

Nors Vandværk A.M.B.A.



Indholdsfortegnelse

Formål med denne dokumentation	4
Procedure som udføres med persondata	4
Applikationsoversigt	5
Den registreredes rettigheder	6
Sletning af persondata og bogføringsloven.....	6
Godkendte databehandlere	7
Henvendelse vedrørende persondata	7
Kontaktoplysninger til den persondataansvarlige:.....	7
Persondatapolitik for Nors Vandværk	8
Information.....	8
Kontaktoplysninger på persondataansvarlig.....	8
Dataansvarlig.....	8
Opbevaring og sletning af persondata	9
Dine rettigheder efter persondataforordningen.....	9
Oplysninger, som vi videregiver	10
Informationssikkerhed	10
Overholdelse og samarbejde med tilsynsmyndigheder.....	11
Ændringer	11
IT-Sikkerhedspolitik.....	12
Information.....	12
Formål med IT-Sikkerhedspolitik	12
Ledelsens mål og principper	12
Principper for sikkerhedsarbejdet	13
Funktionsadskillelse	13
Fysisk sikkerhed.....	13
Driftssikkerhed.....	13
Risikovurdering	14
Risikovurdering for vandværk	14
IT – Beredskabsplan.....	16
Prioriteret systemliste.....	16

Kontaktlister.....	17
Handlingsplaner – IT Beredskab.....	18
Handlingsplan for interne servere og systemer på vandværket	18
Handlingsplan for eksterne services (leveret af eksterne leverandører, herunder cloudleverandører)	18
Handlingsplan for virus- eller hackerangreb	20
Tekniske og sikkerhedsmæssige foranstaltninger	21
Implementerings - Handlingsplan.....	21

Formål med denne dokumentation

Formålet med denne dokumentation, er at dokumentere at Nors Vandværk overholder kravene til håndtering af persondata.

Ved gennemgangen af Nors vandværks processer, har vi skitseret de arbejdsgange hvori der håndteres persondata. Det er minimalt med persondata som håndteres og det er udelukkende i forbindelse med, at vandværket varetager forbrugernes vandforbrug og afregninger.

Procedure som udføres med persondata

Nors vandværk har registreret almindelige persondata som benyttes til grund for afregning af vandforbrug – hvilket vandværket er kontraktlig og retlig forpligtet til.

Persondata kategorierne er almindelige oplysninger og de videregives ikke til andre personer eller virksomheder, med mindre det er databehandlere. Eksempelvis revisionsvirksomheder som varetager selve forbrugerafregningen.

- Navn
- Adresse
- Telefonnummer
- Mobilnummer
- Mail
- Målernummer
- Kundenummer
- Forbrugsdata
- Matrikelnummer

Applikationsoversigt

- Microsoft Office 365 Business
 - Outlook
 - Word
 - Excel
- Xergi, til aflæsning af kurver, vandforbrug, SMS alarm, via Teamviewer
- Kamstrup, måleraflæsning via Ready – (Persondata)
- Thvilum – aflæsning af ledningsnet

Den registreredes rettigheder

- Ret til at modtage besked fra den dataansvarlige om, at der indsamles oplysninger om en selv
- Ret til indsigt i de oplysninger, der behandles om en selv
- Ret til at gøre indsigelse mod, at behandling af oplysninger finder sted, og hvis indsigelsen er berettiget, skal databehandlingen ophøre
- Ret til at gøre indsigelse mod, at oplysninger om en selv videregives med henblik på markedsføring
- Ret til at gøre indsigelse mod, at man undergives afgørelser, der har retsvirkninger for eller i øvrigt berører en selv i væsentlig grad, og som alene er truffet på grundlag af elektronisk databehandling, f.eks. hvis en arbejdsgiver overlader det til en computer at afgøre, om en jobansøger skal afvises
- Retten til at flytte deres personoplysninger, i Word eller PDF format
- Ret til at få oplysninger, der er urigtige eller vildledende, rettet, slettet eller blokeret, samt i den forbindelse at forlange, at andre, der har modtaget oplysningerne, orienteres om dette
- Ret til at tilbagekalde et samtykke
- Den registrerede har ret til at klage til Datatilsynet over behandling af personoplysninger om en selv

