Midtjylland. It er ansvarlig for, at der føres log over alle fejl og mangler samt reparationer og forbyggende vedligeholdelse. Kritiske og følsomme informationer skal beskyttes mod adgang på udstyr, som skal repareres eller vedligeholdes uden for Region Midtjylland, herunder skal det vurderes, hvorvidt data skal slettes inden reparation eller vedligeholdelse.

9.2.5 Sikring af udstyr uden for virksomhedens overvågning

Sikring af udstyr udenfor Region Midtjyllands overvågning handler primært om mobile enheder og hjemmearbejdspladser.

"Retningslinje til sikring af udstyr udenfor Region Midtjyllands overvågning" (ultimo 2013)

Brug af mobile enheder	Bærbart udstyr skal medbringes som håndbagage under rejser.
Opsyn med mobile enheder	Mobile enheder må ikke efterlades uden opsyn i uaflåste rum. Adgang til data på bærbare pc'ere, tablets, mobile enheder og andre enheder skal adgangsbeskyttes.
Sikring af distancearbejdspladser	Distancearbejdspladser og deres kommunikationsforbindelser skal beskyttes i forhold til de informationer og forretningssystemer, de benyttes til.

9.2.6 Sikker bortskaffelse eller genbrug af udstyr

Alt udstyr i Region Midtjylland skal kontrolleres i forhold til personfølsomt eller fortroligt indhold, og eventuel bortskaffelse eller genbrug skal ske i overensstemmelse med gældende lov.

Der henvises til:

"Retningslinje for anvendelse af datamedier i Region Midtjylland"

Bortskaffelse eller genbrug af udstyr	Retningslinje for sikker bortskaffelse af Region Midtjyllands udstyr skal følges.

9.2.7 Fjernelse af virksomhedens informationsaktiver

Udstyr eller medier, som indeholder personoplysninger eller intern vurderet fortrolige informationer må kun medbringes uden for Region Midtjyllands lokationer efter godkendelse fra linjeledelsen.

Udstyr eller medier	Udstyr eller medier, som indeholder personfølsomme oplysninger, eller data der vurderes at være fortrolige, skal behandles forsvarligt og sikres i henhold til pkt. 7.2.2 i Informationssikkerhedshåndbogen.

10 Styring af netværk og drift

Vedligeholdelse og opdatering af it-systemer er nødvendig for at opretholde et passende sikkerhedsniveau for virksomheden. Drift af it-systemer inkluderer elementer af overvågning af systemernes helbredstilstand, opdatering og sikkerhedskopiering af data. De fleste it-systemer i dag er afhængige af netværk, og derfor er administration, opbygning, sikring og vedligeholdelse af netværk vitalt for virksomheden. Den trussel, som uautoriseret adgang indebærer, gør det nødvendigt med klare regler for brugen af virksomhedens netværk samt overvågning af infrastrukturen.

10.1 Operationelle procedurer og ansvarsområder

For Region Midtjylland er sikker og stabil drift af informationsbehandlingssystemer og netværk vigtigt og kritisk. Der skal foreligge klare og dokumenterede retningslinjer og procedurer samt en entydig ansvarsfordeling. Der skal ligeledes foreligge godkendte driftsafviklingsprocedurer, der anvendes af it-driftspersonale.

10.1.1 Driftsafviklingsprocedurer

I Region Midtjylland dokumenteres driftsafviklingsprocedurer for forretningskritiske systemer på Its intranet.

Dokumentation	It skal løbende vurdere dokumentationsbehov for alle væsentlige systemer og it-relaterede forretningsgange.
Driftsansvar	It er ansvarlig for drift og administration af fælles it-systemer samt disses sikkerhed. Dette inkluderer efterlevelse af sikkerhedspolitikker, regler og procedurer. Den daglige drift varetages af driftsafdelingen, der har det overordnede ansvar for afviklingen.
Driftsafviklingsprocedurer	Driftsafviklingsprocedurer for forretningskritiske systemer skal være dokumenterede, ajourførte og tilgængelige for driftsafviklingspersonalet og andre med et arbejdsbetinget behov.

10.1.2 Ændringsstyring

Ændringsstyring (Change Management) sker gennem en formaliseret procedure. Ændringer bør kun gennemføres, når de er forretningsmæssigt velbegrundede.

Der henvises generelt til beskrivelser på It-drifts hjemmeside for change management og Its intranet.

Retningslinier for ændringer	Ændringer skal kun gennemføres, når de er forretningsmæssigt velbegrundede. It har ansvaret for, at der foregår en entydig identifikation og registrering af væsentlige ændringer. It har ansvaret for, at der findes en nødprocedure til at mindske effekten af fejlslagne ændringer.
Planlægning, test og godkendelse af ændringer	Ændringer skal planlægges og afprøves, inden de sættes i drift. Ændringer skal gennem en formaliseret godkendelsesprocedure inden drift.
Ændringsstyring	Ændringsstyringer skal følge angivelser fra It-drift vedrørende "Proces for forhåndsgodkendt ændring"; "Proces for nødændring" eller "Proces for ændringsanmodning" samt "Proces for data og -dokumentstyring".

10.1.3 Funktionsadskillelse

Det skal så vidt muligt sikres, at den samme person ikke har adgang til at tilgå, ændre og anvende informationsaktiver, uden at dette er godkendt. Samme person må ikke godkende og initiere en given handling. Funktionsadskillelse er en organisatorisk sikringsforanstaltning til minimering af risikoen for fejlagtig brug eller bevidst misbrug af systemer og medvirker til at minimere risikoen for uautoriserede eller utilsigtede hændelser. Dispensation skal dokumenteres.

Der henvises til:

"Retningslinje for funktionsadskillelse"

Sikring af forretningskritiske systemer	Forretningskritiske systemer skal beskyttes ved hjælp af funktionsadskillelse, således at risikoen for misbrug af privilegier minimeres.
Funktionsadskillelse: udvikling, test og drift	Der skal være funktionsadskillelse mellem udviklings-, test- og driftsmiljøer.

10.1.4 Adskillelse mellem udvikling, test og drift

Adskillelse mellem udvikling, test og drift skal sikres for at undgå uautoriseret adgang til og ændringer af Region Midtjyllands driftsmiljø.

Der henvises til:

"Retningslinje for adskillelse mellem udvikling, test og drift" (medio 2013)

Adgang til produktionsdata	Systemadministratorers adgang til fortrolige oplysninger skal begrænses og registreres. Produktionsdata må kun tilgås af autoriseret personale.
Sikring af applikationsudviklingsmiljøerne	Udviklingsmiljøer skal sikres mod trusler som uautoriseret adgang, ændringer og tab. Data skal sikres efter klassifikation.
Adskillelse af udvikling, test og drift	Udviklings- og testmiljøer skal være systemteknisk eller fysisk adskilt fra driftsmiljøet.

10.2 Ekstern serviceleverandør

Ved samarbejde med eksterne leverandører skal Region Midtjyllands sikkerhedsniveau opretholdes. Sikkerhedsniveauet skal kunne dokumenteres, verificeres og løbende kunne overvåges.

Der henvises til:

"Vejledning til adgang til Region Midtjyllands netværk og systemer"

"Vejledning til eksterne leverandørers remote support adgang"

10.2.1 Serviceleverancen

Serviceleverance betyder, at der indgåes gensidige aftaler om det ønskede serviceniveau, Aftalerne dokumenteres i formelle Service Level Agreements (SLA).

Samarbejdsaftaler med eksterne serviceleverandører	Ethvert samarbejde med en ekstern serviceleverandør skal formaliseres og være baseret på en samarbejdsaftale herunder udfærdigelse af SLA, fortrolighedserklæring og eventuel ekstern adgang til Region Midtjyllands netværk. Samarbejdsaftaler skal følge de retningslinjer, som er angivet i afsnit 6.2.1.

10.2.2 Overvågning og revision af serviceleverandøren

Indgåede aftaler skal løbende overvåges og gennemgås. Det kan for eksempel være analyse af rapporter og logs fra serviceleverandøren. Kontrol kan være en revision som sikrer at aftaler overholdes, herunder at sikkerhedshændelser bliver håndteret som aftalt.

Overvågning af serviceleverandøren	It skal regelmæssigt overvåge serviceleverandørerne, gennemgå de aftalte rapporter og logninger samt udføre egentlige revisioner for at sikre, at aftalen overholdes, og at sikkerhedshændelser og -problemer håndteres på betryggende vis.

10.2.3 Styring af ændringer hos ekstern serviceleverandør

Region Midtjylland skal sikre sig, at ændringsstyringer hos ekstern serviceleverandører harmonerer med Region Midtjyllands retningslinjer for ændringsstyring.

Styring af ændringer hos serviceleverandøren	It skal sikre, at ændringsstyring af serviceleverandørens ydelser er på samme sikkerhedsniveau som Region Midtjyllands.

10.3 Styring af driftsmiljøet

Områderne i It-drift forestår processerne omkring styring af driftsmiljøet.

10.3.1 Kapacitetsstyring

Driftsplanlægning og overvågning binder It-drifts mange forskellige ydelser og opgaver sammen til en samlet it-serviceleverance for brugerne. Kapacitetsstyring er ikke implementeret i Region Midtjylland for nuværende, mens overvågning af specifikke systemer kan bestilles i It af systemejer.

Kapacitetsplanlægning	It-systemernes dimensionering skal afpasses efter kapacitetskrav. Belastning skal overvåges således, at opgradering og tilpasning kan finde sted løbende. Dette gælder især for forretningskritiske systemer.
Kapacitetsovervågning	Alle serversystemer med kritiske informationer skal løbende overvåges for tilstrækkelig kapacitet for at sikre pålidelig drift og tilgængelighed.

10.3.2 Godkendelse af nye eller ændrede systemer

Godkendelse af nye eller ændrede systemer følger faste procedurer i It-drift.

Sikring af serversystemer	Alle servere skal opfylde alle krav, der angives af It's afdeling for Driftsplanlægning og Overvågning inden idriftssættelse.
Godkendelse af nye eller ændrede systemer	Godkendelse af nye eller ændrede systemer sker gennem Change Management i Region Midtjylland it drift Driftsplanlægning og Overvågning.

10.4 Skadevoldende programmer og mobil kode

Der skal være implementeret foranstaltninger mod skadelig kode på alle arbejdspladser, servere og andre netværksopkoblede enheder ejet af Region Midtjylland. Foranstaltninger mod skadelig kode har til formål at sikre Region Midtjylland mod tab og misbrug af data samt at medvirke til sikring af driftsstabilitet, data integritet og tilgængelighed.

Der henvises til:

"Retningslinje for håndtering af skadelig kode i Region Midtjylland"

10.4.1 Beskyttelse mod skadevoldende programmer

Der skal være etableret forebyggende, opklarende og udbedrende sikrings- og kontrolforanstaltninger som beskyttelse mod skadevoldende kode.

Region Midtjyllands brugere skal have fornøden uddannelse og information omkring foranstaltninger mod skadevoldende kode.

