

## Indhold

- 1) Indledning
- 2) Formål
- 3) Arkenas organisation
- 4) Fysisk sikkerhed
- 5) Sikkerhedsforanstaltninger
- 6) Aftaler mellem Kunden og ARKENA
- 7) Driftsdokumentation
- 8) Kontrol fra offentlige myndigheder

## 1. Indledning

Dette dokument beskriver Arkenas sikkerhedspolitik for vores driftsmiljø og omfatter en beskrivelse af Arkenas driftsmiljø, organisation og generelle sikkerhedsforanstaltninger i forbindelse med primært hosting. Dokumentet bruges internt hos ARKENA som definition på hvilke krav ARKENA skal overholde, og overfor kunder som dokumentation på hvilke sikkerhedsprocedurer ARKENA har implementeret.

ARKENA tilbyder en række hostingydelser. Dels shared hosting af streaming media filer (Arkena MediaHotel), dels facility management (Arkena Managed Streaming Server) og dels hosting af vores ASP applikationer Arkena MediaBuilder, Arkena LiveTool samt tilhørende moduler.

## 2. Formål

Arkenas politik og krav til drifts- og datasikkerhed opfyldes under hensyn til følgende formål:

- At tilbyde et stabilt og fysisk sikkert driftsmiljø med et højt serviceniveau.
- At ARKENA medarbejdere kun har adgang til driftssystemer, hvis de er godkendt til denne adgang, i hht. sikkerhedspolitikens bestemmelser.
- Al uvedkommende personer ikke kan få adgang til driftssystemer.
- At system og data ved brand, strømsvigt og andre force majeure lignende situationer kan gendannes hurtigst muligt og i størst muligt omfang.

## 3. Arkenas organisation

### Om ARKENA

ARKENA A/S er specialiseret indenfor Streaming Media området og beskæftiger sig primært med IP-baserede transmissioner af video/audio.

ARKENA har som en væsentlig del af vores forretningsområde hosting af streaming media, samt tilhørende hosting af egenudviklede applikationer. Arkena er som sådan ikke en traditionel webhosting leverandør, men vores hostingmiljø retter sig primært mod opbevaring og distribution af tunge datatyper som video og audio.

Der findes mere information om ARKENA på adressen [www.Arkena.dk](http://www.Arkena.dk).

### Beskrivelse af sikkerhedsorganisationen

Direktionen har det øverste formelle ansvar for et tilfredsstillende sikkerhedsniveau.

Organisatorisk hører området datasikkerhed direkte under driftschefen. Driftschefen har det daglige ansvar for at opfylde det ønskede sikkerhedsniveau for driftsmiljøet. Driftschefen har i det daglige et tæt samarbejde med de ansatte udviklere, hvorfor disse i særlig grad er involveret i arbejdet med at sikre et højt sikkerhedsniveau.

### Information og vejledning

ARKENA sikrer, at det aktuelle sikkerhedsniveau er kendt for de involverede medarbejdere i organisationen, og hvilke sikkerhedsmæssige foranstaltninger der er gældende. ARKENA autoriserer i den forbindelse medarbejdere (driftsovervågning, teknisk support mv.) til at have adgang til driftssystemer.

### Clearing af medarbejdere

Alt personale hos ARKENA indleverer en pletfri straffeattest ved ansættelse, og derefter hver januar måned under hele ansættelsesforløbet.

Ved ansættelse underskriver alt personale som en del af deres ansættelseskontrakt en tavshedserklæring, som omfatter tavshedspligt i forhold til alt information der opnås kendskab til under ansættelsesforholdet - dette dækker både Arkenas forretningsgange og kunders data. Tavshedspligten fortsætter selvom ansættelsesforholdet måtte ophøre.

### Adgangsniveauer

ARKENA opererer sikkerhedsmæssigt med tre personaletyper: Driftspersonale, udviklingspersonale og øvrigt personale.

