IT-Sikkerhedspolitik

For

NORDICALS

erhvervsmæglere

Indhold

Informationssikkerhedspolitik for Nordicals

1 Målsætning/formål

Sikkerhedspolitikken skal til enhver tid understøtte Nordicals' værdigrundlag og vision samt de strategiske mål, der er i IT-strategien for kæden.

Hensigten med sikkerhedspolitikken er endvidere at tilkendegive over for alle, som har en relation til Nordicals A/S eller de respektive forretninger der bærer kædens navn, at anvendelse af informationer og informationssystemer er underkastet standarder og retningslinjer.

Nordicals ønsker derfor at opretholde og løbende udbygge et IT-sikkerhedsniveau på højde med de krav, som skitseres i 'Den fællesstatslige standard for informationssikkerhed' (DS 484 basale krav). Dokumentet kan desuden være base for en senere ISO certificering. Kravene skærpes på veldefinerede områder, hvor der er specielle lovkrav, aftaleretslige forhold eller evt. særlig risiko (afdækket ved en risikovurdering).

Fastholdelse og udbygning af et højt sikkerhedsniveau er en væsentlig forudsætning for, at Nordicals fremstår troværdig både nationalt og internationalt.

For at fastholde Nordicals' troværdighed skal det sikres, at information behandles med fornøden fortrolighed, og at der sker fuldstændig, nøjagtig og rettidig behandling af godkendte transaktioner.

IT-systemer betragtes, næst efter medarbejderne, som Nordicals' mest kritiske ressource. Der lægges derfor vægt på driftssikkerhed, kvalitet, overholdelse af lovgivningskrav, og på at systemerne er brugervenlige, dvs. uden unødigt besværlige sikkerhedsforanstaltninger.

Der skal skabes et effektivt værn mod IT-sikkerhedsmæssige trusler, således at Nordicals' image og medarbejdernes tryghed og arbejdsvilkår sikres bedst muligt. Beskyttelsen skal være vendt imod såvel naturgivne som tekniske og menneskeskabte trusler. Alle personer betragtes som værende mulig årsag til brud på sikkerheden; dvs. at ingen persongruppe skal være hævet over sikkerhedsbestemmelserne.

Samtidig er det Nordicals' mål med sikkerhedspolitikken, at kunne dokumentere overfor forretningernes kunder, at vi arbejder på at blive Danmarks bedste erhvervsmæglerkæde, også når gælder beskyttelse af kundernes informationer.

Målene er derfor, at:

- Opnå høj driftssikkerhed med høje oppetidsprocenter og minimeret risiko for større nedbrud og datatab - TILGÆNGELIGHED
- Opnå korrekt funktion af systemerne med minimeret risiko for manipulation af og fejl, i såvel data som systemer - INTEGRITET
- Opnå fortrolig behandling, transmission og opbevaring af data - FORTROLIGHED
- Opnå en gensidig sikkerhed omkring de involverede parter - AUTENTICITET
- Opnå en sikkerhed for gensidig og dokumenterbar kontakt - UAFVISELIGHED

Ovenstående mål skal konkretiseres i Service Level Agreements (SLAs) og kontrakter overfor samarbejdspartnere, og understøttes af eventuelle nødvendige sikkerhedsdokumentation mellem Nordicals og leverandører.

Regler og retningslinjer fra informationssikkerhedspolitikken skal løbende indarbejdes i de relevante gældende regler på personalepolitikkens område, såfremt der ikke kan refereres direkte til denne dokumentation.

2. Omfang

Sikkerhedskonceptet omfatter følgende (pr. d.d. nævnt i dokumentets header):

- En informationssikkerhedspolitik, der godkendes af udvalget for informationssikkerhed, på baggrund af indstilling fra Nordicals' IT-sikkerhedskoordinator.
- En informationssikkerheds guide, der opsummere informationssikkerhedspolitikken ift. forretningernes pligt til overholdelse af sikkerhedsreglerne. Tilgængelig på Nordicals' Intranet.
- Et kortfattet og overordnet informationsbrev, der kort beskriver ansvar og plan for IT sikkerheden, overfor de ansvarlige udvalg i kæden.

Omfanget af sikkerhedskonceptet kan uddybes, efterhånden som Nordicals' overordnede plan for IT sikkerheden i kæden bliver udviklet.

3. Gyldighedsområde

Politikken er gældende for alle Nordicals' informationsrelaterede aktiviteter, uanset om disse udføres af ansatte i kæden, tilknyttede franchise forretninger eller af samarbejdspartnere. Dette inkluderer f.eks. alt data om personale, data om finansielle forhold, alle data som bidrager til administrationen af virksomheden, produktionsdata og anlægsdata samt informationer som er overladt til Nordicals af andre. Disse data kan være faktuelle oplysninger, optegnelser, registreringer, rapporter, forudsætninger for planlægning eller anden information, som kun er til intern brug.

Informationssikkerhedspolitikken har gyldighed for alle ansatte i Nordicals kæden og al anvendelse af Nordicals' informationsaktiver.

4. Organisation og ansvar

4.1. Udvalget for informationssikkerhed

Udvalget for informationssikkerhed, er en bestemmende myndighed af Erhvervsudvalget og består af:

- Direktøren for kæden (formand for udvalget)

- Nordicals' IT-sikkerhedskoordinator (Kædekontorets IT ansvarlige)
- En repræsentant for hver af de 5 største forretninger på ledelsesniveau
- Evt. En – eller flere – repræsentanter for brugerfunktionerne

Udvalget er normgivende og fastsætter på grundlag af den vedtagne informationssikkerhedspolitik de principper/retningslinjer, der skal sikre målopfyldelsen.

Udvalget behandler alle sikkerhedsspørgsmål af principiel karakter.

Udvalget foretager en årlig vurdering af informationssikkerhedspolitikken og de tilknyttede sikkerhedsretningslinjer – herunder at disse lever op til de eksterne forpligtelser udtrykt i lovgivning og kontrakter/aftaler. Udvalget vurderer samtidigt, om der er behov for fornyet risikovurdering/ konsekvensanalyse.

4.2. Beredskabsplanlægning

Katastrofer søges undgået gennem en veltilrettelagt fysisk sikring og overvågning af bygninger, tekniske installationer og IT-udstyr. Omfanget af disse foranstaltninger besluttes ud fra en afvejning af risici imod sikringsomkostninger og udmøntes alene af den enkelte forretning som har ansvaret.

Beredskabsplanerne skal omfatte:

- Skadebegrænsende tiltag
- Oversigter over systemer og udstyr
- Etablering af temporære nødløsninger
- Prioriterede krav til genetablering
- Genetablering af permanent løsning

4.3. Sanktionering

Medarbejdere der bryder de gældende informationssikkerhedsbestemmelser i Nordicals, kan straffes disciplinært. De nærmere regler om dette fastsættes i overensstemmelse med den gældende personalepolitik, i den respektive forretning.

4.4. IT Sikkerhedsfunktionen (IT-sikkerhedskoordinatoren)

På grund af Nordicals' store grad af outsourcing af drift og support til underleverandører, og derigennem ofte til større, professionelle samarbejdspartnere, er det ikke hensigtsmæssigt at operere med en større særskilt/funktionsadskilt IT Sikkerhedsafdeling/-funktion. I stedet løses opgaverne primært ved:

- At tage hensyn hertil i aftalegrundlag med samarbejdspartnere, f.eks. ved at pålægge samarbejdspartnere at foretage forskellige former for kontrol og opfølgning og rapportere herom til IT sikkerhedskoordinatoren.

- At iværksætte egne revisionsopgaver og/eller sikkerhedsundersøgelser i det omfang udvalget for informationssikkerhed finder det fornødent.

Kædekontorets IT sikkerhedskoordinator har ansvar for:

- At udarbejde og vedligeholde sikkerhedspolitikken indeholdende sikkerhedsprincipper for informations anvendelsen – evt. med ekstern assistance
- At udarbejde relevante sikkerhedskrav, der operationaliserer informationssikkerhedspolitikken – evt. med ekstern assistance
- At foretage opfølgning og rapportering af indmeldte sikkerhedsbrud
- At behandle dispensationsansøgninger for begrundede afvigelser i forhold til retningslinjerne og rapportere disse til udvalget for informationssikkerhed
- At holde sig ajour med den generelle udvikling på det sikkerhedsmæssige område
- At koordinere relevante initiativer med de øvrige aktører i koncernsamarbejdet

4.5. Forretningsledelsen

Den enkelte forretning i kæden, har ansvar for:

- At informationssikkerhedspolitikken og de regler, der er relevante for hans/hendes ansvarsområde, er kendte og efterleves
- At medarbejderne gennem uddannelse og udvikling opnår sikkerhedsbevidsthed om nødvendigheden af at overholde de sikkerhedsmæssige retningslinjer, og at disse efterleves
- At der, efter behov, udarbejdes yderligere dokumentation vedr. sikkerhed for forretningens område, såfremt IT sikkerhedspolitikken ikke er dækkende for forretningens medarbejdere.
- At koordinere opklaringsarbejdet ved konstateret eller begrundet mistanke om sikkerhedsbrud. Resultatet rapporteres til kædekontorets IT sikkerhedskoordinator.
- At retningslinjerne for ansættelse, introduktion, løbende vurdering, funktionsskift og afvikling af medarbejdere overholdes

Der skal tilstræbes uafhængighed af enkeltpersoner gennem etablering af personbackup for de medarbejdere, der er alene om at dække specialer eller systemer af væsentlig betydning for Nordicals Kædekontor. Som supplement hertil skal dokumentationen tilhørende disse områder også holdes ajourført og evt. udbygges.

4.6. Systemejere

Systemejere (til systemer Nordicals medarbejdere bruger) bærer pga. det valgte koncept en meget væsentlig del af ansvaret for at det valgte sikkerhedsniveau etableres og opretholdes.