Der henvises til:

"Retningslinje for beskyttelse mod skadevoldende programmer" (medio 2013)

Kontrol af antivirus på arbejdsstationer	It skal sikre, at der er installeret antivirus på managed enheder. Medarbejdere skal løbende kontrollere, at antivirusprogrammet er aktivt og opdateret på deres enhed.
Spam-mail beskyttelse	Region Midtjylland bortfiltrerer e-mails, der opfylder Region Midtjyllands kriterier for spam-mails. Medarbejderne skal udvise forsigtighed med deres brugeridentitet i forbindelse med videregivelse af eksempelvis mailadresser samt i forbindelse med modtagelsen af uønskede e-mails.

Spyware	Installation af spyware søges undgået gennem begrænsningerne i muligheder for softwareinstallation. Installation af spyware søges undgået gennem patch-management-processer. It skal sikre, at der regelmæssigt scannes for spyware på alle arbejdsstationer.
Automatisk indholdsfiltrering	Systemerne skal jævnligt scannes for spam- og phishing-mails. Disse mails mv. skal sættes i karantæne automatisk.
Antivirus-produkter på servere	Der skal være installeret beskyttelse mod skadelig kode på alle systemer, hvor dette er muligt. Eventuelle undtagelser skal dokumenteres.

10.4.2 Beskyttelse mod mobil kode

Mobil kode er programmering, som angiver, hvordan programmer udveksler informationer. Typisk brugt af webudviklere, men også til skadelige formål. Programmerne er selvstartende og kan bruges til at overføre data fra en computer til en anden. Typiske mobile koder er Java applets, QR-tags, Active-X, Makroer, Scripts af forskellig art, Quick-time, JRE med flere.

Se iøvrigt afsnit 10.4.1.

Der henvises til :

"Retningslinje for beskyttelse mod mobil kode" (medio 2013)

Antivirus-produkter på arbejdsstationer	It skal sikre, at der er installeret aktive antivirus-produkter på samtlige computere i Region Midtjylland, og at disse opdateres højst et døgn efter leverandørens opdateringer.
Beskyttelse mod mobil kode	Anvendelse af mobil kode som QuickTime, ActiveX, Java, JRE og Adobe skal begrænses og løbende sikkerhedsvurderes.

10.5 Sikkerhedskopiering

Alle systemer, der er placeret i et af regionens driftscentre, skal være omfattet af backup rutiner.

Der henvises til:

"Standard backup politik for Region Midtjylland"

10.5.1 Sikkerhedskopiering

Region Midtjyllands standard backup politik anvendes for alle systemer, som er placeret i et af Region Midtjyllands driftscentre.

Overvågning af procedurer for sikkerhedskopiering	Muligheden for at retablere data fra backup-systemer skal regelmæssigt aftestes i et testmiljø. Endvidere skal retablering testes efter system- eller proces-ændringer, der kan påvirke backup-rutiner.
Beredskabsplaner for sikkerhedskopiering	Alle forretningskritiske systemer skal have en nødplan for sikkerhedskopiering, således at risikoen for tab af data minimeres.
Opbevaring af sikkerhedskopier på ekstern lokation	Der skal forefindes eksternt opbevaringssted for datamedier til retablering af forretningskritiske systemer. Eksternt opbevaringssted skal være i sikker afstand fra primært anlæg.
Sikkerhedskopiering af data på serversystemer	It er ansvarlig for opbevaring og sikkerhedskopiering af alle forretningskritiske informationer på serversystemer, som er placeret i et af Regionens driftscentre.

10.6 Netværkssikkerhed

Netværkssikkerhed varetages af Its netværksafdeling (RMnet) som varetager ethernet baserede netværk i Region Midtjylland samt netværksservices.

Dokumentation forefindes på www.net.rm.dk

10.6.1 Netværket

Its netværksafdeling (RMnet) har driften af Region Midtjyllands netværk og diverse netværksrelaterede services. Netværksafdelingen forestår leverandørkontakt vedrørende regionens netværksforbindelser til eksterne parter og forestår planlægning og implementering af netværksomlægning/modernisering på de lokale netværk.

Sikring af netværk	It har det overordnede ansvar for at beskytte Region Midtjyllands netværk.
Tilslutning af udstyr til netværk	Det er tilladt, at ansatte kobler udstyr til netværket efter aftale med It. Udstyret må ikke forstyrre driften, og It kan kræve det frakoblet.
Adgang til aktive netværksstik	Adgang til aktive netværksstik skal styres af It. It skal sikre, at der ikke er ubenyttede aktive netværksstik i offentligt tilgængelige rum som reception, kantine og lignende. Netværksadgang skal kontrolleres og styres af It. Kun nødvendige adgange må være aktive i infrastrukturen. Alle øvrige skal være lukket ned. Netværksstik i offentligt tilgængelige områder må kun aktiveres, når dette er forretningsmæssigt begrundet.
Indkommende netværksforbindelser	Der må kun etableres forbindelser fra internet til Region Midtjyllands netværk efter forudgående godkendelse fra It's netværksafdeling eventuel suppleret med godkendelse fra It-sikkerhedsfunktionen.

Brug af trådløse lokalnetværk	Brug af trådløse netværk tillades og autoriseres efter arbejdsmæssigt behov. Region Midtjyllands managed enheder kan tilgå Region Midtjyllands autoriserede trådløse netværk, mens andre enheder kan gives tilladelse til at anvende gæstenet med begrænsede services. Enhver opsætning af trådløse netværk skal godkendes af it-sikkerhedsfunktionen.
Placering af trådløse netværk	Opsætning af udstyr til trådløst netværk må kun forbindes til den eksisterende infrastruktur, når der foreligger en sikkerhedsvurdering og godkendelse.
Adgang til trådløst produktionsnetværk	Brugere skal autentificeres ved hjælp af et certifikat, før der gives adgang til Region Midtjyllands trådløse netværk, f.eks. ved hjælp af IEEE 802.1x.
Gæsters brug af Region Midtjyllands trådløse netværk	Netværket kan og må kun anvendes til internetadgang. Gæster og eksterne konsulenter, hvis identitet er kendt, kan få tidsbegrænset adgang til gæstenettet efter forudgående godkendelse og dokumentation.

10.6.2 Netværkstjenester

Its netværksafdeling (RMnet) har driftsansvaret for regionens datanetværk og diverse netværksrelaterede services.

Netværksleverandøren skal kunne levere:	De nødvendige teknologiske muligheder for autentifikation, kryptering og overvågning. De nødvendige tekniske opsætninger til at sikre opkoblinger i overensstemmelse med samarbejdsaftalen mellem netværksleverandøren og Region Midtjylland. Adgangskontrol der sikrer mod uvedkommendes adgang.
Firewall-funktioner på servere	Alle servere skal benytte firewalls til at sikre, at der kun gives adgang til nødvendige services.

10.7 Databærende medier

Databærende enheder skal altid klassificeres og beskyttes efter deres indhold samt anvisninger i pkt. 7.2.2.

Der henvises til:

"Retningslinje for anvendelse af datamedier i Region Midtjylland"

10.7.1 Bærbare datamedier

Der skal foreligge passende procedurer for modtagelse, registrering, behandling, opbevaring, forsendelse og sletning af bærbare datamedier som for eksempel magnetbånd, disketter, flytbare diske, usb-stik, flashcards, cdere og dvd samt lignende medier.

Der henvises til:

"Retningslinje for anvendelse af datamedier i Region Midtjylland"

Bortskaffelse og genbrug af medier	I Region Midtjylland skal der træffes særlige forholdsregler, således at informationer på medier ikke kan genskabes af uvedkommende. Dette kan ske ved, at medier afleveres til InterGen efter aftale eller på anden vis ved overholdelse af gældende retningslinjer. Brugte datamedier (cd'er, disketter, backup bånd, harddiske og papirudskrifter) skal kasseres, således at indholdet af datamediet ikke kan læses af uvedkommende. Det er ikke tilstrækkeligt, at data bliver slettet eller formateret. Data kan genskabes ved hjælp af specielprogrammer. Det er derfor nødvendigt at anvende specialudstyr til destruktion af data eller ødelægge datamediet, således det ikke er muligt at læse data fra dem. Hvis dataindholdet indeholder personfølsomme data eller fortrolige data skal datamediet destrueres på en måde, som overholder persondataloven, og det bør overvejes at foretage en sikker destruktion af mediet.
Brug af datamedier	Anvendelsen af datamedier skal følge angivelserne i "Retningslinje for anvendelse af datamedier i Region Midtjylland".

10.7.2 Destruktion af datamedier

Databærende medier skal destrueres i overensstemmelse med klassificering af data på mediet. Der skal tages særlige foranstaltninger i anvendelse, når det drejer sig om fortrolige og specielt personoplysninger.

Der henvises til:

"Retningslinje for anvendelse af datamedier i Region Midtjylland"

Bortskaffelse eller genbrug af udstyr	Retningslinje for sikker bortskaffelse af Region Midtjyllands udstyr skal følges.

10.7.3 Beskyttelse af datamediers indhold

Databærende mediers indhold skal beskyttes tilstrækkeligt og i overensstemmelse med indholdets karakter. Personoplysninger skal altid være krypterede eller anonymiserede.

Der henvises til:

"Retningslinje for anvendelse af databærende medier i Region Midtjylland"

Udskrivning	Printere, som benyttes til udskrivning af personfølsomme oplysninger eller informationer, som har karakter af fortroligt, skal søges placeret i lokaler, der ikke generelt er offentligt tilgængelige. Materiale med personfølsomme eller fortrolig information skal afhentes umiddelbart efter udprint. Forefindelse af uafhentet materiale skal placeres i skraldespande for fortrolige data.
Beskyttelse af følsomme og fortrolige data på datamedier	It skal etablere procedurer, der sikrer datamediers indhold mod uautoriseret adgang og misbrug af mediernes indhold.

10.7.4 Beskyttelse af systemdokumentation

Systemdokumentation skal beskyttes i overensstemmelse med indholdsmæssig klassifikation jvf. afsnit 7.2.

Lagring og adgangsrettigheder til systemdokumentation	Systemdokumentation opbevares i mindst 5 år.
Beskyttelse af systemdokumentation	It skal opbevare systemdokumentation passende sikkert. Adgangsrettigheder til systemdokumentation skal holdes på et minimum.

10.8 Informationsudveksling

Informationsudveksling skal beskyttes med tilstrækkelige foranstaltninger for at forhindre, at kritiske, fortrolige eller personfølsomme informationer bliver offentliggjort, misbrugt eller slettet.

Der henvises til:

"Retningslinje for anvendelse af datamedier i Region Midtjylland"

10.8.1 Informationsudvekslingsretningslinjer og -procedurer

Der skal foreligge retningslinjer og procedurer for enhver form for informationsudveksling, hvor det er relevant. Man skal være særlig opmærksom ved udveksling af personoplysninger.