- Driftspersonale har fuld adgang til samtlige Arkenas driftssystemer, herunder net-infrastruktur og administratoradgang til alle servere. Desuden har driftspersonalet fysisk adgang til alle servere.
- Udviklingspersonale har adgang til Arkenas driftssystemer i det omfang driftschefen godkender dette. Der opereres med en "deny-politik", dvs. adgang er som udgangspunkt afvist, og der gives kun adgang efter en godkendt vurdering af behovet for den enkelte udviklingsmedarbejder.
- Øvrigt personale har ingen adgang til driftssystemer.

#### 4. Fysisk sikkerhed

##### Driftscenter

Driftcenteret er skalsikret, og maskinstuernes ydre vægge, døre og vinduer er således sikret imod indbrud og brand. Alle eksterne døre er af stål, og der er desuden opsat stålskotter foran alle vinduer.

Alle maskinstuer er forsynet med sensorer til detektering af indbrud og indbrudsforsøg. Der er således monteret åbningskontakter på alle døre og vinduer, samt rystekontakter på ventilationsgitre, vinduer og porte. Der er desuden opsat bevægelsessensorer, der dækker gangarealer i kontorlokalerne.

Driftscenteret er under konstant overvågning med overvågningskameraer - udvendigt ved indgangsdøre og indvendigt med ekstra kameraer i udvalgte lokaler. Der foretages logning af optagelserne.

Det installerede adgangskontrolsystem sikrer, at det kun er muligt at komme ind i maskinstuerne ved hjælp af adgangskort med kode. De fleste døre kræver kort ved såvel ind- som udgang, og der føres logbog over hvilke personer, der har haft adgang i hvilke tidsrum.

Adgangskontrolsystemet sikrer adgang til hostinglokationen på forskellige niveauer:

Adgang til bygningen gives ved indtastning af kode ved gadedøren eller ved at kontakte receptionen via dørtelefon. Koden til gadedøren skiftes hver måned.

Der er elektronisk adgangskontrol til reception, kontorer og mødelokaler.

Der er elektronisk adgangskontrol med kort og kode til maskinstuerne.

Til Driftscenterets maskinstuer er der kunde adgang til Server Camp afsnittet. I resten af maskinstuerne er der kun adgang for autoriseret TDC driftspersonale.

##### Strømforsyning

Alle el-installationer i Driftscenteret er udført i overensstemmelse med gældende internationale regler baseret på en såkaldt N+1 løsning på No-break (UPS) anlæg, batterier og reserveforsyningsanlægget (dieselgeneratorer), dvs. at der er installeret ét batteri-anlæg og én dieselgenerator mere, end det er nødvendigt selv ved fuld belastning.

Dieselgeneratorerne vil kunne levere strøm til Driftcenteret i 3-4 dage uden ekstra påfyldning af olie.

Batteri-anlægget kontrolleres hvert halve år, og dieselgeneratorer testes i en halv til en hel time mindst fire gange om året.

Kundens udstyr monteres i server-racks, der er tilsluttet 2 separate sikringsgrupper.

Gulvene i maskinstuerne er forsynet med en antistatisk belægning og jording.

##### Køling

Driftscenterets køleanlæg er ligeledes opbygget efter en N+1 model. Der er således monteret én køleenhed mere end nødvendigt for køling ved fuldt udnyttet strømkapacitet. Klima-anlægget sikrer en rumtemperatur i maskinstuerne på 18-23 grader C. Der er installeret fugtighedsfølere i forbindelse med køleanlæggene.

##### Brandsikring

I maskinstuerne er installeret et fintfølede brandalarmeringssystem bestående af snifferanlæg og ion-meldere, som indsuger og analyserer luften flere forskellige steder i lokalet og således vil advisere om f. eks. røgudvikling og åben ild.