Systemejere har ansvar for:

- At der ved aftalens indgåelse forefindes en kravspecifikation som tager eksplicit hensyn til sikkerhedsmæssige forhold forud for enhver systemudvikling/–ændring/-anskaffelse/-opdatering
- At der internt udarbejdes en risikovurdering i h.t. kravene hertil
- At der ved idriftsætning af systemet foreligger konkrete regler og procedurer for regulering og administration af adgangsforholdene, såfremt sådanne er relevante – og at disse er i overensstemmelse med de principielle krav hertil
- At autorisere adgangen til systemet i h.t. retningslinjerne herfor
- At foretage opfølgning og rapportering af sikkerhedsbrud til Nordicals Kædekontors IT sikkerhedskoordinator.

I de situationer, hvor der ikke er funktionsadskillelse (autorisation/administration) kompenseres med andre sikkerhedsforanstaltninger, som udmøntes i samarbejdspartneres valgte interne dokumentation.

4.7. Dataejere

Dataejeren (som opbevare sensitiv data for Nordicals, men ikke er systemejer) har ansvar for:

- At der forefindes en risikovurdering i h.t. kravene hertil – for systemtilknyttede data i samarbejde med systemejeren, eller at der forefindes dokumentation for at systemejerens risikovurdering er accepteret som gældende.
- At der inden indrapportering af data i systemer foreligger konkrete regler og procedurer for regulering og administration af adgangsforholdene – og at disse er i overensstemmelse med de principielle krav hertil
- At autorisere adgangen til data i h.t. retningslinjerne herfor samt at sikre, at enhver sikkerhedsmæssig følsom informationsaktivitet kan henføres til den person, som har udført aktiviteten
- At foretage opfølgning og rapportering af sikkerhedsbrud til Nordicals Kædekontors IT sikkerhedskoordinator.

I de situationer, hvor der ikke er funktionsadskillelse (autorisation/administration) kompenseres med andre sikkerhedsforanstaltninger, som udmøntes i samarbejdspartneres valgte interne dokumentation for dataadministrationen.

4.8 Ejere af fysiske aktiver

Alle fysiske aktiver er som udgangspunkt ejet af den indivduelle forretning, medmindre det er IT udstyr som er leaset igennem Nordicals kædekontor.

Såfremt aktivet er omfattet af en aftale om hosting, tages der hensyn hertil i aftalegrundlaget med samarbejdspartneren, f.eks. ved at pålægge samarbejdspartneren at foretage forskellige former for kontrol og opfølgning og rapportere herom.

Ejeren af det fysiske aktiv har ansvar for:

- At overholde informationssikkerhedspolitikken og de regler, der er relevante for den enkeltes arbejdsopgaver
- At rapportere om eventuelle sikkerhedsbrud eller mistanke herom til nærmeste chef
- At der ved ibrugtagning af lokaler/udstyr foreligger konkrete regler og procedurer for regulering og administration af adgangsforholdene – og at disse er i overensstemmelse med de principielle krav hertil
- At autorisere adgangen til lokalerne/udstyret i h.t. retningslinjerne herfor
- At foretage opfølgning og rapportering af sikkerhedsbrud til Nordicals Kædekontors IT sikkerhedskoordinator.

I de situationer, hvor der ikke er funktionsadskillelse (autorisation/administration) kompenseres med andre sikkerhedsforanstaltninger, som udmøntes i forretningens interne dokumentation for kontrol med adgang til fysiske lokaler.

4.9. Medarbejdere

Funktionsadskillelse er det bærende kontrolprincip såvel på person- som på organisations planet. Hvor dette ikke er praktisk eller økonomisk hensigtsmæssigt, skal kompenserende kontroller indføres.

Den enkelte medarbejder har ansvar for:

- At overholde informationssikkerhedspolitikken og de regler, der er relevante for den enkeltes arbejdsopgaver
- At rapportere om eventuelle sikkerhedsbrud eller mistanke herom til nærmeste chef

4.10. Samarbejdspartnere

Samarbejdspartnerne har ansvar for:

- At medarbejderne i deres virksomhed gennem uddannelse og udvikling opnår sikkerhedsbevidsthed om nødvendigheden af at overholde de sikkerhedsmæssige retningslinjer, herunder tiltrædelseserklæringen
- At der, efter behov, forefindes yderligere dokumentation vedr. sikkerhed for samarbejdspartnerens område
- At der ved installation af nye og modifikation af eksisterende interne systemer og komponenter med påvirkningsmulighed til Nordicals' informationsaktiver gennemføres en forudgående risiko-/sikkerhedsvurdering
- At koordinere opklaringsarbejdet ved konstateret eller begrundet mistanke om sikkerhedsbrud. Hændelsen og resultatet rapporteres via egen sikkerhedsorganisation til Nordicals IT sikkerhedskoordinator

5. RISIKOVURDERING OG -HÅNDTERING

5.1 Risikovurdering

5.1.1. IT-risikoanalyse

Væsentlige informations- og fysiske aktiver har en risikovurdering. Ansvarlig for løbende ajourføring af risikovurderinger påhviler udvalget for informationssikkerhed. Mindst én gang årligt skal der ske revurdering af risikovurderingerne, den udførende rolle tilfalder IT sikkerhedsfunktionen.

Risikovurderinger tager udgangspunkt i 2 faktorer. "Sandsynligheden for at hændelsen optræder" samt "Konsekvenser i form af tab hvis hændelsen indtræder".

Følgende formel kan opsættes:

"Sandsynligheden for at hændelsen optræder" x "Konsekvenser i form af tab hvis hændelsen indtræder" = "Estimeret tab ved truslen i form af hændelsen"

Alternativt kan nedenstående model anvendes:

Konsekvens / Sandsynlighed	Lille = 1	Mellem = 2	Høj = 3
Meget usandsynlig = 1	Risiko kan tolereres	Risiko kan tolereres	Moderat risiko
Sandsynlig = 2	Risiko kan tolereres	Moderat risiko	Risiko kan ikke tolereres
Meget sandsynlig = 3	Moderat risiko	Risiko kan ikke tolereres	Risiko kan ikke tolereres

5.2. Håndtering af sikkerhedsrisici

5.2.1 Procedure for risikohåndtering

Med udgangspunkt i risikovurderingerne der ligger over det accepterede risikoniveau, fastsættes der håndtering af disse ud fra følgende :

1. Definér hvad der skal gøres ved risikoen:
    a. Reducér risikoen – flere sikkerhedstiltag, større sikkerhed, nye regler
    b. Eliminér risikoen – nedlæg systemet eller processen der resulterer i risikoen
    c. Overfør risikoen – forsikring i forhold til risikoen, outsourcing til tredjepart
    d. Acceptér risikoen – Det er for dyrt at gøre noget ved risikoen, så ledelsen accepterer den
2. Etablér handlingsplaner for de risici, der er besluttet at gøre noget ved, jf. punkt 1.
    a. Hvad skal der gøres?
    b. Hvem er ansvarlig?
    c. Hvornår er deadline?
    d. Hvor høj er prioriteten?
3. Følg op på handlingsplanerne

   a. Har ansvarlige lavet arbejdet?
   b. Hvor kan resultatet ses?
4. Følg op på risiciene
   a. Opdatering af risikovurdering der hvor der er gennemført handlingsplaner
   b. Er risikoen forøget?
   c. Er risikoen mindsket?
   d. Kan nuværende risici accepteres?

6. INFORMATIONSSIKKERHEDSPOLITIKKER

6.1. Retningslinjer for styring af informationssikkerhed

Det har Nordicals' bevågenhed at efterleve gældende lovgivning og krav til informationssikkerhed, hvorfor informationssikkerhedsudvalget til stadighed udviser opmærksomhed og engagement for informationssikkerhedspolitikken.

6.1.1. Politikker for informationssikkerhed

Den overordnede informationssikkerhedspolitik for forretningerne i Nordicals kæden, har til formål at vejlede medarbejdere og kunder om procedure til overholdes af IT sikkerheden. I IT sikkerhedspolitikken uddybes tiltag for forretningen og dets medarbejdere, samarbejdspartnere, systemejere, databehandler og andre, som håndtere data for Nordicals og i nogle tilfælde Nordicals' kunder.

IT-sikkerhedspolitikken skal først og fremmest sikre, at Nordicals' kunder er fuldstændig trygge ved at deres data, sensitiv eller ej, bliver sikkert opbevaret og håndteret af alle Nordicals' medarbejdere. Sekundært er IT politikken et bemyndiget trin i anskaffelsen af IT sikkerhedscertifikat, som kan verificere ovenstående for interesserede parter, uden nødvendigt kendskab til selve sikkerhedsprocedurerne.

6.1.2. Gennemgang af politikker for informationssikkerhed

IT-sikkerhedspolitikken ajourføres en gang årligt, et år fra sidste revision af dokumentet, af rollen som IT sikkerhedskoordinator. Ændringer som har indflydelse på forretningernes håndtering af IT sikkerheden , skal godkendes af udvalget for informationssikkerhed.

7. ORGANISERING AF INFORMATIONSSIKKERHED

7.1. Intern organisering

7.1.1. Interne organisatoriske forhold

Nordicals kæden er bestående af enkelte franchise forretninger, som selv har ansvar for overholdelse af gældende regler på IT området, heri inkluderet IT sikkerhedsregler fastsat af Nordicals Kædekontor, som også har overordnet ansvar for implementering af nye IT sikkerhedstiltag. IT sikkerhedspolitikken, som betegnes som en del af den overordnede informationssikkerhed, skal godkendes af udvalget af informationssikkerhed, som indeholder 5 af de største forretninger, og som repræsentere størstedelen af medarbejderne i kæden.

Indeholder nye sikkerhedsmæssige tiltag ikke en direkte indflydelse af forretningens medarbejdere, kan Nordicals kædekontor implementere disse uden godkendelse af udvalget for informationssikkerhed. Determinering af tiltagets omfang, udføres af kædekontorets IT sikkerhedskoordinator.