Sletning af persondata og bogføringsloven

Forbrugeren kan ikke forlange at blive slettet fra systemet, så længe forbrugeren har bopæl i forsyningsområdet, idet der skal kunne afregnes vandforbrug. Fraflytter forbrugeren forsyningsområdet og forlanger forbrugeren sine persondata slettet, så slettes forbrugeren persondata 5 år efter fraflytningen i henhold til bogføringsloven.

Godkendte databehandlere

Der er lavet aftaler med nedenstående databehandlere

- Revikon, Per Sørensen, +45 9792 0899, Mail: ps@revikon.dk . Virksomheden varetager forbrugsafregningen pr. husstand.
- Kamstrup, digital måleraflæsning via eButler og Ready

Henvendelse vedrørende persondata

Nors vandværk har indført en procedure som følges af bestyrelsen eller den persondataansvarlige hvis der rettes henvendelser vedrørende persondata. Kontaktoplysninger er tilgængelige via vores hjemmeside.

Kontaktoplysninger til den persondataansvarlige:

Thorsten Balle, telefon +45 22911872, mail info@norsvand.dk

Har bestyrelsen eller den persondataansvarlige brug for rådgivning eller vejledning i forbindelse med IT-sikkerhed og persondata, så kan DVN kontaktes.

Kontaktoplysninger: Peter Toft, tlf.: +45 20 16 55 15, mail: pto@dvn.dk

Persondatapolitik for Nors Vandværk

Information

For at kunne levere vandforsyning er der vigtige personoplysninger, vi har behov for at behandle. Vores persondatapolitik er ment som en hjælp til at forstå, hvilke data vi indsamler, hvorfor vi indsamler dem, og hvad vi anvender dem til. Dette er vigtige oplysninger, så vi håber, at du vil tage dig tid til at læse dem.

Skulle du have spørgsmål, eller ønsker du yderligere information, er du velkommen til at henvende dig til vores persondataansvarlige:

Kontaktoplysninger på persondataansvarlig

Thorsten Balle, telefon +45 2291 1872, mail info@norsvand.dk

Dataansvarlig

Nors Vandværk A.M.B.A.; CVR-nr: 26535891

Dalen 19, 7700 Thisted, telefon +45 2291 1872, mail info@norsvand.dk

Vi behandler personoplysninger, som du eller en anden part, eksempelvis ejendomsmægler eller udlejer, har udleveret til os i forbindelse med din tilflytning til vandværkets forsyningsområde. Endvidere behandler vi løbende oplysninger om dit forbrug af vand.

Disse personoplysninger behandler vi for at kunne leve op til vores kontraktlige forpligtelser overfor dig i forbindelse med afregning af forbrug samt vores forpligtelser i forbindelse med vandforsyningsloven.

Uden disse oplysninger vil vi ikke kunne forsyne dig med vand.

De personoplysninger vi behandler er:

- Navn
- Adresse
- Telefonnummer
- Mobilnummer
- Mail
- Målernummer
- Kundenummer
- Forbrugsdata
- Matrikelnummer

Opbevaring og sletning af persondata

Personoplysninger slettes, så snart de ikke har nogen relevans. Dog opbevarer vi dem altid i minimum 5 år af hensyn til bogføringsloven. Ofte opbevarer vi forbrugsoplysninger længere af hensyn til statistiske formål, eksempelvis i forbindelse med ejerskifte.