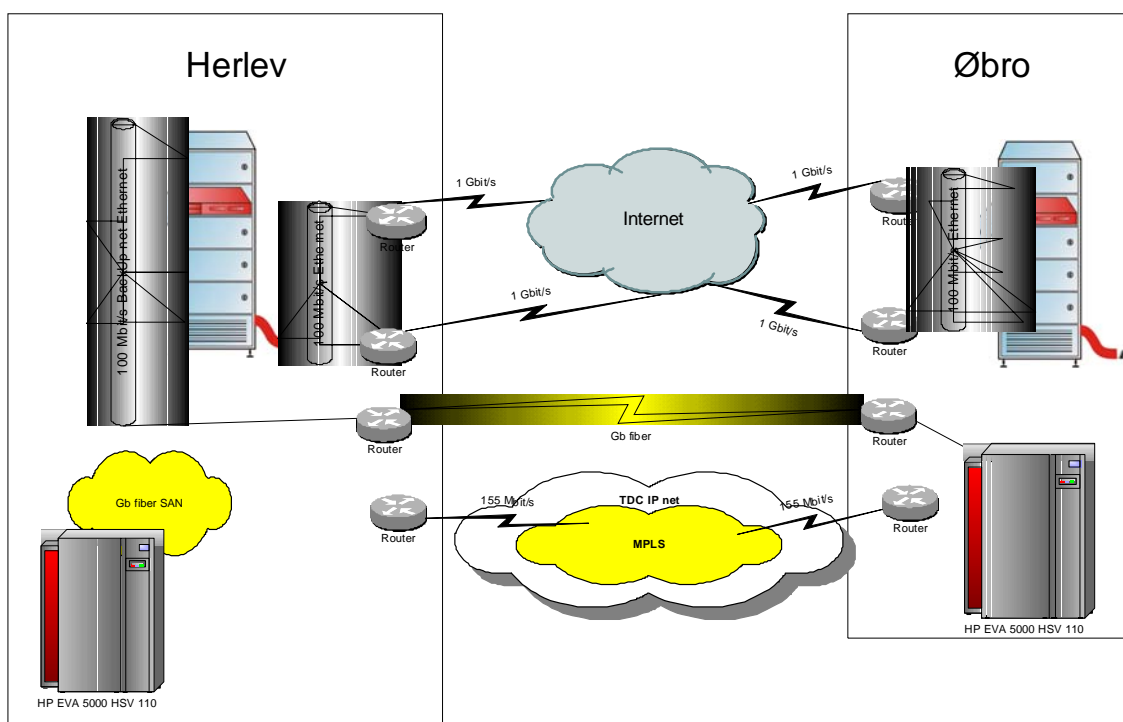
Til brandbekæmpelse er installeret Inergen-anlæg, samt lovbestemte CO2-brandslukkere.

Serverrummene udgør en selvstændig brandcelle med min. BD60-adskillende bygningsdele til andre rum samt min. BD30-døre til gang.

Lynbeskyttelses anlæg med jording kontrolleres hvert femte år.

## IP infrastruktur

### Lokal infrastruktur



Driftscenteret er udstyret med fuld redundans i forhold til driftsmiljø og den direkte adgang til TDC's backbone. Dermed er erstatningsudstyr eller alternative forbindelser klar til at tage over, hvis der sker nedbrud. Dette betyder f. eks., at hvis den normale IP-forbindelse til Driftscenteret mistes, vil trafikken blive dirigeret via en alternativ rute til og fra Driftscenteret.

Erfaringsmæssigt ligger opetiden på Driftscenteret infrastruktur på 99,99 %. Infrastruktur defineres i denne sammenhæng som brandsikring, køl, strømforsyning, samt internetforbindelsen med routere og switche. Internetforbindelsen omfatter forbindelsen frem til kundens netværksstik.