Den daglige koordinering af informationssikkerheden i forretningerne, fastsættes af forretningen selv og er ikke underlagt krav om dokumentering overfor kæden. Nordicals kædekontor anbefaler af én medarbejder i forretningen, som dagligt forefindes på lokationen, udpeges til IT superbruger og dermed også for ansvar for koordinering mellem forretning og kædens IT sikkerhedskoordinator.

Såfremt den ansvarlige for den daglige koordinering af informationssikkerhed ikke er tilstede, kan forretningens medarbejdere kontakte deres indehaver, som er bekendt med IT sikkerhedspolitikken.

7.1.2. Ansvarsplacering

Ansvarlig for sikkerhedsbrud er som udgangspunkt den øverste ledelse, ultimativt bestyrelsen. I tilfælde hvor en fysisk person er ansvarlig for sikkerhedsbrud, vil ansvaret kunne placeres ved denne persons tilførende forretning.

Skyldes sikkerhedsbruddet en samarbejdspartner, kan sikkerhedsbruddet være ansvarspådragende for den pågældende samarbejdspartner.

Sikkerhedsbrud forårsaget af en samarbejdspartner betyder, at den pågældende samarbejdspartner skal dokumentere hændelsesforløbet samt redegøre for, hvordan sikkerhedsbruddet er håndteret samt hvilket beredskab der er for at imødegå sikkerhedsbrud. Der skal ved kontraktindgåelse med leverandører sikres, at det nødvendige beredskab er tilstede og dokumenteret.

7.1.3. Funktionsadskillelse

Forretningskritiske systemer skal beskyttes ved hjælp af funktionsadskillelse, således at risikoen for misbrug af privilegier minimeres. Hvor funktionsadskillelse ikke er muligt, skal der implementeres kompenserende tiltag.

Der bør sikres funktionsadskillelse blandt IT-ansatte så vidt muligt således, at de, der har adgang til evt. logning, ikke er de samme, som dem, der har adgang til data. De, der har adgang til at administrere data, behøver ikke nødvendigvis have læserettigheder. Dette skal sikre, at der ikke kan manipuleres med loggen.

7.1.4. Kontakt med myndigheder

Kontakt til myndigheder ved IT kontrol eller brud på sikkerhedsregler, påfalder den enkelte forretning hvori situationen opstår.

7.1.5. Informationssikkerhed ved projektstyring

Nordicals tager stilling til IT-sikkerhed i vores projekter uanset type og størrelse.

7.2. Mobilt udstyr og fjernarbejdspladser

7.2.1. Politik for mobilt udstyr

Der er ingen begrænsning i de dataklasser, der tillades fjernadgang til på forretningernes netværk.

Fortrolige informationer skal krypteres når de opbevares eller transporteres på bærbare medier, f.eks. USB-hukommelse, PDA'er, cd'er, eller dvd'er. Manglende kryptering tillades hvis medierne, der benyttes til transport af fortrolige data, under transporten er overvåget af betroede personer. Bærbare medier som er overleveret til samarbejdspartnere, skal sikres returnering eller destruering ved projektets afslutning.

7.2.2. Fjernarbejdspladser

Fjernarbejdspladser tillades når sikkerhedspolitikken i øvrigt overholdes.

Personligt ejet IT-udstyr som f.eks. pc, PDA, bærbare harddiske, USB hukommelse, MP3-afspillere, minidisks, cd- eller dvd-brændere må ikke anvendes til kopiering eller opbevaring af fortrolige data, med mindre dette er midlertidig til overførsel til kædens hosting partnere.

8. MEDARBEJDERSIKKERHED

8.1. Før ansættelse

Det er op til den enkelte forretning at beslutte evt. procedurer før ansættelse, som informere om IT sikkerhed. Kæden anbefaler forretningen af referer til den offentlige IT sikkerhedspolitik.

8.1.2. Ansættelsesvilkår og -betingelser

Alle vilkår og -betingelser for nye ansættelser er som udgangspunkt op til den enkelte forretning i Nordicals kæden, med mindre det falder under ansvarlig brug af IT udstyr og software. Som beskrevet i sektion 4.5, skal forretningens ledelse sikre at medarbejder er bekendt med, og overholder, IT sikke rhedsreglerne.

7.2. Under ansættelse

7.2.1. Ledelsens ansvar

Alle vilkår og -betingelser for nye ansættelser er som udgangspunkt op til den enkelte forretning i Nordicals kæden, med mindre det falder under ansvarlig brug af IT udstyr og software. Som beskrevet i sektion 4.5, skal forretningens ledelse sikre at medarbejder er bekendt med, og overholder, IT sikkerhedsreglerne.

7.2.2. Bevidsthed om, uddannelse og træning i informationssikkerhed

Ansvaret for tilgængelighed af uddannelse, træning og oplysning om informationssikkerheden i kæden, påfalder i sidste ende Nordicals kædekontor. Ansvaret for overholdelse af udleveret information, påfalder den enkelte forretning ledelse.

7.2.3. Overvågning af systemanvendelse

Ved mistanke om misbrug har systemadministratorer og de netværksansvarlige ret til at overvåge aktiviteterne, herunder ind- og udgående e-mail, uden på forhånd at informere brugerne herom i det konkrete tilfælde. En sådan overvågning kan kun ske med øverste ledelses forudgående tilladelse.

7.2.4. Sanktioner

Som franchise ejede forretninger i Nordicals kæden, er ansvaret for sanktionsmuligheder ved overtrædelse af informationssikkerhedspolitikken op til den enkelte forretnings ledelse. Eventuelle sanktioner kan være mundtlig eller skriftlig advarsel, eller i yderste tilfælde afskedigelse af medarbejder.

7.3. ANSÆTTELSFORHOLDETS OPHØR ELLER ÆNDRING

7.3.1 Ansættelsesforholdets ophør eller ændring

Der kan deles op i to scenarier, hvor til der handles forskelligt. Den ene situation er den ansatte der selv siger op, eller der sker afskedigelse. Ved afskedigelse kræves der øjeblikkelig handling fra ledelsen.

Ved ophør af ansættelsesforhold sikrer nærmeste indehaver eller daglige leder, at alle rettigheder og adgange til fysiske og tekniske aktiver inddrages. Ved fratrædelse af ledelse, sikre r kædens ledelse, alternativ bestyrelsen, de nødvendige tiltag.

8. STYRING AF AKTIVER

Informationsaktiverne styres af Nordicals kædekontor, som har ansvar for at indkøbe, risikovurdere samt værdisætte aktiverne på kædeplan. Klassificeringen af aktiver så som IT udstyr, samt værdisætning efter endt leasingperioden, fastsættes af Nordicals kædekontor økonomi afdeling.

8.1. Ansvar for aktiver

Der redegøres for i de følgende punkter, hvem der har ansvar for aktiver, samt hvem der udarbejder fortegnelser.

8.1.1. Fortegnelse over aktiver

Herunder er listet hovedinformationsaktiver, eksklusiv fortegnelser over IT hardware, som forefindes på Nordicals kædekontor. Fortegnelser opdateres løbende, og benyttes til afregning mellem kæden og forretningerne. Ajourføring af informationsaktivs fortegnelserne, påhviler kædens IT sikkerhedskoordinator.

Nordicals A/S har følgende informationssystemer

- Nordicals.dk (Website samt CMS)
- Nordicals Intranet (Kun intern adgang)
- Nordicals Forum (Kun intern adgang)
- C&B Ejendomssystem (Varetaget af C&B systemer)

- Microsoft Office 365 + Power BI + Skype For Business (Varetaget af Support IT)
- IT Terminal platform (Varetaget af Support IT)

8.1.2. Ejerskab af aktiver

Det er systemejeren, der har det ledelsesmæssige ansvar for informationsaktivet.

Den ansvarlige sikrer:

a. at informationsaktiver er korrekt klassificeret
b. at regler og retningslinjer for adgang til aktivet er i overensstemmelse med den generelle adgangspolitik samt gældende lovgivning.
c. at der foreligger opdaterede regler/retningslinjer, der er kendte af alle brugere.

8.1.3. Beskyttelse af systemdokumentation

IT sikkerhedskoordinatoren skal opbevare systemdokumentation passende sikkert.

Systemdokumentation kan indeholde fortrolige oplysninger, der beskriver et systems processer, procedurer, datastrukturer, autorisationsprocesser m.v.

Adgangsrettigheder til systemdokumentation skal holdes på et minimum og godkendes af Nordicals ledelse. Dokumentation skal beskyttes mod uautoriseret adgang og indseende.

8.1.3. Accepteret brug af aktiver

Accepteret brug af Nordicals' aktiver fremgår af IT-politikken. Det er ledelsens ansvar at alle brugere er bekendt gjort med disse samt at alle brugere ved, hvor retningslinjerne for accepteret brug af aktiver kan findes.

8.1.4. Tilbagelevering af aktiver

Alle aktiver tilbageleveres til pågældende forretning i Nordicals ved ansættelsesophør. Ved afskedigelse returneres aktiver omgående. Ved egen opsigelse returneres aktiver på sidste arbejdsdag. Efter returnering af aktiver afgør nærmeste leder, om aktivet skal beholdes, destrueres eller friskrives til tidligere medarbejder. Lagringsmedier skal som altid tømmes for data, programmer osv. Dette kan håndteres af Nordicals' hosting partner og IT leverandør, Support IT. Data af forretningsmæssig værdi, som findes på lokale medier (i.e. Ikke i hosted miljø) sikres ved at overføres til hosted miljø, eller nærmeste leders computer.

8.2. Klassifikation af information

Informationer og data i Nordicals kæden, klassificeres efter type og sensitivitet, og opbevares sikkert i henhold til klassificeringen.