Dine rettigheder efter persondataforordningen

I forbindelse med vores behandling af dine personoplysninger følgende rettigheder:

- Ret til at modtage besked fra den dataansvarlige om, at der indsamles oplysninger om en selv
- Ret til indsigt i de oplysninger, der behandles om en selv
- Ret til at gøre indsigelse mod, at behandling af oplysninger finder sted, og hvis indsigelsen er berettiget, skal databehandlingen ophøre
- Ret til at gøre indsigelse mod, at oplysninger om en selv videregives med henblik på markedsføring
- Ret til at gøre indsigelse mod, at man undergives afgørelser, der har retsvirkninger for eller i øvrigt berører en selv i væsentlig grad, og som alene er truffet på grundlag af elektronisk databehandling, f.eks. hvis en arbejdsgiver overlader det til en computer at afgøre, om en jobansøger skal afvises
- Retten til at flytte deres personoplysninger, i Word eller PDF format
- Ret til at få oplysninger, der er urigtige eller vildledende, rettet, slettet eller blokeret, samt i den forbindelse at forlange, at andre, der har modtaget oplysningerne, orienteres om dette
- Ret til at tilbagekalde et samtykke
- Den registrerede har ret til at klage til Datatilsynet over behandling af personoplysninger om en selv

Alle ovenstående rettigheder håndteres manuelt ved henvendelse til vores persondataansvarlige.

Vi kan afvise anmodninger, der er urimeligt gentagende, kræver uforholdsmæssig meget teknisk indgriben (f.eks. at udvikle et nyt system eller ændre en eksisterende praksis væsentligt), påvirker beskyttelsen af andres personlige oplysninger, eller noget som vil være ekstremt upraktisk (f.eks. anmodninger om oplysninger der findes som sikkerhedskopier).

Hvis vi kan rette oplysninger, gør vi naturligvis dette gratis, med mindre det kræver en uforholdsmæssig stor indsats. Vi bestræber os på at vedligeholde vores tjenester på en måde, der beskytter oplysninger fra fejlagtig eller skadelig ødelæggelse. Når vi sletter dine personoplysninger fra vores tjenester, er det derfor muligt, at vi ikke altid kan slette tilhørende kopier fra vores arkivservere med det samme, og det er ikke sikkert, at oplysningerne fjernes fra vores sikkerhedskopisystemer.

Oplysninger, som vi videregiver

Vi videregiver ikke personlige oplysninger til virksomheder, organisationer og enkeltpersoner uden for vandværket. Undtagelsen er i disse tilfælde:

- Med dit samtykke
Vi videregiver personlige oplysninger til virksomheder, organisationer eller enkeltpersoner uden for vandværket, hvis vi har dit samtykke. Vi kræver aktivt tilvalg af videregivelse af alle personoplysninger.
- Til ekstern databehandling
Vi videregiver personlige oplysninger til vores samarbejdspartnere eller andre betroede virksomheder eller personer, der behandler dem for os. Deres behandling er baseret på vores instrukser og i overensstemmelse med vores privatlivspolitik og andre gældende tiltag til fortrolighed og sikkerhed, eksempelvis vores databehandleraftale.
- Af juridiske årsager
Vi videregiver personlige oplysninger til virksomheder, organisationer eller enkeltpersoner uden for vandværket, hvis vi i god tro mener, at adgang, brug, bevarelse eller offentliggørelse af oplysningerne er nødvendig for at:
 - Overholde gældende love, bestemmelser, sagsanlæg eller retsgyldige anmodninger fra offentlige myndigheder.
 - Håndhæve gældende servicevilkår, herunder undersøgelse af potentielle overtrædelser.
 - Registrere, forhindre eller på anden måde beskytte mod problemer med bedrageri, sikkerhed eller tekniske problemer.
 - Holde vandværket fri fra skade, vores medlemmer eller offentlighedens rettigheder, ejendom eller sikkerhed, sådan som det kræves eller tillades i henhold til lovgivningen.

Vi kan dele oplysninger, der ikke identificerer personer, med offentligheden og vores partnere. Vi kan f.eks. dele oplysninger med offentligheden for at vise generelle tendenser om, hvordan vores forbrugeres forbrug fordeler sig.