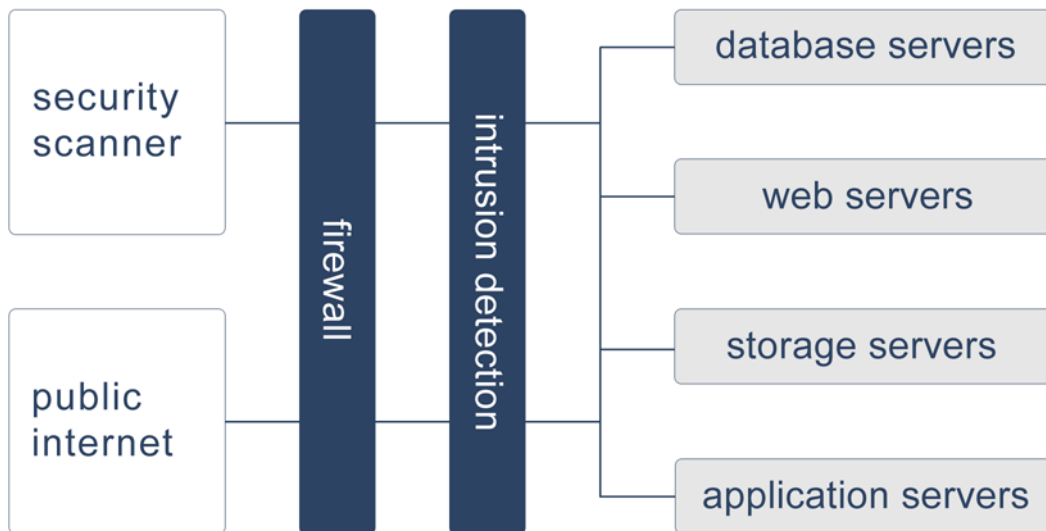
For MPLS ligger opetiden erfaringsmæssigt på 99,5 %

Arkenas driftscenter er placeret hos TDC hosting i Herlev.

## 5. Sikkerhedsforanstaltninger

Til opfyldelse af et generelt højt sikkerhedsniveau, har ARKENA etableret maskinelle, fysiske og administrative sikkerhedsforanstaltninger.

Arkenas driftssystem er opbygget efter følgende model:



Netværket er beskyttet på 2 sikkerhedsniveauer:

**Firewall.** Denne sikrer, at der kun er adgang til de services, som afvikles på den offentlige del af Internet

**Intrusion detection.** Den trafik der passerer firewall'en kan indeholde angreb via de åbne services. Derfor bliver trafikken analyseret. Et eksempel på en åben service er http, som ofte benyttes til at angribe IIS servere med. Da angrebene ligner hinanden kan de let identificeres og stoppes. Inde på Arkenas net er serverne opdelt efter funktion, hvilket minimerer det potentielle antal sikkerhedshuller på den enkelte server. Samtidig opnås bedre performance, da den enkelte server optimeres til en bestemt opgave.

For at være 100 % sikker på at nettet ikke er åbent for angreb, angribes Arkenas eget net ved hjælp af en Security Scanning. Denne scanning indeholder scripts som simulerer alle kendte angreb. Derved bliver nettet effektivt testet for kendte sikkerhedshuller. Der skal anvendes en ekstern leverandør til denne scanning.

Foranstaltningerne er samlet beskrevet nedenfor.

### Firewall

Arkenas firewall er opdelt i 2 niveauer:

- Første filtrering sker i routeren, som alt eksternt trafik passerer. Her filtreres ICMP trafik til ping, traceroute osv. fra, hvilket besværliggør det for hackere at finde ud af hvilke IP-adresser på Arkenas net, der peger på servere, som kan angribes. Desuden filtreres alt unødigt UPD trafik fra på dette niveau.
- Anden filtrering sker på den dedikerede firewall, som alle servere er forbundet igennem. TCP trafik filtreres på dette niveau, så kun services den enkelte server skal stille til rådighed på Internet, er åbne.

### Proaktiv portscanning

Kvartalsvist gennemfører en eksternt leverandør for ARKENA en proaktiv portscanning af Arkenas samlede net for at sikre, at der ingen kendte "exploits" findes på nettet. Til formålet benyttes som leverandør pt. DIR A/S.

### Sikkerhedsmæssige rutiner

ARKENA har i driftschefens stillingsbeskrivelse defineret sikkerheden som et væsentligt ansvarsområde. Driftschefen har selv kompetence til at vurdere hvilke rutiner, som giver den bedste sikkerhed, men der sikres en løbende definition af arbejdsopgaver og -rutiner. De væsentligste punkter pt. er:

- Abonnér på relevante mailing lists på [www.securityfocus.com](http://www.securityfocus.com), så man altid har opdateret information om nyeste angrebstyper og "exploits".
- Opdater straks efter der er frigivet et sikkerhedspatch, både på operativsystem- og applikationsniveau.
- Log alle administratorhandlinger på separat logserver, således at hvis en hacker skulle bryde ind kan handlingerne hurtigt spores. Derved kan angrebet stoppes og muligheden for at pågribe hackeren er stor.
- Definer interne sikkerhedsprocedurer, for bl.a. at sikre at medarbejdere omgås password forsvarligt.
- ARKENA samarbejder desuden med personale hos DIR A/S omkring erfaringsudveksling mellem driftspersonalet. DIR A/S er en af Danmarks største og mest erfarne hosting udbydere. Det er derfor naturligt, at ny viden omkring sikkerhed, procedurer mv. udveksles mellem relevante medarbejdere.

### Aktion ved exploits

Hvis der findes mulige exploits på nogle af serverne, sikkerhedsopdateres disse servere straks. Er der mulighed for virus scannes systemet med antivirus program passende til den inficerede platform. Hvis systemet er blevet kompromitteret, fjernes inficeringen ved at følge instruktioner fra relevante kilder (typisk udbyderen af det inficerede software eller 3. partsinformation som [www.securityfocus.org](http://www.securityfocus.org)). Hvis inficeringen ikke kan verificeres fjernet med 100 % sikkerhed, skal den inficerede server reinstalleret ved førstkomende mulighed, hvor det giver minimal gene for kunderne (typisk førstkomende aften eller weekend).

### Remote access

Remote access – fjernadgang – til driftssystemer er nødvendigt for en effektiv drift. Der er derfor vedtaget følgende retningslinjer for fjernadgang.

- Fjernadgang gives kun for at sikre en effektiv drift.
- Fjernadgang skal ske efter gældende politik for password (se nedenfor).
- Al fjernadgang sker krypteret.
- Der er kun fjernadgang til driftssystemer fra godkendte IP-numre. I praksis betyder det, at et angreb på driftssystemer forudsætter, at angriberen har tiltunget sig fysisk adgang til Arkenas kontorer og derfra foretager et angreb på driftsmiljøet.

## Password politik

Interne passwords: Interne passwords skal være stærke passwords bestående af mindst 8 tegn, som indeholder en kombination af tal, store og små bogstaver. Dette gælder alle passwords på Arkenas systemer, både passwords til driftsadministration, øvrige systemer og personlige passwords.

Formålet med at benytte stærke passwords er at forhindre "brute force" angreb, hvor en lang række passwordkombinationer afprøves. Et stærkt password giver 60 forskellige tegnmuligheder, som fordelt på 8 tegn giver 167.961.600.000.000 mulige kombinationer. Alle systemer giver et "timeout" på mindst 1 sekund ved forkert password. Hvorved den teoretiske indtrængningstid ved et "brute force" angreb vil være mere end 5 mio. år.

Eksterne passwords: Eksterne passwords, er de passwords som benyttes af kunder til at tilgå deres dataområder. Kunder udstyres altid med stærke passwords ved oprettelse men har på visse produkter mulighed for efterfølgende at ændre password. Ved ændringen tillades der medium stærke passwords, dvs. kravet er kun en kombination af tal og bogstaver, der er ikke krav om blandede store/små bogstaver. Kunder kan også bede om, at ARKENA manuelt ændrer password, hvor det er driftspersonalets opgave at sørge for, at dette password som minimum er medium stærkt.

Generering af passwords: Stærke passwords genereres automatisk vha. programmet PWGEN.

Opbevaring af passwords: Opbevaring af passwords til Arkenas interne systemer, herunder passwords der giver fuld adgang til shared hosting servere, opbevares ikke elektronisk. Driftspersonale husker disse passwords, og der er forbud mod at nedskrive disse. Driftschefen opbevarer dog i brandsikret pengeskab en kopi af password.

Passwords der giver adgang til ARKENA CRM, og dermed til kunders produkter (gennem nyt eksternt password), opbevares på et system, der kun kan tilgås med personligt login via ARKENA CRM. Der er SSL kryptering) og kun adgang fra godkendte IP-adresser. Både drifts- og udviklingspersonale har adgang til disse passwords for at sikre kunderne en effektiv support og en effektiv produktion.