Udlevering af personoplysninger	Ved udlevering af personoplysninger skal det sikres, at relevant lovgivning er overholdt. Der skal være tale om sagligt formål, og opmærksomheden henledes på krav om samtykke. Der henvises til Offentlighedsloven og Persondataloven. Interne informationer, som vurderes at være fortrolige, må kun udleveres i krypteret form.
Brug af kryptering i forbindelse med dataudveksling	Personoplysninger og interne informationer, der vurderes at være fortrolige, må kun udveksles i krypteret form. Der skal være implementeret tilstrækkelige muligheder for kryptering af data, således at udveksling af data kan beskyttes på en tilstrækkelig måde.
Kryptering af administrative netværksforbindelser	Netværksforbindelser, der benyttes til system-vedligeholdelse, skal altid krypteres. Dette gælder alt udstyr undtagen terminaler med direkte forbindelse til systemer.
Udskrivning	Printere, som benyttes til udskrivning af personfølsomme oplysninger eller informationer, som har karakter af fortroligt, skal søges placeret i lokaler, der ikke generelt er offentligt tilgængelige. Materiale med personfølsomme eller fortrolig information skal afhentes umiddelbart efter udprint. Forefindelse af uafhentet materiale skal placeres i skraldespande for fortrolige data.

10.8.2 Aftaler om informationsudveksling

Der skal foreligge aftaler om informationsudveksling, hvad enten udvekslingen sker fysisk eller elektronisk. Aftalens sikringsforanstaltninger skal være i overensstemmelse med klassifikationen af de informationer, der udveksles, og deres forretningsmæssige betydning.

Aftaler om informationsudveksling	Ved udveksling af information og software imellem Region Midtjylland og evt. tredjepart skal der foreligge en aftale herom.

10.8.3 Fysiske datamediers sikkerhed under transport

Fysiske datamedier skal sikres tilstrækkeligt under transport for at undgå tab, misbrug og utilgængelighed eller ændring.

Der henvises til:

"Retningslinje for anvendelse af datamedier i Region Midtjylland"

Brug af bærbare medier til fortrolige data	Fortrolige informationer skal krypteres, når de opbevares eller transporteres på bærbare medier, f.eks. USB-stik, PDA, cd, dvd eller disketter.

10.8.4 Elektronisk post og dokumentudveksling

Der henvises til:

"Retningslinje for post, kalender og internet i Region Midtjylland" på Koncern Intranet

"Retningslinjer for formater ved udveksling af elektroniske dokumenter" på Koncern Intranet

Mail indeholdende personoplysninger	Hvis man har behov for at sende personoplysninger elektronisk, skal det som udgangspunkt ske enten via Digital Post eller som en krypteret e-mail. Der findes dog en række undtagelser, hvor man kan sende direkte til modtageren, fordi krypteringen sker automatisk.
Klassifikationsmærkning	Det skal i hvert enkelt tilfælde vurderes, om et informationsbærende medium, der indeholder personoplysninger (f.eks. dokumenter, papirudskrifter, billeder, filer m.v.), bør klassificeres og markeres f.eks. med en label (vandmærke el. lignende) (jf. afsnit 7.2.1).
Spam-mail beskyttelse	Region Midtjylland bortfiltrerer e-mails, der opfylder Region Midtjyllands kriterier for spam-mails. Medarbejderne skal udvise forsigtighed med deres brugeridentitet i forbindelse med videregivelse af eksempelvis mailadresser samt i forbindelse med modtagelsen af uønskede e-mails.
Automatisk indholdsfiltrering	Systemerne skal jævnligt scannes for spam- og phishing-mails. Disse mails mv. skal sættes i karantæne automatisk.
Elektronisk udveksling af post og dokumenter	Hvis e-mail bruges til juridisk bindende aftaler, skal de underskrives med en digital signatur. Elektronisk udveksling af dokumenter, regneark og præsentationer bør som udgangspunkt gemmes i pdf-format inden videredistribution. Alle færdige dokumenter, der skal sendes eksternt, skal sendes i pdf-format.

10.8.5 Virksomhedens informationssystemer

Region Midtjylland betjener sig af en række kommunikationsmedier for at dække medarbejdernes, samarbejdsparternes og omverdenens informationsbehov: papir, elektronisk post, intranet, fælles kalendersystem, internet, almindelig post og telefax. Efterhånden som vægten på disse medier ændrer sig og integrationen øges, opstår der nye risici, som virksomheden skal forholde sig til. Der skal derfor være retningslinjer for brug og integration af virksomhedens informationssystemer.

Integration af informationssystemer	Hvis integration af informationssystemer resulterer i en forøget risiko, skal denne vurderes og godkendes af ledelsen.

10.9 Elektroniske forretningsydelser

Region Midtjylland oplever en stigende tendens til, at der udvikles it-services til borgerne. Disse it-services skal beskyttes i overensstemmelse med Region Midtjyllands informationssikkerhedspolitik.

10.9.3 Offentligt tilgængelige informationer

Ved offentligt tilgængelige systemer, som eksempelvis en hjemmeside, er der ingen begrænsninger i brugeradgang og ingen form for brugeraftaler.

Informationsindholdet skal derfor nøje vurderes, og det er ledelsens ansvar, at det kun er informationer, som må offentliggøres, der bliver offentliggjort. Der skal endvidere være stærke beskyttelsesforanstaltninger mod uautoriserede ændringer.

Offentlig tilgængelig information	Det er systemejer og It som har ansvaret for, at offentlige tilgængelige informationer som f. eks. på Region Midtjyllands web-server er passende beskyttet mod uautoriserede ændringer.

10.10 Logning og overvågning

Logning og overvågning anvendes blandt andet til registrering af uautoriserede adgangsforsøg, performance og kontrol i overensstemmelse med angivelserne i Sikkerhedsbekendtgørelse nr. 528 af 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.

Der henvises til:

"Retningslinjer for logning"

"Retningslinje for tidssynkronisering" (ultimo 2013)

10.10.1 Opfølgningslogning

Alle brugeraktiviteter, afvigelser og sikkerhedshændelser skal logges og opbevares i en fastlagt periode af hensyn til opfølgning på adgangskontroller og eventuel efterforskning af fejl og misbrug.

Overvågning af internet-brug	Den enkelte medarbejders anvendelse af internettet bliver logget. Virksomheden filtrerer og begrænser internetadgang.

Hændelseslogning	Alle produktionssystemer skal logge information om adgang og forsøg på adgang, for at kunne spore uautoriseret aktivitet. Logfiler skal regelmæssigt gennemgås af relevante medarbejdere i It. Alle sikkerhedshændelser skal logges og opbevares i en fastlagt periode af hensyn til opfølgning på adgangskontroller og eventuel efterforskning af fejl og misbrug.
Opfølgningslogning	It skal logge sikkerhedshændelser på Region Midtjyllands systemer. It skal logge væsentlige brugeraktiviteter på Region Midtjyllands systemer.
Opbevaring af opfølgningslog	It skal opbevare logregistreringer i overensstemmelse med systemets klassificering og øvrige forhold så som periode for opbevaring af data.

10.10.2 Overvågning af systemanvendelse

Brugen af Region Midtjyllands informationsbehandlingssystemer skal overvåges og løbende følges op. Niveauet for overvågning skal fastlægges ud fra en risikovurdering og lovgivningens krav.

Overvågning af internetforbindelser	It skal løbende overvåge internetforbindelser med henblik på at detektere elektroniske angreb. Logfiler skal opbevares og gennemgås regelmæssigt.
Overvågning af netværk	It er ansvarlig for kontinuerligt at overvåge brugen og sikkerheden af Region Midtjyllands netværksinfrastruktur. It-drift er ansvarlig for identificering, diagnosticering, løsning og rapportering af hændelser samt for samarbejde med andre interessenter. Der skal være opdateret overvågning af al kritisk netværkstrafik i Region Midtjylland.

10.10.3 Beskyttelse af log-oplysninger

Som udgangspunkt skal en log aldrig ændres. Man kan derfor ikke tale om autoriserede ændringer. Hvis der er fejl i en log, må eventuelle korrektioner fremgå af efterfølgende logninger.Både log-faciliteter og log-oplysninger, skal beskyttes mod manipulation og tekniske fejl. Der henvises iøvrigt til Sikkerhedsbekendtgørelsen nr. 528.

Beskyttelse af log-oplysninger	Log-faciliteter og log-oplysninger skal beskyttes mod manipulation og tekniske fejl.

10.10.4 Administrator- og operatørlog

Aktiviteter udført af systemadministratorer og -operatører samt andre med særlige rettigheder skal logges.

Administratorlog	Der skal foretages logning af alle handlinger udført af personer med administratorrettigheder i forbindelse med systemkomponenter (inklusive netværksudstyr).

10.10.5 Fejllog

Systemejer har sammen med It ansvaret for, at fejl logges og analyseres, således at udbedringer og modforholdsregler kan vurderes og gennemføres. Både brugerrapporterede og systemregistrerede fejl skal fremgå af fejlloggen.

Fejllog	Fejl skal logges og analyseres, og nødvendige udbedringer og modforholdsregler skal gennemføres. Regelmæssig gennemgang af fejlloggen for at sikre, at alle fejl er rettet tilfredsstillende. Regelmæssig gennemgang af de korrigerende og kompenserende foranstaltninger for at sikre, at Region Midtjyllands sikkerhed ikke er blevet kompromitteret, og at de gennemførte foranstaltninger er autoriseret.

10.10.6 Tidssynkronisering

En præcis tidsangivelse kan være kritisk i forbindelse med indgåelse af bindende aftaler, realtidstransaktioner eller efterforskning ved hjælp af logningsinformationer.

Alle ure i Region Midtjyllands intern hostede kritiske it-systemer skal være synkroniseret med en præcis tidsangivelseskilde.

Der henvises til:

"Retningslinje for tidssynkronisering" (ultimo 2013)

Tidssynkronisering	It skal sikre, at systemers ure jævnligt synkroniseres til korrekt tid. Der skal udvælges centrale tidsservere på det interne netværk, som skal synkronisere med eksterne tidssignaler. Øvrige interne servere skal synkronisere med de centrale interne tidsservere.

11 Adgangsstyring

Adgangen til at udføre handlinger på Region Midtjyllands it-systemer beskyttes af autorisationssystemer. Systemerne har til formål at sikre mod uautoriserede ændringer, bestillinger, fejl og svindel. Region Midtjyllands medarbejdere er medvirkende til beskyttelse af informationsaktiverne gennem korrekt brug af autorisationssystemerne.

Der henvises til:

"Retningslinje for straksaktivering" (medio 2013)

"Retningslinje for password"

"Retningslinje for systemadministrators password"

"Retningslinje for tildeling af udvidede adgangsrettigheder for RM it" (april 2013)

"Retningslinje for tildeling af administrator rettigheder for personale ved RM-it" (april 2013)

"Retningslinje i tildeling af nyt bruger password i Region Midtjylland"

"Retningslinje for adgang til personfølsomme data"

"Sikkerhedspolitik for mobile enheder"

"Juridiske vilkår for brugere af bronze serviceniveau"

"Retningslinje for autentifikation af brugere med ekstern netværksforbindelse" (ultimo 2013)

"Retningslinje for fjernarbejdsplads" (medio 2013)

"Vejledning til adgang til RMs netværk og systemer

11.1 De forretningsmæssige krav til adgangsstyring

Brugerstamdatakataloget (BSK) er regionens centrale it-løsning til håndtering af adgange til regionens fælles it-systemer. Visionen er, at BSK på baggrund af viden om medarbejderens rolle og organisatoriske tilknytning automatisk tildeler en række adgange til it-systemer, som medarbejderen kan tage i brug allerede på første arbejdsdag. Når en medarbejder forlader Region Midtjylland, skal BSK tilsvarende sikre, at medarbejderens systemadgange lukkes. BSK er således med til at sikre rettidig, effektiv brugeradministration og øget sikkerhed i regionen.