Informationssikkerhed

Vi bestræber os altid på at sikre vandværket og vores forbrugere mod uautoriseret adgang, ændring, offentliggørelse eller ødelæggelse af personoplysninger, som vi lagrer.

Vi har implementeret følgende organisatoriske og tekniske foranstaltninger generelt på vandværket:

- Antivirus på alle it-systemer, der behandler personoplysninger.
- Backup af alle it-systemer, der behandler personoplysninger.
- Anvendelse af branchetypiske it-systemer til behandlingsaktiviteterne.
- Adgangsbegrænsning til personoplysninger, så der kun gives adgang, hvor det er nødvendigt.
- Databehandleraftaler med leverandører, der behandler personoplysninger på vandværkets vegne.
- Tavshedserklæringer med personale, der har behov for at behandle personoplysninger.
- Vejledning i sikker behandling af personoplysninger og informationsaktiver for personale med adgang til informationssystemer.
- Gennemførelse af ovenstående risikovurdering og dokumentation af alle systemer der behandler personoplysninger for at sikre et oplyst grundlag for sikkerhedsniveauet for persondatabehandlingen i vandværket.

Overholdelse og samarbejde med tilsynsmyndigheder

Vi gennemgår regelmæssigt, at vi overholder vores egen persondatapolitik. Vi overholder også adskillige selvregulerende sikkerhedspolitikker. Når vi modtager formelle skriftlige klager, kontakter vi afsenderen for at følge op på klagen. Vi samarbejder med de relevante lovgivende myndigheder, f.eks. Datatilsynet, om at løse klager om overførsel af personlige data, som vi ikke kan løse direkte med vores brugere.

Ændringer

Vores privatlivspolitik kan ændres fra tid til anden. Vi begrænser ikke dine rettigheder i henhold til denne privatlivspolitik uden dit udtrykkelige samtykke. Eventuelle ændringer af denne privatlivspolitik angives på denne side, og hvis der sker væsentlige ændringer, vil vi gøre opmærksom på dem på en mere iøjnefaldende måde (for visse tjenester oplyser vi bl.a. om ændringer via e-mail).

IT-Sikkerhedspolitik

Information

Denne it-sikkerhedspolitik, som er besluttet af bestyrelsen, udgør den overordnede ramme for at opretholde it-sikkerheden hos Nors Vandværk A.m.b.A. Hermed ønsker vandværket at demonstrere sin seriøse holdning til at skabe sikkerhed for persondata, systemer og andre it-aktiver.

Hensigten er at lægge et fundament, så kritiske og fortrolige informationer og systemer kan bevare deres fortrolighed, integritet og tilgængelighed.

Der bliver fokuseret på de vigtigste krav i EU's generelle persondataforordning.

Formål med IT-Sikkerhedspolitik

Idet brugen af IT anses for at være en meget vigtig forudsætning for vandværkets eksistens, vil det være nødvendigt at sikre vandværkets IT-ressourcer (data, software, hardware og kommunikationsforbindelser).

Derfor vil vi etablere og vedligeholde en afbalanceret it-sikkerhed, som i denne sammenhæng omfatter alle nødvendige organisatoriske, fysiske og tekniske sikkerhedsforanstaltninger.

IT-ressourcerne skal med andre ord beskyttes mod misbrug, manipulation, ødelæggelse og tab, samt mod at blive fejlbehæftede. Beskyttelsen skal virke mod alle former for trusler, interne eller eksterne, hændelige eller bevidste.

Ledelsens mål og principper

Nors Vandværk A.m.b.A ønsker at opnå:

- Fortrolighed og tilgængelighed af persondata i overensstemmelse med kravene i EU's persondataforordning
- Høj driftssikkerhed og minimeret risiko for større nedbrud og tab af data
- Vi ønsker at signalere kvalitet og sammenhæng i brugen af it

It-sikkerhedspolitikken skal danne grundlag for at forebygge og begrænse skader n, for vandværket, kendt og accepteret størrrelse samt sikre fortsat it-drift efter et sikkerhedsbrud – inden for en nærmere defineret tidshorisont.