8.2.1. Klassifikation af information

Klassification af information og data, sker primært automatisk i IT systemerne, på baggrund af data indgangen, eller af medarbejder i den enkelte forretning såfremt data leveres uden for et system.

8.2.2. Mærkning af information

Klassificeringen er dokumenteret og ajourføres løbende, dog minimum årligt ud fra følgende opdeling:

Offentlige data/informationer

Defineres som data/informationer, som alle, der udtrykker et ønske om det, har eller kan få adgang til. Det kan eks. Hjemmesider, brochurer m.m.

Følsomme data/informationer

Defineres som data/informationer, der kræver høj grad af beskyttelse. Adgangen skal begrænses til så få godkendte personer som muligt. Kryptering er et krav i nogle tilfælde, så som personfølsom data.

Interne data/informationer

Defineres som data/informationer, der kun må anvendes og kommunikeres internt, og som i den daglige drift er nødvendig for de brugere, der skal anvende dem. Intern data ligges kun tilgængeligt på interne kanaler, så som intranet, som eksterne ikke har adgang til.

Fortrolige data/informationer

Defineres som data, som kun særligt betroede personer har adgang til, og kun for at kunne udøve deres arbejdsfunktioner. Data kan krypteres, eller placeres i hostet miljø i adgangsbeskyttet områder.

8.2.3 Håndtering af aktiver

Placering og mærkning af informationer og data kan ske ud fra adgangsniveau og tildelt filstruktur for den enkelte. Mærkning kan ske drev-/mappe-/fil- niveau, og sker typisk udfra sagsnummer som er fælles ID for reference til en salgssag.

I Nordicals' hostingmiljø foregår det sådan:

Alle medarbejder har adgang til et personligt drev, samt et fælles drev. Enkelte support afdelinger har adgang til specielle fællesdrev, delt på tværs af kæden mellem forretninger.

På fælles drev har hver forretning en mappe, som kun forretnings medarbejdere kan se og redigere i.

I hver forretningsmappe, findes 7 faste systemmapper, som til sammen udgør fundament for adgangsniveauerne, som er fastsat på kædeplan.

- Indehaver og daglige ledere i forretningerne har adgang til alle 7 mapper, inkl. En beskyttet mappe kun til ledelsen af forretningen, samt HR mappe.
- Økonomi medarbejdere har næst højest niveau, med adgang til 4 almindelige mapper samt en speciel økonomimappe, som kun de og ledelsen har adgang til.
- Andre medarbejdere har laveste niveau, med adgang til 4 almindelige kontor mapper.

HR medarbejdere kan have samme adgang som økonomi, med speciel autorisation til HR mappe.

8.3. Databærende medier

Flytbare datamedier - f.eks. CD´er, usb-nøgler, diske og print, skal beskyttes mod ødelæggelse, tyveri, forlæggelse og uautoriseret anvendelse.

Følsomme og fortrolige data skal beskyttes mod uautoriseret indseende og misbrug. Der skal foreligge procedurer i den enkelte forretning, som sikrer beskyttelse af følsomme og fortrolige data såvel på flytbare arbejdsstationer som på dokumenter, CD'er, usb-nøgler, print, rapporter m.v.. Der skal foreligge procedurer på kædeplan til sikring af, at følsomme og fortrolige data, som er lagret digitalt, beskyttes i henhold til deres klassifikation og personalet skal instrueres om korrekte procedurer ved håndtering af datamedier.

Data på flytbare medier så som USB nøgler, kan krypteres enkeltvis på filerne eller på hele USB nøglen, ved brug af de indbyggede funktioner i Windows. Kæden er ikke ansvarlig for tab af data, som er lagret på krypteret vis. Fremgangsmåde for kryptering kan fås hos Nordicals' IT partner, Support IT.

8.3.1. Bortskaffelse af medier

Når udstyr bortskaffes eller genbruges, skal det sikres at kritiske/følsomme informationer og licensbelagte systemer fjernes eller overskrives. Der er udarbejdet vejledninger, som sikrer, at data på medierne ikke kan genskabes, disse kan findes på Nordicals' Intranet.

8.3.2. Transport af fysiske medier

Fysisk transport af datamedier skal beskyttes mod tab, forvanskning og misbrug af data. Der skal derfor ske transport med pålidelig og troværdig transportør.

9. ADGANGSSTYRING

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

9.1. Forretningsmæssige krav til adgangsstyring

9.1.1. Politik for adgangsstyring

Bestemmelse og udvikling af politiken for adgangsstyring, sker af IT sikkerhedskoordinatoren på Nordicals kædekontor. Politikken er gældende for alle forretninger i Nordicals kæden, når det gælder forretningens

primære fælles mapper på fællesdrev. Implementeringen af adgangsstyringen sker hos Nordicals' IT hosting partner, Support IT.

Forretningernes krav til fysisk adgangskontrol bestemmes af forretningen selv.

9.1.2. Adgang til netværk og netværkstjenester

Nordicals' forretninger arbejder på lokale netværk i den enkelte forretning. For bl.a. at kunne sikre beskyttelse mod ikke godkendte websites, tilslutter samtlige medarbejdere til et hostet miljø, for at få adgang til deres programmer. Det hostede miljø leveres af Support IT, som også sørger for at beskytte mod uautoriserede websites, og download/installation af uautoriseret programmer.

Support IT har den daglige drift og kontrol over hosting miljøet, men træffer ikke overordnede beslutninger uden godkendelse af Nordicals' IT sikkerhedskoordinator.

9.2. Administration af brugeradgang

9.2.1. Brugerregistrering og -afmelding

Brugere oprettet i Support IT's hosting miljø oprettes af Nordicals kædekontor og administreres efter instruks fra Nordicals. Krav til informationer ses af intern formular website, på Support IT's login portal, som er udviklet specielt til Nordicals.

Nordicals har i samarbejde med Support IT, udviklet formularer til oprettelse af medarbejdere i Support IT's hostede miljø. Formularen har påkrævede felter, som sikre af alt relevant information sendes med, og at alle relevante samarbejdspartnere for besked om oprettelsen.

Ved omplacering af medarbejdere skal alle rettigheder for pågældende bruger revurderes af den tilhørende forretnings ledelse.

9.2.2 Tildeling af brugeradgang

Tildeling af privilegier er kontrolleret af den enkelte forretnings daglige ledelse. Som udgangspunkt bliver alle nye brugere oprettet med laveste adgangsniveau, og kan derefter opgraderes hvis nødvendigt, ved at indehaver eller daglig leder sender bekræftelse til Support IT.

9.2.3. Styring af privilegerede adgangsrettigheder

For at få adgang til Nordicals' hostede miljø hos Support IT, skal bruger selv opdatere deres kodeord ved første login i systemet. Kravene til kodeord, er at det skal bestå af minimum 8 karakterer, med minimum 1 stort bogstav, 1 lille bogstav og 1 tal eller specialtegn. Kodeordet må desuden ikke indeholder personlige informationer så som navn, CPR nummer, fødselsdato m.m.

9.2.4. Styring af hemmelig autentifikationsinformation om brugere

Nordicals medarbejdere bliver uddannet i IT-sikkerhed, herunder håndtering af fortrolige informationer såsom deres logon informationer mv. af forskellige instanser. De får ved oprettelse general information om sikkerhed og systemerne fra kædekontoret, og mere uddybende information om brug af disse systemer samt evt. fysiske systemer, af deres tilhørende forretning.

9.2.5. Gennemgang af brugernes adgangsrettigheder

Proceduren for regelmæssig gennemgang af adgangsrettigheder, sker løbende i samarbejde med forretningerne i Nordicals kæden. Ved fakturering af omkostninger for adgang til IT systemerne for brugerne, bliver forretningernes ledelse mindet om at kontrollere tilmeldte bruge re og deres tildelinger af adgangsrettigheder med tilhørende privilegier for at afdække, om uønskede adgangsrettigheder eller privilegier er opnået uden om de gældende vilkår. Overtrædelser indmeldes til kædekontoret.

9.2.6. Nedlæggelse eller tilpasning af adgangsrettigheder

Det er forretningens ledelses ansvar, at de tildelte privilegier ajourføres ved ændring af medarbejdernes arbejdsopgaver, herunder sletning ved medarbejderens fratrædelse.

9.3. Brugernes ansvar

Uautoriseret brugeradgang må ikke kunne forekomme. Opnåelse af betryggende sikkerhed forudsætter, at de autoriserede brugere følger de vedtagne retningslinjer for håndtering af kodeord m.v. Alt hvad der foretages via brugerens brugernavn er entydigt forretningens ansvar. De nedenstående punkter skal derfor overholdes af brugeren, og informeres om af forretningen.

9.3.1. Brug af hemmelig autentifikationsinformation

Kodeord bør, udover at de skal følge Nordicals normale regelsæt for kodeord, konstrueres efter følgende retningslinjer: Undgå "hackervenlige" kodeord såsom egne børns navne, ægtefælles navn, hundens navn og lignende d.v.s. ord, der kan forekomme i en ordbog. Bland bogstaver, tal og/eller specialtegn. Genbrug aldrig kodeord.

Adgangsoplysninger og koder holdes strengt fortrolige.

Se krav til kodeord under punkt 9.2.3.

9.4. Styring af adgang til system- og applikationsadgang

9.4.1. Begrænset adgang til informationer

I Nordicals er der opdelt adgang til data alt efter hvilke roller, de enkelte bruger er tildelt. Se mere om opdelingen under punkt 8.2.3. På lokale miljøer er det op til den enkelte forretning at fastlægge regler for den enkelte bruger, dog skal kædens protokoller fra IT sikkerhedspolitikken som minimum følges.

9.4.2. Procedure for sikker log-on

Medarbejdere i Nordicals kæden, er ved brug af Nordicals hostede miljø hos Support IT beskyttet af flere tiltag for en sikker log-on grænseflade.

For det første sikre Support IT af log-on information opbevares utilgængeligt for alle, se mere under sektion 9.4.3.