Der henvises til:

"Retningslinje for straksaktivering" (medio 2013)

"Retningslinje for password"

"Retningslinje for tildeling af nyt bruger password i Region Midtjylland"

"Retningslinje for tildeling af udvidede adgangsrettigheder for RM it" (april 2013)

"Retningslinje for til af administrator rettigheder for personale i Region Midtjylland" (april 2013)

"Din nye pc-arbejdsplads"

11.1.1 Retningslinjer for adgangsstyring

Der skal foreligge dokumenterede og ajourførte retningslinjer for Region Midtjyllands adgangsstyring.

Adgangsbegrænsning til informationer	Systemer bør have adgangskontrol implementeret for at hindre uautoriseret adgang til data og funktionalitet. Detailopsætning og specificering afhænger af form og indhold af data dokumenteret i risikoanalysen af systemet.
Retningslinier for adgangsstyring	Systemejere har det overordnede ansvar for at etablere og vedligeholde procedurer for adgangsstyring for hvert system.
Tildeling af brugerrettigheder	Systemejer fastlægger principper for tildeling af de nødvendige brugerrettigheder for systemet.
Administratorbeskyttelse	Der skal anvendes en særskilt systemadministratoradgang til alle systemer.
Administration af arbejdsstationer	Som udgangspunkt har medarbejderne ikke administrative rettigheder til deres pc'er.
Brugerprofiler for konsulenter og deltidsansatte	Personer, som er ansat eller har konsulentaftale og har behov for adgang til Region Midtjyllands it-systemer, skal tildeles personlig brugerID. Det samme gælder for vikarer og timelønnede. Ophører samarbejdet, ansættelses- eller vikaraftale, skal brugerprofilen øjeblikkeligt nedlægges.
Fratrædelse	Ved fratrædelse er det linjeledelsens ansvar at informere relevante instanser, herunder HR og It, om ansættelsens ophør, således at de almindelige procedurer i forbindelse med fratrædelsen kan foretages. Lederen har desuden ansvar for returnering af udleveret udstyr.
Når borgere får adgang skal man være opmærksom på:	Formålet med adgangen. Hvilke serviceydelser borgeren får adgang til. Region Midtjyllands ret til at overvåge og afbryde den aftalte serviceydelse. Henholdsvis Region Midtjyllands og borgerens ansvar. Tilstrækkelig beskyttelse af systemerne herunder af personoplysninger. Sikring af aftalt tilgængelighed for systemer og services. Adgangskontrolforanstaltninger skal som minimum følge Region Midtjyllands generelle retningslinjer for adgang til systemer. Adgang til systemer som indeholder personoplysninger skal ske på et sikkerhedsniveau, der svarer til en 2-faktor autentifikation.

11.2 Administration af brugeradgang

Administration af brugeradgang har til formål at sikre autoriserede brugeres adgang og forhindre uautoriserede adgange til Region Midtjyllands systemer.

Administration af brugeradgang dækker formaliserede forretningsprocesser for tildeling og nedlæggelse af adgang.

11.2.1 Registrering af brugere

Der skal forefindes procedure for tildeling og fjernelse af brugeradgange.

Der henvises til:

"Vejledning til adgang til RMs netværk og systemer"

Registrering af brugere	Brugere skal have unikt RegionsID. Adgangsrettigheder skal afstemmes med de forretningsmæssige behov. Der skal ske en verifikation af, at rettighedsniveauet er i overensstemmelse Region Midtjyllands generelle sikkerhedsretningslinier. Brugere skal modtage en bekræftelse af de tildelte rettigheder. Serviceleverandørerer skal anvende tilsvarende eller samme autorisationsprocedure som Region Midtjylland. Systemejer skal sikre, at systemet kan vedligeholde brugerfortegnelser. It skal fastlægge procedurer for, hvordan bruger-ID eller rettigheder fjernes eller ændres ved ophør eller ændring af brugeres jobfunktion. Adgangsrettigheder må ikke krænke eventuelle krav om funktionsadskillelse. Autorisation til brugeradgang skal godkendes af linjeledelsen.
Medarbejderes omplacering	Medarbejdernes rettigheder og privilegier skal revurderes ved ændringer i ansættelsen i forbindelse med omplacering, ændrede arbejdsopgaver, organisationsændringer med mere.
Skift af administratoradgangskode ved fratrædelse	Hvis en medarbejder med kendskab til fælles administrative adgangskoder fratræder, skal disse adgangskoder ændres med det samme.

11.2.2 Udvidede adgangsrettigheder

En tildeling af udvidede adgangsrettigheder skal begrænses og overvåges.

Der henvises til:

"Retningslinje tildeling af administratorrettigheder for personale ved RM-it"

"Retningslinje for tildeling af administratorrettigheder for personale i Region Midtjylland"

"Retningslinje for tildeling af udvidede adgangsrettigheder for RM it" (april 2013)

Administratorbeskyttelse	Der skal anvendes en særskilt systemadministratoradgang til alle systemer.
Ændring af administrative adgangskoder	Administrative adgangskoder skal ændres hvert kvartal. Administrative adgangskoder skal ændres, hvis udenforstående får kendskab til disse, herunder hvis administratorer forlader Region Midtjylland.
Udvidede adgangsrettigheder	De udvidede adgangsrettigheder må kun tildeles i begrænset omfang og alene ud fra et arbejdsbetinget behov. De udvidede adgangsrettigheder skal registreres. De udvidede adgangsrettigheder må ikke sættes i kraft, før den fornødne autorisation er indhentet. Automatiserede systemtekniske processer skal anvendes i videst muligt omfang for at begrænse behovet for tildeling af udvidede rettigheder. De enkelte brugerprogrammer skal, så vidt muligt, tilrettelægges, så de begrænser behovet for indgreb med udvidede rettigheder.

11.2.3 Adgangskoder

Tildeling af adgangskoder skal ske ved en formaliseret proces.

Der henvises til:

"Retningslinje for passwords"

"Retningslinje for systemadministratorers password"

"Retningslinje ved skift af adgangskode"

Retningslinier for adgangskoder	It skal etablere og vedligeholde en procedure for, hvordan en brugers identitet fastslås, før en ny midlertidig adgangskode må udleveres. Ved brugeroprettelse eller nulstilling af adgangskode skal brugere tildeles en sikker, midlertidig adgangskode, som skal ændres umiddelbart før første anvendelse. Midlertidige adgangskoder skal være unikke og opfylde de almindelige krav til adgangskoder.

Autentificering ved adgang til netværket	Adgangen til det interne netværk fra andre lokationer end Region Midtjyllands skal være adgangskodebeskyttede. Fjernadgang til det interne netværk skal beskyttes med tilstrækkelige sikkerhedsforanstaltninger såsom autentificering, VPN med individuelle certifikater og TACACS .
Adgangskoder er strengt personlige	Adgangskoder er strengt personlige og må ikke deles med andre. Adgangskoder skal ændres, hvis andre får kendskab til dem.
Overdragelse af adgangskode	Ved overdragelse af adgangskoder må brugernavn ikke fremgå samtidig.
Rapportering af sikkerhedshændelser	Adgangskoder må aldrig lagres elektronisk i klartekst.
Sikring af kritiske data	It skal ændre standardadgangskode efter installation af et nyt system.

11.2.4 Periodisk gennemgang af brugernes adgangsrettigheder

Adgangsrettigheder skal gennemgåes med jævne mellemrum for at sikre, at der kun forefindes autoriserede adgange til Region Midtjyllands informationsaktiver.

Gennemgang af brugerprofiler	Alle brugerprofiler bør gennemgås mindst en gang årligt for at identificere inaktive profiler eller tilsvarende, der skal fjernes eller ændres.

11.3 Brugerens ansvar

Brugerne i Region Midtjylland skal gøres opmærksom på deres ansvar i forhold til personlige adgange til Region Midtjyllands systemer.

11.3.1 Brug af adgangskoder

Der henvises til:

"Retningslinje for passwords"

Krav til skift af adgangskode	Adgangskoder skal skiftes mindst en gang om året.
Valg af sikre adgangskoder	Det er brugerens ansvar at vælge tilstrækkeligt sikre adgangskoder i adgangskontrolsystemerne.

Krav til indhold af adgangskode	Adgangskoder skal indeholde kombinationer fra mindst tre af følgende kategorier: store bogstaver, små bogstaver, tal og specialtegn. Der må ikke benyttes brugernavn, navn eller datoer som en del af adgangskoden.
Krav til længde af adgangskode	Adgangskoder skal indeholde mindst 8 tegn.
Genbrug af adgangskode	Samme adgangskode bør ikke genbruges på interne og eksterne systemer.
Brug af autologin funktioner	Der må ikke anvendes automatiserede log-on processer for eksempel ved anvendelse af makroer, scripts eller lignende, som indeholder adgangskode.
Ændring af administrative adgangskoder	Administrative adgangskoder skal ændres hvert kvartal. Administrative adgangskoder skal ændres, hvis udenforstående får kendskab til disse, herunder hvis administratorer forlader Region Midtjylland.

11.3.2 Uovervåget udstyr

Uovervåget udstyr skal sikres tilstrækkeligt - specielt hvis udstyret ikke er placeret i særligt sikrede lokaler.

Brug af adgangskodebeskyttet pauseskærm	Alle arbejdsstationer aktiverer automatisk skærmlås, som It har defineret. Af hensyn til sikkerheden bør alle brugere dog aktivere skærmlåsen, når de forlader arbejdsstationen f.eks. i forbindelse med frokostpauser.

11.3.3 Beskyttelse af datamedier på den personlige arbejdsplads

Datamedier skal beskyttes i overensstemmelse med deres klassificering i forhold til indholdet af informationer.

Der henvises til:

"Anvendelsen af datamedier i Region Midtjylland"

Opbevaring af fysiske dokumenter	Papirdokumenter med personfølsomme oplysninger skal opbevares i aflåst rum, skuffe eller skab. Skriveborde skal ryddes for fortrolige dokumenter senest ved arbejdsdagens afslutning. Dokumenter må gerne ligge fremme, såfremt kontorlokaler er aflåste.

Udskrivning	Printere, som benyttes til udskrivning af personfølsomme oplysninger eller informationer, som har karakter af fortroligt, skal søges placeret i lokaler, der ikke generelt er offentligt tilgængelige. Materiale med personfølsomme eller fortrolig information skal afhentes umiddelbart efter udprint. Forefindelse af uafhentet materiale skal placeres i skraldespande for fortrolige data.