Principper for sikkerhedsarbejdet

Funktionsadskillelse

Det er ofte vanskeligt at opretholde funktionsadskillelse, men et fravalg af dette princip vil være at sætte it-sikkerheden i fare. Derfor vil vi som minimum kræve (ligesom det er tilfældet ved adgang til kassen/bankbeholdningen), at en anden person (bestyrelsesmedlem, næstformand eller formand) medvirker.

Fysisk sikkerhed

Kritisk it-udstyr skal være anbragt i sikre områder beskyttet af de nødvendige fysiske barrierer, adgangskontroller samt alarmer for at minimere risikoen for uheld og ulykker. Endvidere skal kritisk udstyr sikres mod forsyningsvigt (blandt andet el-, vand- og teleforbindelser).

Driftssikkerhed

Driftssikkerhed drejer sig om at opnå korrekt og sikker drift af faciliteterne, der behandler information.

Heri indgår dokumentering af procedurer for drift og softwareinstallation samt styring af de ændringer, der løbende forekommer og som kan påvirke informationssikkerheden.

Endvidere skal der indføres sikkerhedsforanstaltninger, der kan opdage og forhindre sikkerhedsbrud forårsaget af malware samt efterfølgende sikre genstart af driftssystemerne.

For at sikre at al væsentlig information, software og systemer kan genskabes efter et nedbrud/sikkerhedsbrud, skal der foreligge en backupplan, som følges i praksis. Endelig skal der, hvor det er muligt, gennemføres løbende logning og overvågning af brugeraktivitet med henblik på, at kunne dokumentere hændelsesforløbet i forbindelse med et sikkerhedsbrud.

Desuden skal der gennemføres en styring af tekniske sårbarheder, for at forhindre, at disse udnyttes i skadeligt øjemed.

Risikovurdering

Risikovurdering for vandværk

#	Trussel	Sandsynlighed	Konsekvens	Samlet risikobillede	Forslag til yderligere sikkerhedstiltag for at imødegå de konstaterede trusler
1	Uautoriseret adgang til it-systemer	HØJ	HØJ	KRITISK	Undgå at bruge faste passwords. Indfør personlige passwords samt krav til sværhedsgrad og ændring af passwords
2	At en ansat får uretmæssig adgang til fortrolige data	LAV	MIDDEL	ACCEPTABEL	Lav løbende kontrol af, at brugerrettigheder er korrekte. Opsæt logning på adgang til filer med persondata, gennemse log.
3	Fratrædt bestyrelse får ikke frataget adgangsrettigheder	MIDDEL	MIDDEL	MIDDEL	Implementer procedurer for nedlukning af tidligere medarbejderes it-adgange
4	Vandværket rammes af et ransomware eller virusangreb	HØJ	HØJ	KRITISK	Implementer software, der blokerer trusler proaktivt (før der sker angreb)
5	Samme login og password bruges af flere	MIDDEL	MIDDEL	MIDDEL	Hvis det ikke kan undgås, må logning gøres mere effektiv
6	Datamedier, diske eller dokumenter med fortrolige data bliver stjålet/tabt/glemte, f.eks. under transport	HØJ	HØJ	KRITISK	Indfør værktøjer til at slette data på computeren, hvis den mistes. Efterlad aldrig fortroligt materiale i bil, når den forlades
7	Misbrug af anden brugers adgang da der ikke logges ud efter brug af systemet	MIDDEL	MIDDEL	MIDDEL	Indfør automatisk logoff, når computeren har været inaktiv i 5 minutter (pauseskærm)
8	Brugere skifter ikke adgangskode løbende	HØJ	MIDDEL	MIDDEL	Indfør passwordpolitik, med jævnlig ændring af passwords. Kontroller at den følges
9	Der er fejl på backup, så data ikke kan genskabes ved datatab eller nedbrud	LAV	HØJ	KRITISK	Test jævnligt om backup virker ved at udføre tests af genoprettelse
10	En medarbejder modtager og aktiverer virus eller trojansk hest via e-mail, browser eller usb-nøgle	MIDDEL	HØJ	KRITISK	Indfør sikkerhedsværktøjer, virusscanning af e-mail osv.
11	Brug af privat computer eller brug af firmacomputer til private formål åbner for misbrug eller hacker/virusangreb	HØJ	HØJ	KRITISK	Undlad at gøre brug af privat computer. Brug computer kun til firmaformål/vandværk
12	En ansat lokkes til at udlevere fortrolig/kritisk information til uvedkommende (social engineering)	LAV	MIDDEL	ACCEPTABEL	Informer medarbejdere, om hvad man skal passe på. Lad fortrolighedserklæringer indgå i ansættelsesaftaler/-kontrakter
13					
14					