Sekundært sikres disse kodeord mod uautoriseret brug, ved at pålægge bruger indtastning når de logger på det hostede miljø. Dette sker på terminal autorisationsniveau, således at selv om bruger har aktiveret browser genkendelse af kodeord, skal koden manuelt indtastes af bruger for at komme ind.

Dette sikre at uautoriserede brugere ikke kan få adgang til det hostede miljø, såfremt en PC skulle blive stålet fra en forretnings fysiske lokation.

9.4.3. System for administration af adgangskoder

Nordicals' IT hosting partner, Support IT, opbevarer kodeord krypteret og utilgængeligt for alle. Support IT har selv ikke adgang til at brugeres adgangskoder, kun nulstille den hvis bruger har glemt adgangskodeord.

9.4.4. Styring af adgang til kildekode.

Adgang til kildekoder styres af Nordicals' kædekontor. Kildekoder, objektkoder og andre fundamentale datakilder opbevares typisk forsvarligt hos Nordicals' IT partner, Support IT. Alt adgang til disse data, styres hos kædekontoret, og udleveres kun til samarbejdspartnere af kædekontorets IT chef.

10. KRYPTOGRAFI

10.1. Kryptografiske kontroller

10.1.1. Politik for anvendelse af kryptografi

Nordicals' kædekontor har udviklet og implementeret kryptografiske metoder, og fået andre gennem leverandører af IT samarbejdspartnere. Der findes introduktion og anvendelses politikker for brug af disse, på Nordicals interne intranet. Nordicals kædekontor opfordrer altid til sikker overførsel af følsom data, ved brug af de kryptografiske metoder. Ansvaret for overholdes af interne metoder og i forbindelse med EU bestemte GDPR regler, tilfalder dog den enkelte forretning som selvstændig juridisk enhed.

10.1.2. Kryptografiske protokoller

I og uden for Nordicals' hostede miljø hos Support IT, forefindes forskellige kryptografiske protokoller, for at dække så mange bruger scenarier som muligt, samtidig med at metoderne holdes så enkle som muligt. Detaljer om brugen af protokollerne, kan findes på Nordicals intranet.

- Sikring af direkte mail kommunikation mellem Nordicals og firmaer med kryptografiske certifikater.
- Sikring af direkte mail kommunikation mellem Nordicals og firmaer med offentlige certifikater.
- Sikring af direkte kommunikation mellem Nordicals og individer uden certifikater, via brug af tilkøbte tredjeparts systemer.

- Sikring af data på hostet miljø via adgangskontrol.
- Sikring af data på lokale miljøer via standard kryptografiske metoder.

11. FYSISK SIKRING OG MILJØSIKRING

Nordicals kæden består af et landsdækkende udvalg af selvstændige forretninger, på franchise koncept. Derfor falder visse områder også ind under forretningens egen ansvarsområde, heriblandt procedure for fysisk sikring af de lejede lokaler. Der findes en oversigt over alle Nordicals forretning, på websitet www.nordicals.dk.

11.1. Sikre områder

11.1.1. Fysisk adgangskontrol

Det er forretningen selv som varetager at uautoriseret personer ikke kan få adgang til de fysiske lokaler, når medarbejdere ikke er til stede. Det er ikke krav om videoovervågning, men alle aktiver skal opbevares forsvarligt uden for åbningstid.

11.2. UDSTYR

11.2.1. Placering og beskyttelse af udstyr

Nordicals anbefaler følgende beskyttelse af datamedier på den personlige arbejdsplads:

- Efterlad ikke udstyr åbent og uovervåget uden at låse med kode.
- Vær opmærksom på faren for tab og kompromittering af data på mobile medier.
- Vær opmærksom på unormal adfærd hos andre, specielt udefrakommende, og rapportér denne information til nærmeste leder eller dennes stedfortræder.

11.2.4. Vedligeholdelse af udstyr

Udstyr som er lejet af kædekontoret gennem Support IT, vedligeholdelse af deres support team på baggrund af aftale mellem Nordicals kæden og Support IT. Er udstyret ikke omfattet af lejeaftale, eller på anden måde uden for aftale i kæden, varetager forretningen selv omkostninger forbundet med service på udstyr.

11.2.5. Sikring af udstyr og aktiver uden for organisationens lokaler

Udstyr som indeholder sensitive informationer, skal opbevares forsvarligt når det forlader forretning ernes fysiske lokationer. Dvs. i aflåst lokale eller f.eks. biler. Personligt mobilt udstyr så som smartphone, tablets eller bærbare computere må ikke efterlades uden opsyn.

11.2.6. Sikker bortskaffelse eller genbrug af udstyr

Udstyr som skal bortskaffes eller genbruges (afskrevet) skal slettes for alt indhold som er firma relateret, inden de forlader firmaets lokationer. Forretningen skal kontakte Nordicals' IT partner Support IT, for introduktion i forsvarlig sletning af indhold, før udstyret gives videre.

11.2.8 Brugerudstyr uden opsyn

Alle Nordicals medarbejdere i forretningerne arbejder på terminal sessioner, hosted af Support IT. Når sessionerne har været inaktive efter 15 minutter, låses sessionen automatisk, og bruger skal logge ind med deres kodeord igen for at åbne for sessionen. Denne regel kan ikke omgås.

Uovervåget udstyr

Data der er lagret på uovervågede pc'er (stationære og bærbare) betragtes i sikkerhedsmæssig henseende som offentligt tilgængelige med mindre maskinen er fysisk beskyttet (låst inde, hvilket betragtes som adgangskontrol). Følsom eller personlige data må ikke lagres på ubeskyttede enheder.

Medbringes data midlertidigt på mobile enheder, skal disse være beskyttet af personlige adgangskoder, samt automatisk låses efter højest 5 minutters inaktivitet.

12. DRIFTSSIKKERHED

Stabil og sikker drift af informationsbehandlingsudstyr og it-drift er afgørende for Nordicals. Det modsatte kan være afgørende kritisk for driften. En høj forsyningssikkerhed og pålidelig administration er væsentlig og foreskriver dokumenterede retningslinjer samt processer med angivelse af ansvar og vedligeholdelse.

Driftsafbrydelser vil forekomme, hvorfor beskrevne og indlærte beredskabsplaner skal medvirke til genetablering og sikring af normal drift. Beredskabsplaner er primært håndteret af Nordicals' IT partner, Support IT, som varetager alt daglig drift af hosting miljøet.

Alt andet IT drift på fysiske lokationer i forretninger, varetages af samarbejdspartnere eller forretningen selv. Såfremt samarbejdspartner er hyret på baggrund af kæde aftale, kan kontakt information til support findes på Nordicals' intranet.

12.1. Driftsprocedure og ansvarsområder

12.1.1. Dokumenterede driftsprocedurer

Driftsafvikling af samtlige kritiske systemer hos Nordicals er fastlagt i beskrevne procedurer hos Support IT, der er kendt af relevant personale. I de beskrevne procedurer skal der fremgå krav til driftstider, systemadgange og sikkerhedskopiering. Krav er fastlagt af Nordicals kædekontor, ved indgåelse af samarbejdsaftale.

12.1.2. Ændringsstyring

Enhver ændring i de kritiske systemer skal styres/ledes og leve op til kravene i denne dokumentation for IT-sikkerhedsregler, afsnit 14 "Anskaffelse, udvikling og vedligeholdelse".

12.1.3 Kapacitetsstyring

IT-systemerne belastning og dimensionering overvåges løbende for at sikre, at nødvendig kapacitet er til rådighed. Belastning skal overvåges således, at opgradering og tilpasning kan finde sted løbende. Dette gælder især for virksomhedskritiske systemer.

I forbindelse med den årlige planlægning vurderes kapacitetsbehov for netværk og maskinel.

Reservekapacitet skal koordineres og kravene til reservekapacitet skal med fastlagte tidsrum revurderes.

Det påhviler den enkelte medarbejder at gøre nærmeste leder opmærksom på ressourceforbruget i forhold til IT-systemer, såfremt nødvendige og tilstrækkelige ressourcer ikke er til rådighed.

12.1.4. Adskillelse af udviklings-, test- og driftsmiljøer

Såfremt Nordicals indgår i udviklings- eller testprojekter skal der sikres fuldstændig adskillelse mellem data til udvikling, test og drift.

12.2. Malwarebeskyttelse

IT-systemer er sårbare over for uautoriserede indgreb eller ændringer. Derfor skal de beskyttes mod indvirkninger fra ondsindede programmer (trojanske heste, orme, logiske bomber, virus) i daglig tale gående under fællesbetegnelsen vira. Selvom Nordicals hosting miljø er beskyttet af systemer hos Support IT, hviler beskyttelse mod vira primært på brugernes opmærksomhed på sikkerheden. Det vil sige, at brugerne skal instrueres om at beskyttelse er den primære sikringsforanstaltning.

12.2.1. Kontroller mod malware

Ejere af IT-aktiver skal være på vagt over for vira. Især skal behovet for sikringsforanstaltninger, som kan beskytte og opdage vira, overvejes.

Flytbare datamedier af fremmed oprindelse skal - ligesom data modtaget via eksterne netværk - kontrolleres for virus, inden de anvendes på systemerne. Eneste undtagelse er data fra IT-systemer, der med sikkerhed vides at være fri for virus. Strategien er dels at forhindre vira i at komme i udbrud, dels at forhindre spredning af virusbefængte filer.

Al elektronisk post og datatrafik, der sker via Nordicals' hostning miljø, scannes for virus og spam samt malware. På hosting miljøet foretages skanning af de permanente filer. Der findes et virusberedskab, der dagligt administrerer overvågningssystemet og analyserer alle alarmer fra virusbeskyttelsen.

For at beskytte mod ulovlig indtrængen udefra skal netværket været beskyttet af en vedligeholdt og overvåget firewall. Der skal foreligge klare og kendte procedure for korrekt håndtering af udstyr ved smitte eller frygt for smitte af virus/malware. Kontakt altid nærmeste leder eller dennes stedfortræder.