## Administrativ sikkerhed

Passwords som ikke længere er i brug annulleres, og det er vedtaget, at der ikke må forekomme hosting, CMS eller andre kundeabonnementer (og dermed passwords), som ikke er i brug.

Ved nedlæggelse af hostingabonnement opfordres kunden til at foretage egen backup, alternativt bede ARKENA om at varetage dette. Ved dato for nedlukning slettes alle data og kundeinformationer, herunder passwords, permanent.

## Arkivering af logs

Serverlogs opbevares som minimum 1 år efter gældende dansk lov.

## Oppetid

ARKENA tilstræber som servicemål 100 % oppetid på alle produkter.

Planlagt "downtime", vedligehold mv., som finder sted efter det aftalte varsel, medregnes ikke i fht. opfyldelse af servicemål.

Der kan indgås aftale om drift med garanteret opetid, typisk 99 %.

Ved aftalens indgåelse afklares, hvad ARKENA er ansvarlig for. Som udgangspunkt er det hardware, styresystem og de applikationer, som produktet indeholder. Hvis kunden har specialudviklede applikationer, som ARKENA skal være ansvarlige for, samt supportere disse, skal det aftales særskilt, og der skal altid foreligge en driftsmanual på disse applikationer.

### Overvågning

Der er opsat automatisk varslingsystem, som varsler driftspersonalet ved linje-, applikations- eller performance problemer. Varsling sker både via datalinjer (e-mail) og via mobiltelefon (SMS), så varsling ikke er afhængig af kun én transportrute.

### Backup

Der foretages daglig backup af alle servere i shared hosting. Backup foregår ved overførsel af data til datacenter i DIX, dvs. fysisk opbevares backup data ikke i Arkenas driftscenter. Overførslen foregår krypteret. Servere i facility hosting (dedikerede servere) har ikke inkluderet backup i basisydelsen, men denne kan tilkøbes.

### Båndbredde, gennemsnitlig og max belastning

ARKENA har TDC som leverandører på internetforbindelserne i driftscenteret og kan således leve op til de krav og specifikationer som er specificeret i TDCs SLA. Internetforbindelsen til driftscenteret består pt. af 2 x 622mbit forbindelser, som løbende overvåges og opgraderes ved overbelastning.

ARKENA er pt. forbundet med 100mbit forbindelse til central switch i driftscenteret. Nedenfor er TDC's ip-backbone kort beskrevet.

### TDC's IP-backbone

TDC har et veludbygget IP-net, dels i form af den danske IP-backbone dels med en række internationale forbindelser.

Kvalitetsparametre i IP-nettet udtrykkes ved hjælp af følgende parametre:

- Tilgængelighed
- Round Trip Delay
- Pakketab

TDC opsamler til stadighed statistik og udfører målinger med henblik på at sikre, at kvalitetskravene for disse parametre overholdes og for at planlægge nødvendige kapacitetsudvidelser.

Nettets tilgængelighed udtrykkes ved hjælp af tilgængeligheden for de enkelte accesspunkter udregnet som gennemsnit over en måned.

Målsætningen er en tilgængelighed pr. accesspunkt på 99,5 % pr. måned svarende til mindre end fire timers utilgængelighed. Erfaringsmæssigt er tilgængeligheden pr. accesspunkt i gennemsnit bedre end 99,99 % pr. måned svarende til under 5 minutters utilgængelighed pr. måned.

Målsætningen er et gennemsnitligt Round Trip Delay (RTD) i TDC's IP-net på mindre end 25 millisekunder pr. måned, og at 97 % af målingerne ligger under 150 millisekunder. Erfaringsmæssigt er RTD mindre end 10 millisekunder og 97 % -fraktilen mindre end 50 millisekunder.

Pakketabet vurderes stikprøvevis ved hjælp af testtrafik foretaget med ping-funktionen. Manglende svar på ping betragtes som et pakketab.

Målsætningen er et pakketab på mindre end 1 % pr. måned, men erfaringsmæssigt er pakketabet betydeligt mindre end 0,1 % om måneden. Pakketabet må intet steds lokalt være større end 10 % gennem flere dage.