11.4 Styring af netværksadgang

Netværksadgang styres af It og der henvises til beskrivelser under pkt. 10.6

11.4.1 Retningslinjer for brug af netværkstjenester

Brugerne skal kun have adgang til de netværksservices, de er autoriseret til at tilgå.

Netværkstjenester driftes af It. Der henvises til nærmere beskrivelser på Its intranet.

Retningslinier for brug af netværkstjenester	Brugere skal kun have adgang til de tjenester, de er autoriseret til at benytte. It har ansvaret for, at der findes en fortegnelse over de netværk og tjenester, der må tilgås.
Installation af netværksudstyr	Det er ikke tilladt at installere netværksudstyr uden forudgående sikkerhedsgodkendelse fra It's netværksafdeling.

11.4.2 Autentifikation af brugere med ekstern netværksforbindelse

Brugere med ekstern netværksforbindelse til Region Midtjyllands systemer skal autentificeres i overensstemmelse med klassifikationen af de informationer, forbindelsen giver adgang til. Ved adgang til personoplysninger eller fortrolige informationer bør der gives adgang svarende til en 2-faktor autentificering.

Der henvises til:

"Retningslinje for autentifikation af brugere med ekstern netværksforbindelse" (ultimo 2013)

Indkommende netværksforbindelser	Der må kun etableres forbindelser fra internet til Region Midtjyllands netværk efter forudgående godkendelse fra It's netværksafdeling eventuel suppleret med godkendelse fra It-sikkerhedsfunktionen.

11.4.3 Identifikation af netværksudstyr

Brug af automatisk identifikation af netværksudstyr	It skal etablere automatisk identifikation af netværksenheder på netværkssegmenter, hvor det er væsentligt, at kommunikationen kun må ske fra specifikt udstyr eller specifik lokation.

11.4.4 Beskyttelse af diagnose- og konfigurationsporte

Diagnose- og konfigurationsporte skal være beskyttede mod uautoriserede tilgang, således at fysiske og logiske adgange kan kontrolleres.

Beskyttelse af diagnose- og konfigurationsporte	Fysisk og logisk adgang til diagnose- og konfigurationsporte skal kontrolleres.

11.4.5 Opdeling af netværk

Netværkets opbygning håndteres, udvikles og styres af It-drift. Der henvises til beskrivelser på Its intranet.

Opdeling af netværk	It skal segmentere netværk for at etablere en passende adskillelse mellem forskellige tjenester, brugergrupper eller systemer. Mindstekrav til netværkssegmentering er, at It etablerer en "demilitariseret zone" (DMZ), hvor offentligt tilgængelige servere placeres adskilt fra internt tilgængelige servere.

11.4.6 Styring af netværksadgang

For at undgå uautoriseret anvendelse af fælles netværk og hertil knyttede tjenester skal brugernes adgang styres i overensstemmelse med netværkets fælles adgangsretningslinjer og forretningsbetingede krav.

It-drift har ansvaret for styring af netværksadgange i Region Midtjylland.

Styring af netværksadgang	Der skal implementeres et automatiseret adgangskontrolsystem.

11.4.7 Rutekontrol i netværk

It-drift har driftsansvaret for implementering, udvikling og vedligeholdelse af netværket i Region Midtjylland herunder rutekontrol. Der henvises generelt til beskrivelser på Its intranet.

Rutekontrol	It skal begrænse rutning mellem forskellige netværkssegmenter, således at kun nødvendig trafik videresendes. It skal sikre passende netværks- eller node-autentificering til ethvert netværkssegment.

11.5 Styring af systemadgang

Styring af systemadgang har til formål at sikre, at der udelukkende er autoriserede adgange til Region Midtjyllands systemer.

11.5.1 Sikker log-on

Sikker log-on	Systemadgang skal beskyttes af en sikker log-on-procedure.

11.5.2 Identifikation og autentifikation af brugere

Alle brugere i Region Midtjylland skal have en RegionsID til personlig brug og der skal vælges passende autentifikationsmetode til verifikation af brugerens identitet.

Identifikation og autentifikation af brugere	Alle brugere skal have en unikt RegionsID til personligt brug. Der skal benyttes en passende autentifikationsteknik til verifikation af brugernes identitet. Brugeridentiteten skal kunne spores til den person, som er ansvarlig for en given aktivitet. Der må ikke anvendes fælles adgangskoder eller brugerprofiler. It-sikkerhedschefen kan dispensere.

11.5.3 Styring af adgangskoder

Styring af adgangskoder skal overholde angivelser i "Retningslinje for passwords".

Systemer til styring af adgangskoder	Så vidt muligt skal der benyttes it-systemer, der automatisk kan styre de krav, der findes til adgangskoder.

11.5.4 Brug af systemværktøjer

Brug af systemværktøjer skal begrænses til et arbejdsbetinget behov.

Brug af systemværktøjer	It skal begrænse og styre adgangen til systemværktøjer f.eks. utilities, der kan påvirke eller omgå systemers eller enheders sikkerhed. It skal sikre, at unødige systemværktøjer ikke er installeret eller tilgængelige på brugeres pc'er. It skal sikre, at brugen af systemværktøjer begrænses til et minimum af betroede og autoriserede brugere. Der skal være en procedure for autorisation ved ad hoc anvendelse af systemværktøjer. Al brug af systemværktøjer skal logges. It skal definere, hvem der er autoriseret til at anvende hvilke systemværktøjer. Hvor funktionsadskillelse er påkrævet, må brugere ikke have adgang til både systemværktøjer og brugersystemer.

11.5.5 Automatiske afbrydelser

Der skal, hvor det er muligt, implementeres foranstaltninger, som foretager automatisk afbrydelse efter en passende periode af inaktivitet.

Automatiske afbrydelser	Systemejer skal vurdere, om det er nødvendigt at implementere automatisk afbrydelse af funktioner i et system, som ikke har været aktivt i et fastlagt tidsrum.

11.5.6 Begrænset netværksforbindelsestid

Specielt for forretningskritiske systemer skal det vurderes, hvorvidt der skal indføres begrænset netværksforbindelsestid, særligt hvis systemerne kan tilgås fra offentlige lokaler eller lokaler udenfor Region Midtjyllands kontrol.

Begrænset netværkstid	Systemejer skal vurdere, om brugersystemer med særlig høj risiko skal kræve fornyet autentifikation med fastlagte intervaller.

11.6 Styring af adgang til it-systemer og informationer

Styring af adgang til brugersystemer og informationer har til formål at sikre, at der udelukkende er autoriserede adgang til Region Midtjyllands brugersystemer og informationer.

11.6.1 Begrænset adgang til informationer

Adgangen for brugere og medarbejdere med supportfunktioner skal begrænses og være i overensstemmelse med forretningsbetingede krav.

Begrænset adgang til informationer	Brugere og medarbejdere med supportfunktioner må kun få adgang til systemfunktioner og informationer, hvis dette er forretningsmæssigt begrundet.

11.6.2 Isolering af særligt kritiske systemer

Isolering af særligt kritiske it-systemer	Særligt kritiske it-systemer skal placeres på isoleret informationsbehandlingsudstyr.

11.7 Mobilt udstyr og fjernarbejdspladser

Der er sket en rivende udvikling med brugen af mobilt udstyr både til privat og erhvervsmæssig brug. Der er samtidig en stigende grad af opmærksomhed på datasikkerhed i takt med udviklingen.

Der henvises generelt til:

"Retningslinje for fjernarbejdsplads" (ikke udviklet)

"Sikkerhedspolitik for mobile enheder"

"Juridiske vilkår for brugere af bronze serviceniveau"

11.7.1 Mobilt udstyr og datakommunikation

Region Midtjylland har retningslinjer for anvendelsen af mobilt udstyr uden for virksomhedens kontrollerede område herunder hvilke nødvendige beskyttelseforanstaltnigner, der er implementeret.

Opbevaring af bærbare computere	Bærbare computere skal fjernes eller låses inde efter arbejdstidens ophør.
Sikkerhedskontroller for fjernopkoblet udstyr	Mobile enheder skal sikres med antivirus, firewall og adgangskontrolsystemer. Disse foranstaltninger skal opdateres løbende.
Antivirus-programmer	Antivirus-programmer skal installeres på alle mobile enheder og fjernarbejdspladser. Programmerne skal opdateres dagligt.
Virusscanning af mobile datamedier	Region Midtjyllands antivirusløsning skanner automatisk ethvert mobilt medie (ekstern harddisk, cd'er, usb med mere). Der kan dog undtagelsesvis være enkelte formater eller enheder, som systemet ikke skanner. Brugeren opfordres derfor aktivt til at sikre at et nyt medie er skannet af antivirus systemet. Vær opmærksom på, at mobile datamedier i denne sammenhæng ikke dækker smartphones.

Brug af kryptering i forbindelse med opbevaring af data	Med opbevaring af interne informationer, som vurderes at være fortrolige på bærbare computere og håndholdte enheder, skal det vurderes, hvorvidt informationerne skal krypteres. Personoplysninger skal være krypteret med stærk kryptering, når de opbevares på transportabelt udstyr f.eks. bærbare computere, håndholdte computere.
Fortrolige data på mobile enheder	I Region Midtjylland skal alle smartphones og tablets, som anvendes i arbejdssammenhæng, registreres på et service- og sikkerhedsniveau. Personoplysninger eller interne data, som vurderes værende fortrolige, og som ønskes opbevaret på mobile enheder, skal beskyttes tilstrækkeligt ved kryptering.

11.7.2 Fjernarbejdspladser

Fjernarbejdspladser dækker først og fremmest over arbejde, der sker fra medarbejderens hjem, men omfatter også arbejde, der foregår uden for Region Midtjyllands lokationer.

Der henvises til:

"Retningslinje for fjernarbejdspladser" (medio 2013)

Opbevaring af fortrolige informationer på privat udstyr	Der må ikke behandles eller opbevares personhenførbare eller fortrolige informationer på udstyr, der ikke tilhører Region Midtjylland.
Fjernarbejdspladser	Tillades, når sikkerhedspolitikken i øvrigt overholdes.
Adgang fra fjernarbejdspladser	Der må kun gives adgang til sikkerhedsgodkendte systemer på internt netværk. Adgang gives kun fra godkendte og faste ip-adresser.
Adgang til netværket	Adgangen til Region Midtjyllands netværk må kun ske gennem sikkerhedsgodkendte løsninger.
Indkommende netværksforbindelser	Der må kun etableres forbindelser fra internet til Region Midtjyllands netværk efter forudgående godkendelse fra It's netværksafdeling eventuel suppleret med godkendelse fra It-sikkerhedsfunktionen.
Adgang til applikationer på Region Midtjyllands netværk	Der gives kun adgang til applikationer på internt netværk, som er sikkerhedsgodkendt af It.
Adgang til data på Region Midtjyllands netværk	Ved fjernadgang til data på Region Midtjyllands netværk må der ikke gemmes data på lokale harddiske eller andre eksterne medier.
Antivirus-programmer	Antivirus-programmer skal installeres på alle mobile enheder og fjernarbejdspladser. Programmerne skal opdateres dagligt.