Adware beskyttelse baseres på medarbejder-"awareness", sikkerhedsindstillinger i internetbrowser samt begrænsninger i brugeres muligheder for softwareinstallation. (eks. Blokering for automatisk eksekvering af Active X Java Applets mv)

12.3. Backup

Der foretages dagligt en sikkerhedskopiering i Nordicals hosting miljø, som sikrer, at alle Nordicals essentielle data og programmer samt parameteropsætninger, kan gendannes i tilfælde af fejl og uheld. Sikkerhedskopiering på lokale maskiner, er op til den enkelte forretning, såfremt det er nødvendigt. Faciliteterne til sikkerhedskopiering skal være omfattet af de krav, der er anført i Nordicals beredskabsplaner og de specifikke regler vedrørende sikkerhedskopiering for de enkelte systemer skal godkendes af forretningens ledelse.

12.3.1. Backup af information

Sikkerhedskopiering af data gemt i Nordicals hosting miljø foretages af Support IT. Intervaller for opbevaring ses af SLA (Service Level Agreement), eller ved kontakt til IT sikkerhedskoordinatoren på kædekontoret.

12.4. Logning og overvågning

Driftslogning af Nordicals' systemer og data i det hostede miljø, foretages af Support IT til kontrol og efterspring af, hvad der sker i driftsafviklingsforløbet og netværksstyringen.

12.4.1. Hændelseslogning

Sikkerhedshændelser, fejlhændelser og væsentlige brugeraktiviteter på Nordicals' systemer logges.

Fejllogs fra alle IT-systemer, i Nordicals' hostingmiljø, opsamles på den centrale logserver, hvor disse skannes automatisk for uregelmæssigheder og en rapport sendes til den vagthavende IT-medarbejder hos Support IT.

12.4.2. Beskyttelse af log-oplysninger

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

12.4.3. Administrator- og operatørlog

Aktiviteter udført, i Nordicals' hostingmiløø, af systemadministratorer og -operatører samt andre med særlige rettigheder logges.

12.5. Styring af driftssoftware

12.5.1 Softwareinstallation i driftssystemer

Inden ibrugtagning skal driftsafviklingssystemer, netværk og brugersystemer afprøves. Testen skal godkendes af Support IT.

Ved anskaffelse af nye og ved større ændringer af kritiske systemer udarbejdes en kravspecifikation som grundlag for en evt. tilbudsgivning/udbudsforretning.

Ved systemændringer og -opdateringer sker afprøvning som hovedregel ved en grundig afprøvning af et testsystem med samme funktionalitet som produktionssystemet i henhold til kravene i systemets klassificering. Afprøvning sker i samarbejde mellem dataejer og IT-sikkerhedskoordinatoren hos Nordicals.

Produktionssystemerne ændres/opgraderes og afprøves med så få ulemper for brugerne som muligt.

12.6. Sårbarhedsstyring

12.6.1. Styring af tekniske sårbarheder

Nordicals' IT partner vil løbende vurdere tilgængelige sikkerhedsrettelser, for eksempel "patches" eller "hot-fixes", til anvendte operativsystemer. Udrulning/installation skal foretages efter behov.

Større opdateringer skal testes grundigt for kompatibilitet med anvendte applikationer, inden opdateringerne installeres i produktionsmiljøet.

12.6.2. Begrænsninger på softwareinstallation

For at minimere risikoen for utilsigtede ændringer af kildekoder og objektkoder til software skal der foretages kontrol med adgangsrettigheder og privilegier til brug af kildekoder og objektkoder, der findes i programbibliotekerne.

12.7. Overvejelser i forbindelse med audit af informationssystemer

12.7.1. Kontroller i forbindelse med audit af informationssystemer

Revisionskrav og revisionshandlinger i forbindelse med systemer i drift skal planlægges omhyggeligt og aftales med de involverede for at minimere risikoen for forstyrrelser af Nordicals forretningsaktiviteter.

De personer, der udfører revisionen, skal være uafhængige af det reviderede område.

Beskyttelse af revisionsværktøjer

Adgangen til revisionsværktøjer skal begrænses for at forhindre misbrug. Løsning hertil kan være brug af ekstern rådgiver.

13. KOMMUNIKATIONSSIKKERHED

13.1. Styring af netværkssikkerhed

Lokalnetværkets driftsstabilitet i forretningerne og på kædekontoret skal sikres. Ethvert lokalnetværk skal planlægges omhyggeligt og dets funktionalitet skal kontrolleres løbende.

Netværkets tilgængelighed, ydeevne, oppetid og driftsstabilitet skal kontrolleres, dette kan eventuelt ske i samarbejde med Nordicals' IT partner, Support IT. Den enkelte forretning har selv ansvar for at sikre lokal netværket i deres lokaler.

13.1.1. Netværksstyring

Nordicals anvender såvel kablede som trådløse netværk. Det anbefales fra Nordicals kædekontor at netværkene er segmenterede således, at der er fuld adskillelse mellem administration, SRO og gæstebrugere.

Det kablede netværk er det interne net, hvor der ikke er adgang for andre end oprettede administrative brugere.

Gæster, hvis identitet er kendt, må få udleveret kodeord til gæstenettet og tilslutte eget udstyr til gæstenettet, forudsat at udstyret ikke generer andre systemer.

Det trådløse netværk kan og må kun anvendes til internetadgang. Direkte adgang til interne systemer må kun ske med tilladelse fra den ansvarlige for IT-sikkerheden via en krypteret forbindelse (VPN eller lign).

Nordicals har for nylig indgået en aftale med telefoni og internet leverandøren TDC, om etablering af fiber i alle forretninger, som ikke allerede har fiber på lokationer. Aftalen forventes implementeret i Q4 2019.

13.1.2. Sikring af netværkstjenester

Brugere skal kun have adgang til de tjenester, de er autoriseret til at benytte.

Det er tilladt Nordicals brugere at anvende sociale netværkstjenester som f.eks. Facebook, Twitter og LinkedIn fra Nordicals netværk, forudsat at brugen ikke generer eller forhindrer almindelig drift og brug af virksomhedens IT-systemer.

Al anden information om Nordicals, f.eks. præsentationer, billeder, film og andre data må ikke offentliggøres på sociale netværk hvis det kan indebære tvivl om hvorvidt Nordicals bevarer sine rettigheder til informationerne.

13.2. Informationsoverførsel

13.2.1. Politikker og procedurer for informationsoverførsel

Adgangen til det interne netværk fra andre lokationer end Nordicals sker ved brug af login portalen hos Support IT.

13.2.2. Identifikation af netværksudstyr

De enkelte netværksenheder er grupperet inden for en af de følgende 3 kategorier:

Perifere enheder: Betegner netværksudstyr, som er koblet direkte op mod Internettet på mindst et interface, f.eks. firewalls, VPN og dial-in udstyr.

Kerneenheder: Betegner netværksudstyr, som er en del af Nordicals' backbone netværk, f.eks. centrale routere.

Distributions/access enheder: Betegner netværksudstyr, som enten distribuerer trafikken mellem backbone netværket og de enkelte organisatoriske enheder på Nordicals, eller netværksudstyr, som distribuerer trafikken i en enkelt organisatorisk/geografisk enhed, f.eks. fordelingsswitche i lokale krydsfelter.

Det er kun medarbejdere hos Nordicals IT partner, der har administrativ adgang til perifere - og kerneenheder, hvorimod det kan tillades at give andre IT-medarbejdere, herunder også de enkelte forretningers IT-medarbejdere eller samarbejdspartnere, adgang til distributions/access enheder.

Beskyttelse af diagnose- og konfigurationsporte

Forbindelser til diagnoseporte skal sikres mod uautoriseret anvendelse , og adgangen skal kontrolleres. Der skal udarbejdes en procedure således, at diagnoseporte kun er tilgængelige i en tidsbegrænset periode, som er aftalt mellem ejeren og den eksterne leverandørs tekniske personale.

13.2.3. Aftaler om informationsoverførsel

Tab, modifikation eller misbrug af data under forsendelse eller transmittering skal forebygges. Udveksling af data og programmer må kun ske på basis af formelle aftaler.

Der skal indgås skriftlig aftale om al rutinemæssig dataudveksling, således oplysninger sikres, rette kompetencer er til stede og ansvar placeres. Alt data overførsel som er del af et kontinuerlig projekt mellem kædens forretninger og tredjeparts firmaer, og som ikke er midlertidig deling i forbindelse med en sag, skal arrangeres af Nordicals kædekontor.

13.2.4. Elektroniske meddelelser

Alle E-mails eller dokumenter der udveksles via Nordicals systemer tilhører den enkelte forretning i Nordicals, eller kæde for kædekontorets ansatte. Ansatte kan benytte E-mail til privat brug i moderat omfang. Private E-mails skal tydeligt markeres i emnefeltet med "Privat". E-mails kan i særlige tilfælde blive læst af forretningens ledelse.

13.2.5. Fortroligheds- og hemmeligholdelsesaftaler

Der er etableret fortrolighed generelt for alle involverede i vores forretning. Dette sker via ansættelseskontrakter eller samarbejdsaftaler med underleverandører og samarbejdspartnere.

Fortrolige og følsomme oplysninger må ikke komme uvedkommende til kendskab, derfor skal der ske udveksling i krypteret form.

De særlige sikkerhedsrisici i forbindelse med elektronisk dataudveksling skal vurderes iht. datas klassificering.

Print/kopier af følsomme/fortrolige oplysninger må ikke efterlades i printer eller kopimaskine. Disse skal fjernes evt. makuleres straks efter eksekvering af jobbet.