### Overvågning af infrastrukturen

No-break anlæg og køl overvåges via CTS-anlæg, og opetidsstatistikker for køl og strøm behandles på statusmøder mellem de driftsansvarlige på driftscenteret

Alarmer fra brandmeldere, adgangskontrol og CTS-anlæg videregives til en central drifts- og overvågningscentral i TDC samtidig med, at der sendes SMS til udvalgte personer i TDC.

Brandbekæmpelsessystemet har alarmoverførsel direkte til brandvæsenet.

Kapaciteten bliver overvåget ved hjælp af SNMP, som danner grafer over trafikmængder igennem netværksenhederne. Alle forbindelser opgraderes løbende til sikker overkapacitet, når belastningen har nået 60 % af kapaciteten.

### I tilfælde af brand og servernedbrud

Hvis Arkenas driftscenter brænder ned, skal der anskaffes nye servere, hvilket vil tage nogle dage, hvor alt vil være nede. Der vil selvfølgelig blive arbejdet i døgndrift på fuldstændig reetablering. Ved servernedbrud på enkelte maskiner, kan reetablering ske langt hurtigere, typisk inden for 12-24 timer.

### Nødproduktion

I tilfælde af totalt nedbrud vil ARKENA reetablere servere til nødproduktion hurtigst muligt. ARKENA er kun ansvarlig for at reetablere den del af serveren, som indgår i aftalen mellem ARKENA og kunden.

## 6. Behandling af kundeinformationer

### Fortrolighed

Al information som kunden videregiver til ARKENA forbliver kundens ejendom, og ARKENA forpligter sig til at behandle informationen fortroligt:

- Informationen behandles og beskyttes som fortrolig information.
- ARKENA afstår fra at bruge den pågældende information på anden måde end i forbindelse med det aftalte samarbejde.

- ARKENA må ikke videregive eller offentliggøre fortrolig information til tredje part uden forudgående skriftlig tilladelse fra kunden. Uanset ovenstående skal ARKENA ikke være forpligtet overfor kunden i tilfælde, hvor:
- Den pågældende information bliver en del af den almindelige offentlige viden, uden at det skyldes Arkenas handlinger eller forsømmelser.
- Informationen erhverves lovligt fra en tredje part under omstændigheder, der tillader informationens videregivelse.
- Informationen videregives til en tredje part, idet en sådan videregivelse er nødvendig for samarbejdet mellem de oprindelige parter, og idet en sådan videregivelse betinger, at modtageren er underkastet samme krav om tavshed og hemmeligholdelse som ARKENA.
- Informationen kræves udleveret af offentlig myndighed, og at denne myndighed gør kravet gældende jævnfør dansk lovgivning.

Såfremt ARKENA bryder fortroligheden, er kunden berettiget til at søge om erstatning jævnfør dansk lovgivning. Hvis ARKENA som følge af bruddet på fortroligheden opnår økonomisk gevinst, er kunden berettiget til at modtage kompensation svarende til den gevinst, ARKENA måtte have opnået.

## 7. Driftsdokumentation

I forbindelse med Managed Streaming Server, udarbejder ARKENA i samarbejde med kunden driftsdokumentation for applikationer, som ligger ud over de standardapplikationer, som Managed Streaming Server konfigureres med. Ved shared hosting (Arkena MediaHotel) udgør Arkenas vilkår og forretningsbetingelser driftsdokumentationen.

Der kan udarbejdes yderligere driftsdokumentation efter nærmere aftale mellem ARKENA og kunden.

## 8. Kontrol fra kunden eller offentlige myndigheder

ARKENA er til rådighed for kunden og Datatilsynet med hensyn til kontrol af det fastlagte sikkerhedsniveau og de trufne sikkerhedsforanstaltninger. Tidsforbrug på kontrol som ikke er initieret af ARKENA som en del af den vanlige kontrol, vil blive afregnet på timebasis. De trufne sikkerhedsforanstaltninger gennemgås mindst en gang om året af ARKENA.