IT – Beredskabsplan

Prioriteret systemliste

Prioritet (Mest kritiske først)	It-system	Maksimal nødvendig reetableringstid	Mulighed for manuel arbejdsgang i tilfælde af længerevarende nedbrud/utilgængelighed
1	Thvilum	<i>F.eks. 8 timer</i>	
2	Xergi	<i>F.eks. 8 timer</i>	
3	Kamstrup Ready	<i>F.eks. 8 timer</i>	
4	eButler.dk måler aflæsning	<i>F.eks. 8 timer</i>	Foretag manuel aflæsning ved fysisk at besøge alle målere. Bed alternativt forbrugerne om at aflæse.
5		<i>F.eks. 8 timer</i>	
6		<i>F.eks. 8 timer</i>	
7	E-mail	<i>F.eks. 8 timer</i>	Kommunikér vigtige beskeder via telefon.
8	Internetforbindelse på vandværk	<i>F.eks. 8 timer</i>	Brug mobiltelefon som internethotspot. Arbejd alternativt hjemmefra (hvor der er en fungerende internet forbindelse). Ved manglede forbindelse til drift og overvågning på vandværket vil manuel kontrol og drift være nødvendig.
9	PC nedbrud	<i>F.eks. 8 timer</i>	Kontakt evt. DVN og få status på PC, bestil nyt udstyr
10	<i>Indsæt system navn her</i>		

Reetableringstiden sker som udgangspunkt i normal arbejdstid, med mindre andet er aftalt.

Kontaktlister

Intern kontaktliste for vandværket						
Rolle	Primær/substitut	Navn	Adresse	E-mail	Tlf.	Alternativ tlf. og e-mail
Daglig leder på vandværket	Primær					
	Substitut					
Administrativ medarbejder på vandværket	Primær					
	Substitut					
Teknisk medarbejder på vandværket	Primær					
	Substitut					
Bestyrelsesformand	Primær					
Bestyrelsesmedlem	Primær					

Kontaktliste for leverandører						
Rolle	Primær/substitut	Navn	Adresse	E-mail	Tlf.	Alternativ tlf. og e-mail
Thvilum	Primær					
	Substitut					
Kamstrup Ready – Kamstrup	Primær					
	Substitut					
Altibox - Internetforbindelse	Primær					
	Substitut					
Driftsleverandør – computere	Primær	Peter Toft		pto@dvn.dk	20165515	
	Substitut					
Driftsleverandør – inhouse servere	Primær					
	Substitut					
DVN IT Konsulent	Primær	Peter Toft		pto@dvn.dk	20 16 55 15	

Ønsker vandværket at DVN skal assistere i forbindelse med virus og hackerangreb, kan vi godt tilbyde at lave en aftale om leverance og løbende beredskab. Kontakt venligst DVN angående tilbud.

Handlingsplaner – IT Beredskab

Handlingsplan for interne servere og systemer på vandværket

Denne handlingsplan er baseret på interne servere og systemer. Det vil sige systemer, som står på vandværkets adresse, og som vandværket har det fulde driftsansvar for.

I situationer hvor det eksisterende hardware eller infrastruktur ikke kan genbruges, skal der skaffes nyt udstyr til at reetablere it-systemets drift.