Faren for at røbe følsomme eller fortrolige oplysninger skal iagttages ved samtaler i mobiltelefon i det offentlige rum, eller ved at koble mobilt udstyr til offentligt tilgængelige netværk. Ansatte hos Nordicals skal være opmærksomme på dette og undlade sådanne handlinger, når det er muligt.

14. ANSKAFFELSE, UDVIKLING OG VEDLIGEHOLDELSE AF SYSTEMER

Indkøb, udvikling og implementering af nye systemer skal foregå kontrolleret for at undgå en unødvendig forøgelse af risiko for informationssikkerheden. Implementering af nye systemer foregår altid fra Nordicals kædekontor. Når løsninger implementeres bør sikkerhedsovervejelser altid indgå som en integreret del af processen.

Godkendelsesprocedure ved anskaffelser

Nordicals har indgået samarbejdsaftale med Support IT om indkøb af IT hardware, til forretningerne i Nordicals kæden. Andre aktiver, så som router, switche og telefoni udstyr anskaffes af forretningen, ved brug af kæde opsatte samarbejdsaftaler, eller på egen hånd. Serviceaftaler (SLA) supporteres kun på udstyr der er dækket af samarbejdsaftaler mellem kæden og partnere.

14.1. Sikkerhedskrav til informationsbehandlingssystemer

Det skal sikres, at nyanskaffelser ikke giver anledning til konflikt med eksisterende krav i sikkerhedspolitikken. Anskaffelser må ikke give anledning til forøget risiko for sikkerhedshændelser, med mindre at Nordicals IT-sikkerhedskoordinatoren accepterer den øgede risiko.

14.1.1. Sikring af applikationstjenester på offentlige netværk

Det er driftsleverandørens ansvar at offentlig tilgængelig information, for eksempel på virksomhedens web-server(e), er passende beskyttet mod uautoriserede ændringer.

14.1.2. Elektronisk fakturering

Nordicals henter og sender elektroniske fakturaer via E-conomic. E-conomic systemet har indbygget krypteringsløsninger til afsendelse af sikker mail, så det opfylder samme krav som Nordicals' interne, i forhold til sektion 10.1.

14.2. Sikkerhed i udviklings- og hjælpeprocesser

14.2.1. Sikker udviklingspolitik

Ved indgåelse af samarbejdsaftale med udviklingspartnere, skal Nordicals kædekontor sikre at information som skal bruges til test og drift benyttelse, ikke gives videre til tredjeparter. Data benyttet i forbin delse med udvikling, skal enten være fiktiv eller beskyttet i lukkede miljøer.

14.2.2. Procedure for styring af systemændringer

Der skal føres kontrol med implementering af udvidelser og ændringer af brugersystemer for at minimere fejl og misbrug. Sikkerheds- og kontrolprocedurer må ikke kompromitteres.

14.2.3. Teknisk gennemgang af applikationer efter ændringer af driftplatforme

De ansvarlige for udviklings-, vedligeholdelses- og driftsstøttefunktioner har ansvar for at ændringer bliver gennemgået for at sikre at de ikke kompromitterer sikkerheden i et brugersystem eller dets operationelle miljø. Ansvaret vil primært placeres hos udviklingsfirmaet, men kædekontorets IT medarbejdere vil til tider også være en del af endelig kontrol inden implementering af ændringer.

14.2.4. Begrænsning af ændringer softwarepakker

Ændringer skal begrænses for at fastholde et standardprograms driftsstabilitet. Ændringer til driftstabile programmer, puljes i pakker som opdateres samlet, hvis muligt på faste intervaller. Dette gøres for at opnå rutine i opdateringerne, og dermed genere slutbrugere mindst muligt, og for at reducere omkostninger til ressource forbrug hos udviklingsfirmaet.

14.2.5. Principper for udvikling af sikre systemer

Inddatavalidering skal beskytte brugersystemet mod inddatafejl og skal anvendes, hvor det vurderes hensigtsmæssigt for at sikre, at data overholder formelle formatkrav. Her tænkes specielt på dataudveksling med leverandører osv.

Validering af uddata

Dataejeren skal stille krav om at uddata fra Nordicals systemer eller applikationer løbende valideres med det formål at sikre, data så vidt muligt er korrekte.

14.2.6. Sikkert udviklingsmiljø

Udviklingsmiljø vil så vidt muligt blive placeret hos Nordicals IT hosting partner, Support IT for at sikre miljø mod uautoriseret adgang og sikring af data.

14.2.7. Outsourcet udvikling

I forbindelse med systemudvikling udført af ekstern leverandør bør Nordicals som udgangspunkt kræve:

- Adgang til at overvåge udviklingsprocessen
- Afleveringstest
- Dokumenteret løbende kvalitetssikring
- Deponering af kildekode
- Ophavsrettighed på kildekode

14.3. Testdata

14.3.1. Sikring af testdata

Testdata skal beskyttes og kontrolleres. Brug af virkelige persondata til test skal begrænses. Hvis sådanne data anvendes til test, skal de så vidt muligt anonymiseres.

15. LEVERANDØRFORHOLD

15.1. Informationssikkerhed i leverandørforhold

Nordicals har som naturlig konsekvens af den daglige drift en række eksterne samarbejdspartnere.

Før indgåelse af samarbejde med leverandører og samarbejdspartnere, skal der udarbejdes risikovurderinger i forbindelse med det forventede samarbejde. Leverandøren/samarbejdspartneren, skal tillige dokumentere sikkerhedsprocedurer er indarbejdet i det daglige arbejde. Dette kan ske via dokumenterede politikker/standarder eller underskrevne revisionserklæringer.

Særligt ved håndtering af persondata, skal der være øget opmærksomhed overfor samarbejdspartnere.

15.1.1. Informationssikkerhedspolitik for leverandørforhold

Eksterne serviceleverandører/samarbejdspartnere skal have minimum samme krav til informationssikkerhed som Nordicals; alternativt efterleve Nordicals' informationssikkerhedspolitik. Det er kædekontorets ansvar, at dette sikres.

15.1.2. Håndtering af sikkerhed i leverandøraftaler

Før ethvert samarbejde kan indgås/påbegyndes skal skriftlig dokumentation foreligge. Evt underskrives erklæring om overholdelse af informationssikkerhedspolitik.

15.2. Styring af leverandørydelser

15.2.1. Overvågning og gennemgang af leverandørydelser

Risici ved brug af eksterne serviceleverandørers styring af driftsafvikling skal identificeres og sikkerhedsforanstaltninger skal aftales og fremgå af driftsservicekontrakten.

Anvendelsen af ekstern databehandler skal ske med respekt for Persondatalovens retningslinjer.

Sikkerhedsregler skal i hvert enkelt tilfælde aftales med eksterne serviceleverandører.

15.2.2. Tavshedserklæringer

Det kan I visse tilfælde være nødvendigt at supplementære underskrivelse af overholdelse af IT sikkerhedspolitikken, med underskrivelse af NDA (Non-Disclosure Agreement) af leverandøren, hvis leverandøren skal håndtere forretningsmæssig sensitiv information eller leverandørforholdet omfatter deling af lignende information mellem leverandørfirmaets medarbejder. Underskrevet NDA skal arkiveres ved siden af kontrakten digitalt på kædekontorets fællesdrev.

I forhold til leverandører og samarbejdspartnere, bør der i databehandleraftaler og andre kontrakter fremgå krav til tavshedserklæringer hos den pågældende leverandør/samarbejdspartner for relevant personale.

Der skal under samarbejde med serviceleverandører ske kontrol med overholdelse af gæld ende aftaler. Er der tale om fortløbende samarbejde skal der mindst 1 gang årligt i forbindelse med revision foreligge dokumentation for overholdelse af indgåede aftaler.

15.2.3. Styring af ændringer af leverandørydelser

Såfremt en ekstern serviceleverandør ønsker at foretage ændringer i sit miljø, både af teknisk og fysisk karakter, der har indflydelse på det indgåede samarbejde, skal serviceleverandøren gøre opmærksom på dette. Det er kædekontorets ansvar, at dette klart fremgår ved kontraktindgåelse.

16. STYRING AF INFORMATIONSSIKKERHEDSBRUD

16.1. Styring af informationssikkerhedsbrud og forbedringer

16.1.1. Ansvar og procedurer

Alle Nordicals medarbejdere har ansvar for at indmelde informationssikkerhedsbrud. Medarbejderne skal instrueres om, at alle har ansvar for at reagere ved tegn på sikkerhedstruende eller tabsgivende hændelser under driftsafviklingen. Det er af afgørende, at nødvendige tiltag sker rettidigt, så eventuelle skader minimeres og efterfølgende forebygges.

Sikkerhedshændelser er brud på informationssikkerheden og eksempel kan være: brud på et informationsaktivs tilgængelighed, fortrolighed eller integritet.

Forskellige sikkerhedshændelser kan være forårsaget af:

- Bevidst ondsindet menneskelig handling
    - Indbrud (fysisk eller via netværk)
    - Tyveri
    - Hærværk

- Menneskelige fejl (bevidste/ubevidste)
    - Forretningsgange/procedure/vejledninger følges ikke
    - Manglende uddannelse
    - Brud på adgangskontrol

- Systemfejl

  - Hardwarefejl
  - Fejl i operativsystem
  - Fejl i øvrig software
  - Forsyningssvigt

- Usædvanlige hændelser
  - Gentagelse af indlognings billeder, Malware infektion og udbrud (virus, spyware osv.)

16.1.2. Rapportering af informationssikkerhedshændelser

Ved konstatering af brud eller formodede brud på IT-sikringsforanstaltninger skal rapportering straks ske til IT-sikkerhedskoordinator på Nordicals Kædekontor. Hvis der er tale om brud af kritisk karakter, skal rapporteringen ske til Nordicals IT partner Support, samt kædekontoret.

16.1.3. Rapportering af sikkerhedssvagheder

Ved konstatering af svagheder på IT-sikringsforanstaltninger skal rapportering hurtigst muligt ske til Nordicals kædekontor. Programfejl indrapporteres til leverandøren af produktet.