Fjernstyring og administration	Det er tilladt at benytte værktøjer til fjernadministration, hvis der foreligger sikkerhedsgodkendelse af produktet.

12 Anskaffelse, udvikling og vedligeholdelse af informationsbehandlingsystemer

Sikkerhedsovervejelser bør altid indgå som en integreret del af processen, når der indkøbes, udvikles og implementeres nye systemer i Region Midtjylland.

12.1 Sikkerhedskrav til informationsbehandlingssystemer

Design, udvikling og implementering af informationsbehandlingssystemer, som understøtter Region Midtjyllands daglige drift, kan have afgørende betydning for sikkerheden. Kravene til sikkerheden skal være identificeret og aftalt inden udvikling og implementering af informationsbehandlingssystemer.

12.1.1 Analyse og specifikation af krav til sikkerhed

Region Midtjyllands krav til såvel nye som bestående systemer skal indeholde krav til sikkerheden med udgangspunkt i en risikovurdering.

Sikkerhed i systemplanlægning	It-sikkerhedskrav skal tages i betragtning ved design, aftestning, implementering og opgradering af it-systemer samt ved systemændringer.
Sikkerhed i applikationsudvikling	Sikkerhed skal inkluderes som en integreret del af alle udviklingsprojekter.
Sikring af udviklingsmiljøer	Udviklingsmiljøer skal specielt sikre integritet i udviklingsprocessen herunder sikring mod tab af data.
Sikkerhedskrav til informationsbehandlingssystemer	Sikkerhedskrav til kritiske systemer såvel nye som bestående tager udgangspunkt i en risikovurdering

12.2 Korrekt informationsbehandling

Passende sikringsforanstaltninger skal være vurderet og indarbejdet i Region Midtjyllands systemer med det formål at sikre korrekt databehandling.

12.2.1 Validering af inddata

Data, som sendes ind i systemer, skal valideres for korrekthed.

Integritet af andre data	Integriteten for data skal beskyttes med validering efter behov. Der kan være andre former for kontroller.

Databaseintegritet	Databasesikkerhed, integritetsstyring og datavalidering skal anvendes efter behov for at reducere muligheden for kompromittering af integriteten.
Validering af inddata	Data, der sendes ind i systemerne, skal valideres for korrekthed, hvor det er nødvendigt. Der skal vedligeholdes log over de aktiviteter, der sender data ind i systemer.

12.2.2 Kontrol af den interne databehandling

Kontrol af datas korrekthed skal indarbejdes i informationsbehandlingssystemer med det formål at overvåge, om data indeholder fejl, eller er modificeret enten på grund af systemfejl eller bevidste handlinger.

Kontrol af intern databehandling	Systemejer skal sikre kontrol af datas korrekthed i Region Midtjyllands systemer eller applikationer med det formål at afsløre, om data kan eller er blevet modificeret enten på grund af systemfejl eller bevidste handlinger.

12.2.3 Meddelelsers integritet

Krav til sikring af datas autenticitet og integritet i elektroniske meddelelser (f. eks. dataforsendelser) skal identificeres, og dertil passende sikringsforanstaltninger skal identificeres og implementeres. Kryptografi kan være et hensigtsmæssigt værktøj til at sikre meddelelsers integritet.

Integritet af meddelelser	Der skal foretages risikovurderinger af, hvorvidt meddelelsers integritet skal beskyttes samt den mest hensigtsmæssige metode til at implementere dette på.

12.2.4 Validering af uddata

Data fra systemer skal valideres med det formål at sikre, at de under de givne omstændigheder er korrekte.

Validering af uddata	Uddata fra Region Midtjyllands systemer eller applikationer skal valideres efter behov.

12.3 Kryptografi

Kryptografi har til formål at sikre fortrolighed, autenticitet og integritet af informationer.

Kryptologi er læren om hemmeligholdelse af informationer. Kryptografi er metoden til at omdanne informationer, så de bliver ulæselige ved hjælp af algoritmer.

12.3.1 Retningslinjer for brugen af kryptografi

Der skal være udarbejdet retningslinjer for Region Midtjyllands anvendelse af kryptografi.

Kryptering af harddiske	Indholdet af harddiske på Region Midtjylland ikke managed bærbare computere skal altid krypteres, hvis harddiskens indhold kan klassificeres som fortroligt eller indeholder personoplysninger.
Kryptering af filer	Filer, som indeholder personoplysninger, skal krypteres ved lagring udenfor systemer, der er beregnet til opbevaring af personfølsomme data. Det skal vurderes om interne dokumenter, der vurderes at være fortrolige, skal beskyttes med kryptering.
Kryptering af administrative netværksforbindelser	Netværksforbindelser, der benyttes til system-vedligeholdelse, skal altid krypteres. Dette gælder alt udstyr undtagen terminaler med direkte forbindelse til systemer.
Godkendelse af krypteringsprodukter	It-sikkerhedsfunktionen skal godkende alle produkter, der indeholder kryptografi, før disse må benyttes til fortrolige data.
Godkendte krypteringsprodukter	It skal vedligeholde en liste over godkendte krypteringsløsninger.
Fortrolige data på mobile enheder	I Region Midtjylland skal alle smartphones og tablets, som anvendes i arbejdssammenhæng, registreres på et service- og sikkerhedsniveau. Personoplysninger eller interne data, som vurderes værende fortrolige, og som ønskes opbevaret på mobile enheder, skal beskyttes tilstrækkeligt ved kryptering.

12.3.2 Nøglehåndtering.

Der bør være etableret et nøglehåndteringssystem, som understøtter Region Midtjyllands anvendelse af kryptografi.

Nøglehåndtering	It skal etablere et nøglehåndteringssystem, som understøtter Region Midtjyllands anvendelse af kryptografi.

12.4 Styring af driftsmiljøet

Adgangen til systemtekniske filer og kildekode skal være kontrolleret. Det skal sikres, at fortrolige og følsomme informationer ikke offentliggøres i testmiljøer.

12.4.1 Sikkerhed ved systemtekniske filer

Der skal være procedure for installation af systemer i Region Midtjylland.

Ændringer i forretningskritiske systemer	Alle ændringer i forretningskritiske systemer skal udføres efter godkendt procedure. Alle procedurer skal indeholde en alternativ plan til retablering af det forretningskritiske system. Vilkårene for aktivering af den alternative plan skal ligeledes fremgå af proceduren.
Softwareopdateringer generelt	It skal holde sig informeret om væsentlige programrettelser til de programmer, der anvendes i Region Midtjylland og snarest installere disse på alle computere, f.eks. servere og arbejdsstationer, når det vurderes, at rettelserne har positiv indflydelse på den samlede sikkerhed. Systemejer skal i samarbejde med it løbende vurdere, om der er et sikkerhedsmæssigt behov for opdatering af software til nye versioner for Region Midtjyllands fælles administrative systemer.
Rettelser til operativsystemer	It skal have en procedure for vurdering af tilgængelige sikkerhedsrettelser herunder patches eller hot-fixes til anvendte programpakker. Udrulning/installation på relevante systemer skal foretages snarest muligt efter en vurdering og en positiv funktions- og kompatibilitetstest.
Rettelser til applikations-programpakker	It skal vurdere tilgængelige sikkerhedsrettelser, f. eks. patches eller hot-fixes til anvendte programpakker. Udrulning/installation på relevante systemer skal foretages snarest mulig efter en vurdering og positiv funktions- og kompabilitetstest.
Større programpakkeopdateringer f.eks. "service packs"	Større opdateringer skal testes i et testmiljø, inden opdateringerne installeres i produktionsmiljøet.
Større operativsystemopdatinger f.eks. "service packs"	Større opdateringer skal testes grundigt for kompatibilitet med anvendte applikationer, inden opdateringerne installeres i produktionsmiljøet.

12.4.2 Sikring af testdata

Data, som anvendes til test, skal udvælges omhyggeligt, kontrolleres nøje og beskyttes i henhold til deres klassifikation. Angivelser i ISO 27002 afsnit 12.4.2 skal vurderes.

Sikring af testdata	Data fra driftsmiljøet må kun kopieres til testmiljø efter godkendelse af systemejer eller dataejer. Data til test skal udvælges, kontrolleres og beskyttes omhyggeligt og i henhold til deres klassifikation. Data fra driftsmiljøet, der anvendes i testmiljøer, skal slettes omgående efter afsluttet test. Kopiering og brug af data fra driftsmiljøet til test skal logges for at sikre kontrolsporet.

12.4.3 Styring af adgang til kildekode

Adgangen til kildekode skal begrænses.

Adgangskontrol for kildetekst	Kildetekst til applikationer under udvikling skal beskyttes med adgangskontrolsystemer for at sikre integriteten.
Kontrolleret adgang til kildekode	Kildekoden til udviklingsprojekter skal sikres mod uautoriseret adgang. Ændringer skal kontrolleres for at sikre integritet. Dette gælder især kritiske applikationer. Kildekode må ikke opbevares i driftsmiljøet. Kildekode og bibliotekerne med denne skal sikres. Hjælpepersonale må kun med specifikt autoriseret adgang få adgang til kildebiblioteker. Eventuelle udskrifter af kildekode skal opbevares sikkert.
Filsystemers integritet	Checksummer af kritiske eksekverbare filer og konfigurationsfiler bør regelmæssigt sammenlignes med en database over kendte og kontrollerede checksummer for at sikre mod uautoriserede ændringer eller fejl.

12.5 Sikkerhed i udviklings- og hjælpeprocesser

Sikkerhed i udviklings- og hjælpeprocesser har til formål at opretholde sikkerheden i brugersystemer.

12.5.1 Ændringsstyring

Kontrolleret styring af ændringer i systemer, hvor It har driftsansvaret, skal ske, når eksisterende systemer ønskes ændret, eller eksisterende systemer ønskes slettet fra produktionsmiljøet.

Processen for change management er beskrevet på Its intranet.

Ændringsstyring	Ændringsstyringer skal følge angivelser fra It-drift vedrørende "Proces for forhåndsgodkendt ændring"; "Proces for nødændring" eller "Proces for ændringsanmodning" samt "Proces for data og -dokumentstyring".

12.5.2 Teknisk gennemgang af forretningssystemer efter ændringer i styresystemerne

Gennemgang af systemer efter ændringer	Når driftsmiljøerne ændres, skal kritiske forretningssystemer gennemgås og testes for at sikre, at det ikke har utilsigtede afledte virkninger på Region Midtjyllands drift og sikkerhed.

12.5.3 Begrænsninger i ændringer til standardsystemer

Ændringer i standardsystemer	Ændringer i eksternt leverede systemer skal begrænses til nødvendige ændringer, og sådanne ændringer skal styres omhyggeligt.

12.5.4 Lækage af informationer

Der skal implementeres foranstaltninger, som begrænser risici for lækager af informationer.