Denne handlingsplan er gældende for følgende servere og systemer:

- Lokale computere
- Microsoft Office 365 Business Premium

Nr.	Handling	Beskrivelse	Tid
1	Vurder situationen Status gennemgås, og det vurderes, om eventuelle manuelle arbejdsgange skal iværksættes i forhold til den prioriterede systemliste.	Kontakt relevant leverandør fra kontaktliste.	Start: Slut:
2	Anskaf nyt hardware Fremskaf hardware og relevante komponenter til infrastruktur og etabler ny server/systemmiljø.	Kontakt relevant leverandør fra kontaktliste.	Start: Slut:
3	Anskaf og installer backup Skaf backup og installer den.	Kontakt relevant leverandør eller interessent fra kontaktliste.	Start: Slut:
4	Fastlæg datatab og informer interessenter Fastlæg omfanget af datatabet og informer brugerne og andre interessenter om, hvor stort et tidsrum der mangler i systemet.	Kontakt relevante interessenter fra kontaktliste.	Start: Slut:
5	Implementer almindelige driftsrutiner Implementer de almindelige driftsrutiner og konfigurationer såsom backup, overvågning mv.	Kontakt relevant leverandør eller vandværkskontakt fra kontaktliste.	Start: Slut:
6	Informer relevante interessenter Informer relevante interessenter, når systemet er reetableret og klar til brug. (f.eks. brugere af systemet, samt ledelse).	Kontakt relevante interessenter fra kontaktliste.	Start: Slut:

Handlingsplan for eksterne services (leveret af eksterne leverandører, herunder cloudleverandører)

Ved nedbrud hos en af vandværkets eksterne leverandører skal beredskabet iværksættes, så snart det vurderes at være nødvendigt. Nedenstående handlingsplan har til formål at informere den konkrete leverandør og sikre dialogen med leverandøren under hele forløbet.

Denne handlingsplan er gældende for følgende systemer:

- Kamstrup, måler aflæsning via eButler og Ready
- Thvilum – aflæsning af ledningsnet

Nr.	Handling	Beskrivelse	Tid
1	Vurder situationen Status gennemgås, og det vurderes om eventuelle manuelle arbejdsgange skal iværksættes i forhold til den prioriterede systemliste.	Kontakt evt. relevant leverandør og interessenter fra kontakliste.	Start: Slut:
2	Undersøg leverandørforhold Det undersøges hvilke opgaver, som er outsourcet til den eksterne leverandør.	Kontakt evt. relevant leverandør og interessenter fra kontakliste.	Start: Slut:
3	Kontakt leverandør Hvis dette ikke allerede er sket, f.eks. i tilfælde af at leverandøren har konstateret og informeret om hændelsen, tages kontakt til leverandøren.	Kontakt relevant leverandør fra kontakliste.	Start: Slut:
4	Vurder situationen med leverandøren Status gennemgås, og situationen vurderes i samarbejde med leverandøren. Hvis leverandøren har behov for adgang til vandværkets adresse, aftales det, hvordan adgangen finder sted.	Kontakt evt. relevant leverandør og interessenter fra kontakliste.	Start: Slut:
5	Planlæg indsatsen Planlæg opgaver og aftal det videre forløb.	I samarbejde med leverandør og interessenter.	Start: Slut:
6	Kommunikation og kontakter Planlæg hvordan kommunikationen med leverandøren skal foregå, og oplys kontaktoplysninger til eventuelle øvrige parter, som leverandøren skal kommunikere med.	Kontakt evt. relevant leverandør og interessenter fra kontakliste.	Start: Slut:

Handlingsplan for virus- eller hackerangreb

Handlingsplanen for virus- eller hackerangreb skal sikre en effektiv indsats i tilfælde af virusangreb eller hackerangreb.