16.1.4. Vurdering af og beslutning om informationssikkerhedshændelser

Det er IT-sikkerhedskoordinatoren i samarbejde med IT-leverandøren der vurdere om en informationssikkerhedshændelse, skal forfølges og hvilke håndtering der skal tages.

16.1.5. Håndtering af informationssikkerhedsbrud

Alle ansatte i Nordicals har ansvar for at indrapportere til Nordicals kædekontor, såfremt der er mistanke eller vished om sikkerhedshændelse.

IT-sikkerhedskoordinatoren har ansvar for at definere og koordinere en struktureret ledelsesproces, der sikrer en passende reaktion på sikkerhedshændelser.

Ved sikkerhedshændelser, der påvirker informationsaktiver, der kategoriseres som følsomme eller fortrolige, skal øverste ledelse informeres (evt. bestyrelse).

16.1.6. Erfaring af informationssikkerhedsbrud

Alle hændelser skal registreres, ligesom løsningen, der har afhjulpet hændelsen, registreres.

16.1.7. Indsamling af beviser

Hvis et sikkerhedsbrud afstedkommer et retsligt efterspil, uanset om sikkerhedsbruddet er foretaget af en person eller en virksomhed, så skal der indsamles, opbevares og præsenteres et fyldestgørende bevismateriale.

17. INFORMATIONSSIKKERHEDSASPEKTER VED NØD-, BEREDSKABS- OG RETABLERINGSSTYRING

Risikostyring og kriseplanlægning er nødvendige for at sikre Nordicals mod uforudsete hændelser.

Nødplanerne skal være med til at opretholde driften således at skaderne for Nordicals minimeres.

17.1. Informationssikkerhedskontinuitet

- Det skal vurderes, hvordan hændelige og forsætlige ulykker og fejl i IT-systemerne kan indvirke på Nordicals aktiviteter, samt med hvilke midler aktiviteterne kan fortsætte, indtil retablering af IT-systemerne er foretaget.
- De kritiske systemer skal udpeges og prioriteres indbyrdes.
- Tidsrammer for, hvor hurtigt systemerne igen skal være operationelle efter et uheld, fastlægges.
- Ledelsen beslutter hvilke systemer, der skal udarbejdes beredskabsplaner for og har kompetence til at iværksætte dem.

17.1.1. Planlægning af informationssikkerhedskontinuitet

IT-sikkerhedskoordinatoren skal udarbejde og vedligeholde en tværorganisatorisk beredskabsstyringsproces, som skal behandle de krav til informationssikkerhed, der er nødvendige for Nordicals fortsatte drift.

17.1.2. Implementering af informationssikkerhedskontinuitet

Beredskabsplanen skal angive betingelserne for, i hvilke situationer den helt eller delvis skal aktiveres. Den skal præcisere, hvilke persongrupper der har det overordnede ansvar under en IT-beredskabssituation, hvordan de alarmeres, og hvordan den koordinerede indsats organiseres.

Den IT-ansvarlige skal fastlægge en ensartet ramme for Nordicals beredskabsplaner for at sikre, at alle planer er sammenhængende og tilgodeser alle sikkerhedskrav, samt at de fastlægger prioriteringen af afprøvning og vedligeholdelse.

17.2. Redundans

17.2.1. Tilgængelighed af informationsbehandlingsfaciliteter

Det skal være klart defineret, hvem der har ansvaret for aktivering af beredskabsplaner.

Medarbejdere, der udgør en del af beredskabsplaner, skal være informeret om dette ansvar.

Alle medarbejdere skal være informeret om beredskabsplanernes eksistens.

Nordicals kædekontor har overordnet kontakt med forsikringsselskaber i forbindelse med anmeldelse af skade, medmindre skadeomfanget falder ind under forretningens egen forsikringsdækning.

18. OVERENSSTEMMELSE

Mange aspekter af Nordicals virke kan være omfattet af lovgivning eller påvirket af kontrakter eller eksterne parters rettigheder. Nordicals systemer skal være i overensstemmelse med lovbestemte og kontraktlige krav. Forretningsgange, procedurer og politik for IT-sikkerhed skal årligt tages op til vurdering af, om der er behov for justeringer.

18.1. Overensstemmelse med lov- og kontraktkrav

18.1.1. Identifikation af gældende lovgivning og kontraktkrav

Nordicals kædekontor er ansvarlig for at identificere lovgivning der er relevant for Nordicals drift, eller udpege en person der er ansvarlig for denne opgave.

Nordicals kædekontor er ansvarlig for at alle eksterne sikkerhedskrav og Nordicals håndtering heraf, klarlægges, dokumenteres og løbende vedligeholdes.

18.1.2. Immaterielle rettigheder

Materiale, der er beskyttet af ophavsret, må ikke kopieres uden samtykke fra den, der er indehaver af ophavsretten. Ophavsretten er styret ved udstedelse af licenser. Ved salg eller videregivelse af IT-udstyr skal det sikres, at programlicenserne overføres til de nye brugere. I modsat fald skal de berørte programmer slettes, inden IT-udstyret videregives.

18.1.3. Beskyttelse af registreringer

Nordicals lovbestemte data skal beskyttes mod tab, uautoriseret modifikation og forfalskning, herunder:

- Beskyttelse mod tab og manglende tilgængelighed
- Sikring af den nødvendige fortrolighed
- Integriteten opretholdes

18.1.4. Privatlivets fred og beskyttelse af personoplysninger

Nordicals ønsker at overholde persondatalovgivningen, herunder persondataforordningen fra EU. Nordicals privatlivspolitik kan til enhver tid ses på Nordicals website, www.nordicals.dk.

Der må ikke behandles personoplysninger af fortrolig karakter på privat pc.

Lov om behandling af personoplysninger gælder ved enhver opbevaring og behandling af persondata.

Personoplysninger af fortrolig karakter må ikke opbevares eller behandles på bærbar pc, med mindre kryptering anvendes, og at reglerne i persondataloven overholdes.

I forhold til kunder/forbrugere skal der foreligge privatlivspolitikker der beskriver de registreredes rettigheder.

Generelt stræber Nordicals efter behandling og håndtering af data jf. standarderne for god databehandlingsskik.

I henhold til Persondataforordningens artikel 33 stk. 1 skal der ske anmeldelse til Datatilsynet, ved brud på persondatasikkerheden, uden unødig forsinkelse og om muligt senest 72 timer, efter den dataansvarlige er blevet bekendt med bruddet.

18.2. Gennemgang af informationssikkerhed

18.2.1. Uafhængig gennemgang af informationssikkerhed

Nordicals ledelse skal sikre sig, at dens IT-sikkerhedspolitik bliver overholdt, og at vedtagne sikringsforanstaltninger bliver implementeret og fungerer med den tilsigtede effekt. Til dette formål må ledelsen indføre og vedligeholde et betryggende internt kontrolsystem for det daglige arbejde, således at medlemmerne af ledelsen på alle niveauer til stadighed fastholdes på deres ansvar for sikkerheden i eget funktionsområde.

18.2.2. Overensstemmelse med virksomhedens sikkerhedspolitikker og sikkerhedsstandarder

Mindst en gang årligt skal der udføres systematisk opfølgning på overholdelse af sikkerhedspolitikken i hele organisationen. Hver enkelt forretnings leder skal løbende sikre sikkerhedspolitikken bliver overholdt inden for eget ansvarsområde.

18.2.3. Undersøgelse af teknisk overensstemmelse

Løbende kontroller af de tekniske sikringstiltag (Firewall, Antivirusprogram, spamfilter osv.) foretages af kvalificeret personale hos Nordicals IT partner, Support IT eller andre eksterne samarbejdspartnere. Alle tekniske ændringer som ikke er foretaget af Support IT, skal indmeldes til dem. Dette for at Support IT kan levere service funktion og holde overblik over tekniske ændringer.

19. KOMPLEMENTERENDE KONTROLLER

19.1.1. Privatlivspolitik

Nordicals' kunder har ansvaret for at læse Nordicals' privatlivspolitik, som altid kan findes på websitet www.nordicals.dk. Oplysning om privatlivspolitikkens ikrafttræden og lokation, sker på alle relevante dokumenter og websites som leveres og præsenteres for kunden.

19.1.2. Kryptering af kommunikation mellem kunder og Nordicals

Krypering af følsomme eller persondata relaterede kommunikation mellem Nordicals og kunder, vil ske krypteret fra Nordicals side. Det er kundens ansvar at benytte de tilbudte protokoller for svar på krypteret henvendelser, for at sikre at kommunikationen tilbage til Nordicals forretninger, sker på forsvarlig måde.

19.1.3. Sletning af persondata i Nordicals systemer

Kunder eller andre samarbejdspartnere kan til enhver tid få slettet deres persondata i Nordicals' systemer, i henhold til EU persondata lovgivning. Afhængig af dataens placering og type, foregå dette på forskellige måder. Kunder kan altid rette henvendelse direkte til forretningen som opbevare deres data, for at få slettet data vedrørende deres sag.

Nordicals kædekontor opbevarer ikke data på sager, medmindre det er til udviklings eller test formål, og data er dermed fiktive eller anonymiseret som beskrevet i sektion 14.3.1.

20. ÆNDRINGER, KONTAKT OG OPHAVSRET

20.1.1. Ændringer i perioden

Beskrivelse af hvilke forhold, der er ændret i revisionsperioden. Alene væsentlige områder omtales.

- Ingen ændringer siden første udgave, August 2019.

20.1.2. Kontakt oplysninger

Nordicals IT sikkerhedspolitik er udarbejdet af IT chefen for Nordicals kæden. Henvendelser vedrørende sikkerhedspolitikkens udformning eller indhold, kan ske til Nordicals kædekontor på info@nordicals.dk, eller telefon 70 20 41 10.

20.1.3. Ophavsrettigheder