Sikring af netværk	It har det overordnede ansvar for at beskytte Region Midtjyllands netværk.
Overvågning af netværk	It er ansvarlig for kontinuerligt at overvåge brugen og sikkerheden af Region Midtjyllands netværksinfrastruktur. It-drift er ansvarlig for identificering, diagnosticering, løsning og rapportering af hændelser samt for samarbejde med andre interessenter. Der skal være opdateret overvågning af al kritisk netværkstrafik i Region Midtjylland.
Opdeling af netværk	It skal segmentere netværk for at etablere en passende adskillelse mellem forskellige tjenester, brugergrupper eller systemer. Mindstekrav til netværkssegmentering er, at It etablerer en "demilitariseret zone" (DMZ), hvor offentligt tilgængelige servere placeres adskilt fra internt tilgængelige servere.
Kapacitetsovervågning	Alle serversystemer med kritiske informationer skal løbende overvåges for tilstrækkelig kapacitet for at sikre pålidelig drift og tilgængelighed.
Anskaffelser	Anskaffelser skal følge Region Midtjyllands indkøbspolitik.

12.5.5 Systemudvikling udført af en ekstern leverandør

Der skal etableres overvågning og kontrol af eksterne leverandører, som udfører systemudvikling for Region Midtjylland.

Systemudvikling udført af ekstern leverandør	Der skal foreligge klare aftaler med eksterne leverandører med hensyn til overvågning af udviklingsprocessen, afleveringtest, løbende dokumenteret kvalitetssikring, deponering af kildekode og ophavsret på kildekode.

12.6 Sårbarhedsstyring

Sårbarhedsstyring har til formål at forhindre skader fra angreb, som udnytter kendte sårbarheder.

12.6.1 Sårbarhedssikring

Information om nye trusler, virus og sårbarheder	It skal holde sig orienteret om eventuelle trusler mod de benyttede it-platforme og netværk. It er ansvarlig for eksternt samarbejde med de fornødne informationskanaler herunder samarbejde omkring it-sikkerhed med relevante eksterne interessegrupper og sikkerhedsorganisationer. It skal etablere en proces for identifikation af nye sårbarheder. Der skal udpeges en ansvarlig person eller gruppe for dette. It skal informere relevante personer i ledelsen om nye trusler, som potentielt kan berøre de pågældende forretningsenheder. It er ansvarlig for etablering af interne og eksterne netværk til sikring af fornøden information og vidensdeling samt opkvalificering af specifikke vidensområder.

13 Styring af sikkerhedshændelser

Formålet med afsnittet er at sikre, at der er etableret tilstrækkelige foranstaltninger, som kan dokumenterer sikkerhedshændelser og svagheder på en måde, som muliggør rettidig håndtering.

Der henvises til:

"Retningslinje for rapportering af sikkerhedshændelser" (ultimo 2013)

"Retningslinje for rapportering af sikkerhedssvagheder" (ultimo 2013)

"At lære af sikkerhedsnedbrud" (ultimo 2013)

13.1 Rapportering af sikkerhedshændelser og svagheder

Der skal foreligge rapportering af sikkerhedshændelser og svagheder, som kan sikre en rettidig håndtering.

13.1.1 Rapportering af sikkerhedshændelser

Sikkerhedshændelser og svagheder skal rapporteres og formidles hurtigst muligt for at sikre en korrekt og rettidig håndtering.

Der henvises til:

"Retningslinje for rapportering af sikkerhedshændelser" (ultimo 2013)

Rapportering af formodede sikkerhedshændelser	Ved konstatering af brud eller formodede brud på it-sikringsforanstaltninger skal rapportering straks ske til linjeledelsen, it-sikkerhedsfunktionen eller informationssikkerhedsfunktionen. Sikkerhedshændelser kan også oprettes som sag i Service Desk systemet.
Registrering af driftsstatus	It skal registrere væsentlige forstyrrelser og uregelmæssigheder i driften af systemerne.
Rapportering af sikkerhedshændelser	It eller outsourcingpartnere skal vedligeholde en opgørelse over sikkerhedshændelser. Væsentlige sikkerhedshændelser skal med jævne mellemrum rapporteres til Informationssikkerhedsudvalget.
Kontrol og opfølgning på sikkerhedsbrud	Brud på sikkerheden, uautoriseret adgang og forsøg på uautoriseret adgang til systemer, informationer og data skal registreres.
Kapacitetsovervågning	Alle serversystemer med kritiske informationer skal løbende overvåges for tilstrækkelig kapacitet for at sikre pålidelig drift og tilgængelighed.

13.1.2 Rapportering af svagheder

Svagheder skal noteres og rapporteres. Der bør foreligge anvisninger til alle brugere om, at svagheder og uhensigtsmæssigheder indrapporteres.

"Retningslinje for rapportering af svagheder" (ultimo 2013)

Rapportering af formodede sikkerhedshændelser	Ved konstatering af brud eller formodede brud på it-sikringsforanstaltninger skal rapportering straks ske til linjeledelsen, it-sikkerhedsfunktionen eller informationssikkerhedsfunktionen. Sikkerhedshændelser kan også oprettes som sag i Service Desk systemet.

13.2 Håndtering af sikkerhedsbrud og forbedringer

Der skal være etableret proces til løbende håndtering af sikkerhedsbrud og forbedringer. Herunder placering af ansvar for håndtering af sikkerhedsbrud. Der skal ligeledes være etableret en procedure for rapportering, som på en let og tilgængelig måde formidler sikkerhedshændelser.

Der henvises til:

"Utilsigtet offentliggørelse af personoplysninger på internettet"

13.2.1 Ansvar og forretningsgange

Ledelsens ansvar og de nødvendige procedurer skal være fastlagt for at sikre en hurtig, effektiv og metodisk håndtering af sikkerhedsbrud.

Ansvar og forretningsgange for sikkerhedshændelser	Informationssikkerhedsfunktionen i Region Midtjylland er ansvarlig for at fastlægge retningslinjer, der sikrer en hurtig, effektiv og metodisk håndtering af sikkerhedsbrud.
Proces for reaktion på hændelser	Ved mistanke om et sikkerhedsbrud kontaktes den nærmeste linjeledelse, it-sikkerhedsfunktionen eller informationssikkerhedsfunktionen. Der kan også oprettes en sag i ServiceDesk systemet. It-sikkerhedsfunktionen er ansvarlig for at definere og koordinere en struktureret ledelsesproces, der sikrer en passende reaktion på sikkerhedshændelser. It-sikkerhedsfunktionen skal etablere og vedligeholde en procedure, der sikrer et passende svar til personer, som rapporterer en mulig sikkerhedshændelse.
Information om sikkerhedshændelser	Så snart It-sikkerhedsfunktionen er bekendt med, at der er sket sikkerhedsbrud, skal relevante parter internt og eksternt informeres herom.
Overvågning af tilgængelighed	It skal løbende overvåge alle forretningskritiske it-systemer og regelmæssigt dokumentere systemernes tilgængelighed.
Tilgængelighedshændelser	Hændelser, der har indflydelse på tilgængelighed, skal afklares i henhold til gældende driftsaftaler (SLA). Driftshændelser, der ikke kan afklares inden for aftalt tid, skal udløse procedurer for hændelseshåndtering. De ramte brugere og systemejere skal informeres.

13.2.2 At lære af sikkerhedsbrud

Sikkerhedsbrud skal registreres, således at sikkerhedshændelserne kan analyseres i forhold til en række faktorer som konsekvens, sandsynlighed, antal, behov for overvgåning og omkosningerne forbundet med hændelsen. Registreringen skal være medvirkende til at afdække størrelsen og arten af sikkerhedsforanstaltninger.

Der henvises til:

"Retningslinje for læring af sikkerhedsbrud" (ultimo 2013)

Opfølgning på rapporterede sikkerhedshændelser	It-sikkerhedschefen er ansvarlig for at indsamle statistik for rapporterede sikkerhedshændelser.
Vurdering af tidligere hændelser	Mindst en gang om året skal it-sikkerhedsfunktionen gennemgå den forgangne periodes væsentlige hændelser og på denne baggrund, anbefale hvorvidt it-sikkerhedssystemet kan forbedres eller præciseres. Dette kan udmunde i forslag om opdaterede regler og/eller procedurer eller opdateret risikovurdering.

13.2.3 Indsamling af beviser

Sikkerhedshændelser og brud på sikkerheden kan have et retsligt efterspil. Informationer omkring hændelsen skal derfor indsamles, opbevares og præsenteres på en måde, der er i overensstemmelse med reglerne for bevismaterialers antagelighed under gældende lovgivning.

Der henvises til:

Vejledning om bevissikring (DI og DI ITEK)

Indsamling af beviser	Indsamling, opbevaring og præsentation af fyldestgørende bevismateriale skal følge angivelser i DI og DI ITEK's "Vejledning om bevissikring", som forefindes på Dansk Industrie's hjemmeside og It's intranet.

14 Beredskabsstyring

Beredskabsstyring skal modvirke afbrydelser i Region Midtjyllands forretningsaktiviteter og beskytte kritiske informationsaktiver mod effekten af et større nedbrud eller en katastrofe og sikre hurtig reetablering. Formålet er at begrænse konsekvenserne til et acceptabelt niveau samt at være i stand til at genoprette gennem forebyggende og udbedrende foranstaltninger.

Risikostyring og katastrofeplanlægning har til formål at mindske risikoen for og effekten af uforudsete hændelser.

Nødplaner skal være med til at opretholde driften, således at skaderne for regionen minimeres.

14.1 Beredskabstyring og informationssikkerhed

Beredskabsplanlægning skal etableres for at mindske risici af ulykker og fejl i Region Midtjylland ved nedbrud gennem genetablering af de mest kristiske systemer.

Region Midtjylland skal implementere beredskabsstyring som en løbende opgave med det formål at begrænse konsekvenserne af tab af informationsaktiver forårsaget af katastrofer og sikkerhedsbrister til et acceptabelt niveau samt at genoprette situationen gennem en kombination af forebyggende og udbedrende foranstaltninger. I forbindelse med beredskabsstyringen skal virksomhedens kritiske forretningsaktiviteter identificeres, og beredskabskravene vedrørende informationssikkerhed skal integreres med andre beredskabskrav vedrørende drift, personale, materiel, transport og øvrige

faciliteter.

14.1.1 Informationssikkerhed i beredskabsstyringen

Der skal udarbejdes og vedligeholdes en tværorganisatorisk beredskabsstyringsproces, som skal behandle de krav til informationssikkerhed, der er nødvendige for Region Midtjyllands fortsatte drift.

Beredskabsstyringsproces	It-sikkerhedschefen skal udarbejde og vedligeholde en tværorganisatorisk beredskabsstyringsproces, som skal behandle de krav til informationssikkerhed, der er nødvendige for Region Midtjyllands fortsatte drift.
Forsikring mod hændelser	Det skal vurderes, om forsikring kan medvirke til at minimere konsekvensen af tab. Især på områder, hvor sikringsforanstaltninger er vurderet som uhensigtsmæssige eller utilstrækkelige, skal dette overvejes.