Nr.	Handling	Beskrivelse	Tid
1	Vurder situationen Vurder situationen. Hvis der er risiko for, at data kan blive ødelagt eller skadet, afbrydes internetforbindelsen.	Kontakt evt. relevant leverandør og interessenter fra kontakliste.	Start: Slut:
2	Luk systemer Vurder, om der er behov for at lukke systemer for at undgå spredning af angrebet. Informer relevante systemejere, brugere mv.	Kontakt evt. relevant leverandør og interessenter fra kontakliste.	Start: Slut:
3	Iværksæt undersøgelse Iværksæt en undersøgelse af angrebet. Kontakt DVN Peter Toft tlf.: +45 20 16 55 15.	Kontakt evt. relevant leverandør og interessenter fra kontakliste.	Start: Slut:
4	Skift adgangskoder Vurder, om adgangskoder bør skiftes.	Kontakt evt. relevant leverandør og interessenter fra kontakliste.	Start: Slut:
5	Aktiver ekstra systemlogging Vurder, om der bør iværksættes ekstra logging af systemer og netværk for at opklare og indsamle beviser om hændelsen.	Kontakt evt. relevant leverandør og interessenter fra kontakliste.	Start: Slut:
6	Kontakt leverandører Kontakt leverandørerne, hvis de ramte områder driftes eksternt.	Kontakt evt. relevant leverandør og interessenter fra kontakliste.	Start: Slut:
7	Kontakt myndigheder Vurder, om der skal foretages politianmeldelse, og om der er andre myndigheder som bør kontaktes, f.eks. ødelæggelse af persondata.	Kontakt evt. relevant leverandør og interessenter fra kontakliste.	Start: Slut:
8	Informér interessenter Eventuelle øvrige interessenter informeres.	Kontakt interessenter fra kontakliste.	Start: Slut:

Ønsker vandværket at DVN skal assistere i forbindelse med virus og hackerangreb, kan vi godt tilbyde at lave en aftale om leverance og løbende beredskab. Kontakt venligst – Peter Toft tlf.: +45 20 16 55 15.

Tekniske og sikkerhedsmæssige foranstaltninger

Implementerings - Handlingsplan

#	Opgave / Projekt	Status	
1	Der er aflåst gitterlåge omkring vandværket	Gennemført	
2	Der er opsat sensor belysning ude ved gitterlåge	Gennemført	
3	Password er implementeret på vandværkets computer	Gennemført	Opgaven lægges i ledelsessystemet Mitdrikkevand, så der kan følges op på password politik.
4	Pauseskærm aktiveres efter 15 minutter	Gennemført	
5	Nyt backupprogram implementeres	Igangsat	Der implementeres en backup- og restore plan, så retningslinjerne vedr. Persondataforordningen overholdes og vandværkets data sikres.
6	Mapper med forbrugeroplysninger/persondata låses inde i skab på kontor	Igangsat	Der indkøbes nøgleskab så mapper med persondata
7	Makulator er indkøbt til makulering af dokumenter med forbrugernes persondata	Gennemført	
8	Der er implementeret antivirus program på vandværkets computer	Gennemført	
9	I Windows 10 er firewall aktiveret	Gennemført	
10	Internetudbyderens firewall er aktiveret i routeren	Gennemført	TDC routerens firewall er aktiveret på gl. router. Ny udbyder (Altibox) installerer ny internetforbindelse på vandværket. Firewall SKAL kontrolleres. Opgave i Mitdrikkevand
11	Tavshedserklæringer med personale og bestyrelse som behandler persondata	Forslag	DVN foreslår at der implementeres en tavshedserklæring for personale og bestyrelse.

12	Implementering af IT-beredskabsplan	Forslag	DVN bidrager gerne med rådgivning omkring udvikling og vedligehold af en IT-Beredskabsplan og får lagt de faste opgaver ind i Mitdrikkevand kalenderen, så man får tilsikret at den altid vedligeholdes og udvikles i takt med udviklingen på vandværket.
13	Der er alarm på den ejendom hvor administrationen foretages	Gennemført	Nors Vandværk – Administration Dalen 19, 7700 Thisted
14	Ny opgave?		