14.1.2 Beredskab og risikovurdering

Informationssikkerhedens betydning for beredskabet skal baseres på identifikation af sikkerhedshændelser (eller sekvens af hændelser), der kan forårsage afbrydelser i virksomhedens forretningsprocesser ved f.eks. fejl på udstyr, menneskelige fejl, tyveri, brand, naturkatastrofer og terrorisme. Dette skal efterfølges af en risikovurdering for at fastlægge sandsynligheden for og omfanget af sådanne afbrydelser med fokus på tid, skadens omfang og den tid, det tager at retablere.

Risikoanalyse	Der skal udarbejdes en overordnet risikovurdering for alle forretningskritiske systemer.
Konsekvensvurdering	Konsekvenser af hændelser i forbindelse med it-systemerne skal løbende vurders af It-sikkerhedsfunktionen i samarbejde med systemejer.

14.1.3 Udarbejdelse og implementering af beredskabsplaner

Der skal udarbejdes planer for vedligeholdelse og retablering af virksomhedens forretningsaktiviteter inden for den fastsatte tidsramme efter en afbrydelse af eller fejl i Region Midtjyllands kritiske forretningsprocesser.

Der henvises generelt til:

"Proces for Major Incident"

"Proces for Situation Management"

"Proces for intern audit"

Beredskabsplan	Beredskabsplan skal foreligge for alle forretningskritiske systemer og processer
Retablering af forretningskritiske systemer på ny lokation	For alle Region Midtjyllands forretningskritiske systemer skal der forefindes en plan for retablering på ny lokation.
Aktivering af beredskabsplanen	Det skal være klart defineret, hvem der har ansvaret for aktivering af beredskabsplaner. Medarbejdere, der udgør en del af beredskabsplanen, skal være informeret om dette ansvar. Alle medarbejdere skal være informeret om beredskabsplanernes eksistens.

14.1.4 Rammerne for beredskabsplanlægningen

Ledelsen skal fastlægge en ensartet ramme for Region Midtjyllands beredskabsplaner for at sikre, at alle planerne er sammenhængende og tilgodeser alle sikkerhedskrav, samt at de fastlægger prioriteringen af afprøvning og vedligeholdelse.

Hver beredskabsplan skal beskrive behovet for beredskab, f.eks. behovet for at sikre informationerne og informationsbehandlingssystemets tilgængelighed og sikkerhed.Hver beredskabsplan skal klart beskrive betingelserne for dens aktivering samt de personer, der har ansvaret for de enkelte dele af planen. Når der identificeres nye krav, skal alle nødplaner, f.eks. planer for evakuering eller andre planer for nødfaciliteter, om fornødent ajourføres. Beredskabsplaner skal inkluderes i Region Midtjyllands ændringshåndtering for at sikre, at Region Midtjyllands fortsatte drift altid bliver tilgodeset.

Beredskabsplan	Beredskabsplan skal foreligge for alle forretningskritiske systemer og processer
Beredskabsplaner for sikkerhedskopiering	Alle forretningskritiske systemer skal have en nødplan for sikkerhedskopiering, således at risikoen for tab af data minimeres.
Beredskabsplaner for backup	Hvert forretningskritisk system skal have en nødplan for at sikre data. Dette skal testes løbende.
Aktivering af beredskabsplanen	Det skal være klart defineret, hvem der har ansvaret for aktivering af beredskabsplaner. Medarbejdere, der udgør en del af beredskabsplanen, skal være informeret om dette ansvar. Alle medarbejdere skal være informeret om beredskabsplanernes eksistens.
Iværksættelse af nødplaner	Det skal være klart defineret, hvem der har ansvaret for at aktivere nødplaner.

14.1.5 Afprøvning, vedligeholdelse og revurdering af beredskabsplaner

Region Midtjyllands beredskabsplaner skal løbende opdateres og afprøves for at sikre, at de er tidssvarende og effektive. Katastrofeplaner skal ligeledes opdateres i forhold til, hvordan myndigheder og beredskabsledelsen alarmeres, bygninger evakueres med mere.

Beredskabsplan	Beredskabsplan skal foreligge for alle forretningskritiske systemer og processer
Beredskabsplaner for sikkerhedskopiering	Alle forretningskritiske systemer skal have en nødplan for sikkerhedskopiering, således at risikoen for tab af data minimeres.
Opdatering af beredskabsplaner	Mindst 1 gang om året skal beredskabsplaner gennemgås med henblik på opdatering.
Beredskabsplaner for backup	Hvert forretningskritisk system skal have en nødplan for at sikre data. Dette skal testes løbende.
Afprøvning og vedligeholdelse af beredskabsplaner	Beredskabsplaner skal løbende afprøves og opdateres for at sikre, at de er tidssvarende og effektive.

15 Overensstemmelse med lovbestemte og kontraktlige krav

De fleste aspekter af Region Midtjyllands virke er omfattet af lovgivning, påvirket af kontrakter eller eksterne parters rettigheder.

15.1 Overensstemmelse med lovbestemte krav

Fornøden juridisk og informationssikkerhedsmæssig ekspertise skal involveres til vurdering af lovbestemte krav i forbindelse med anskaffelse eller udvikling af informationsbehandlingssystemer.

15.1.1 Identifikation af relevante eksterne krav

Identifikation af relevant lovgivning	Linjeledelsen er ansvarlig for, at relevant lovgivning er kendt og følges. Informationssikkerhedsudvalget er ansvarlig for, at alle eksterne sikkerhedskrav samt Region Midtjyllands håndtering af disse klarlægges, dokumenteres og løbende vedligeholdes.
Overholdelse af lovgivningen	Alle it-systemer skal overholde relevante lovmæssige krav.
Overholdelse af lov om markedsføring	Alle medarbejdere i organisationen skal være opmærksomme på, at lov om markedsføring overholdes.

15.1.2 Ophavsrettigheder

Installation af programmer på arbejdsstationer	Kun udstyr og software, der er godkendt af It, supporteres af It. Privat udstyr supporteres ikke med mindre der foreligger en dispensation fra it-chefen
Forbudte og tilladte programmer	It vedligeholder programporteføljen.
Anskaffelser	Anskaffelser skal følge Region Midtjyllands indkøbspolitik.
Administration af softwarelicenser	Registrering af software licenser sker gennem It. Det er it-chefens overordnede ansvar, at der er et tilstrækkeligt antal licenser. Medarbejdere skal koordinere brug af software-licenser med It. Medarbejdere må ikke forpligte Region Midtjylland ved at acceptere licensvilkår i software, som ikke er accepteret af It.
Retningslinier for ophavsrettigheder	Ledelsen har det overordnede ansvar for, at Region Midtjylland fastholder en passende opmærksomhed på ikke at krænke tredjeparts ophavsrettigheder. It skal vedligeholde dokumentation for ejendomsretten af licenser, originalmateriale og manualer. It skal løbende kontrollere, at software-licensaftaler overholdes f.eks. ved at eventuelle begrænsninger i antal brugere, servere eller kopier overholdes. Brugere må ikke kopiere, konvertere eller udtrække information fra billed- og lydfiler eller tilsvarende ressourcer, medmindre dette specifikt tillades fra rettighedshaveren. Brugere må ikke, helt eller delvist, kopiere bøger, artikler, rapporter eller andre dokumenter, medmindre dette specifikt tillades fra rettighedshaveren.

15.1.3 Sikring af Region Midtjyllands kritiske data

Opbevaring og behandling af data	Forretningskritiske data skal altid opbevares og behandles således, at dataintegriteten ikke kan drages i tvivl.
Sikring af Region Midtjyllands lovbestemte data	Region Midtjyllands lovbestemte data skal opbevares og behandles således, at datatab, uautoriseret modifikation og forfalskning undgås.

15.1.4 Beskyttelse af personoplysninger

Opbevaring og behandling af personoplysninger	Opbevaring og behandling af personoplysninger er reguleret af "Lov om behandling af personoplysninger" (Persondataloven) og "Sundhedsloven". Der må ikke behandles personoplysninger af fortrolig karakter på privat pc.
Opbevaring og sletning af e-mail	E-mail, der indeholder personoplysninger, skal slettes efter 30 dage.
Kontrol af overholdelse af persondatalovgivning	It-sikkerhedsfunktionen skal kontrollere overholdelse af persondatalovgivning.
Sporbarhed	Behandling af personrelaterede informationer skal logges automatisk, således at det er muligt for en revisor at kontrollere hvem, der har arbejdet med hvilke informationer på hvilke tidspunkter.

15.1.5 Beskyttelse mod misbrug af informationsbehandlingsfaciliteter

Misbrugsbeskyttelse af it-udstyr	Linjeledelsen skal se til, at it-udstyr anvendes til det, det er berettiget til. Enhver anvendelse til private formål uden ledelsens forudgående accept eller uautoriseret anvendelse betragtes som uberettiget anvendelse. Såfremt en sådan uberettiget anvendelse identificeres, skal nærmeste leder orienteres herom mhp. eventuelle sanktioner.

15.1.6 Lovgivning vedrørende kryptografi

Regulering på kryptografiområdet	I Danmark er der ikke nogen lovgivning vedr. kryptografi.

15.2 Overensstemmelse med sikkerhedspolitik og -retningslinier

Fastholdelse af det af Regionsrådets ønskede sikkerhedsniveau er en vedvarende proces, som kræver tilbagevendende opfølgning. Målet er at sikre, at Region Midtjyllands sikkerhedspolitik- og retningslinjer er implementeret og efterleves.

15.2.1 Overensstemmelse med Region Midtjyllands sikkerhedsretningslinjer

Revision af sikkerhedspolitik	Informationssikkerhedsudvalget tager, på grundlag af den løbende overvågning og rapportering fra it-sikkerhedsfunktionen, Informationssikkerhedspolitikken op til revurdering en gang om året.
Opfølgning på implementering af sikkerhedspolitikken	Linjeledelsen er ansvarlig for, at informationssikkerheden løbende sikres lokalt.

15.2.2 Opfølgning på tekniske sikringsforanstaltninger

Sikkerhedstest af interne it-systemer	Der udføres uddybende sikkerhedstest af sikkerhedsniveauet i internt netværksudstyr og servere efter behov.
Sikkerhedstest af eksterne it-systemer	Der skal udføres sikkerhedstests af kontroller og netværksforbindelser for at identificere og undgå uautoriserede adgangsforsøg efter behov.

15.3 Beskyttelsesforanstaltninger ved revision af informationsbehandlingssystemer

15.3.1 Sikkerhed i forbindelse med systemrevision

Sikkerhed i forbindelse med revision	Revisionskrav og revisionshandlinger i forbindelse med systemer i drift skal planlægges omhyggeligt og aftales med de involverede for at minimere risikoen for forstyrrelser af Region Midtjyllands forretningsaktiviteter. De planlagte revisionshandlinger må kun omfatte læseadgang til systemer og data. Hvis revisionen nødvendiggør mere end læseadgang, skal dette så vidt muligt ske på kopier af de berørte filer. Filerne skal slettes efter brug. Al adgang i forbindelse med revision skal logges. De personer, der udfører revisionen, skal være uafhængige af det reviderede område.

15.3.2 Beskyttelse af revisionsværktøjer

Beskyttelse af revisionsværktøjer	Adgangen til revisionsværktøjer skal begrænses for at forhindre misbrug.