



Beredskabsplan for it-systemer

Prioriteret systemliste

Prioritet <small>(Mest kritiske først)</small>	It-system	Maksimal nødvendig reetableringstid	Mulighed for manuel arbejdsgang i tilfælde af længerevarende nedbrud/utilgængelighed
1	Telefonforbindelse på vandværk	8 timer	<i>Ved manglede forbindelse til drift og overvågning på vandværket vil manuel kontrol og drift være nødvendig.</i>
2	Lokal filserver til deling og opbevaring af filer	24 timer	
3	webservice	24 timer	
4	E-mail	24 timer	<i>Kommunikér vigtige beskeder via telefon.</i>
5	Kamstrup READy	24 timer	
6	Internetforbindelse	24 timer	<i>Brug mobiltelefon som internethotspot.</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	Formand				
	Substitut	Kasserer				
Administrativ medarbejder på vandværket	Primær	Formand				
	Substitut	Kasserer				
Teknisk medarbejder på vandværket	Primær	Lee Smedie Steen Yding Pedersen	Lee Byvej 55 8850 Bjerringbro	leesmedie@firma.tele.dk	40 18 48 96	86 68 60 06
Bestyrelsesformand	Primær	Se gældende bestyrelse på www.lee-vand.dk under "Bestyrelsen"				
Bestyrelsesmedlem	Primær	Se gældende bestyrelse på www.lee-vand.dk under "Bestyrelsen"				

Kontaktliste for leverandører						
Rolle	Primær/ substitut	Navn	Adresse	E-mail	Tlf.	Alternativ tlf. og e-mail
Kamstrup Ready – Kamstrup	Primær	Kamstrup Support	Industrivej 28 8660 Skanderborg	Support.systems@kamstrup.com		
	Substitut					
TDC – telefon	Primær	TDC				
	Substitut					

Handlingsplaner

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:

- Lokal filserver
- Lokal computer
- Lokal smartphone

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:

Nr.	Handling	Beskrivelse	Tid
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 READY

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 kontaktliste.	Start: Slut:
2	Undersøg leverandørforhold Det undersøges hvilke opgaver, som er outsourcet til den eksterne leverandør.	Kontakt evt. relevant leverandør og interessenter fra kontaktliste.	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 kontaktliste.	Start: Slut:

Nr.	Handling	Beskrivelse	Tid
4	<p>Vurder situationen med leverandøren</p> <p>Status gennemgås, og situationen vurderes i samarbejde med leverandøren. Hvis leverandøren har behov for adgang til vandværkets adresse, aftales det, hvordan adgangen finder sted.</p>	<p>Kontakt evt. relevant leverandør og interessenter fra kontaktliste.</p>	<p>Start:</p> <p>Slut:</p>
5	<p>Planlæg indsatsen</p> <p>Planlæg opgaver og aftal det videre forløb.</p>	<p>I samarbejde med leverandør og interessenter.</p>	<p>Start:</p> <p>Slut:</p>
6	<p>Kommunikation og kontakter</p> <p>Planlæg hvordan kommunikationen med leverandøren skal foregå, og oplys kontaktoplysninger til eventuelle øvrige parter, som leverandøren skal kommunikere med.</p>	<p>Kontakt evt. relevant leverandør og interessenter fra kontaktliste.</p>	<p>Start:</p> <p>Slut:</p>

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 kontaktliste.	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 kontaktliste.	Start: Slut:
3	Iværksæt undersøgelse Iværksæt en undersøgelse af angrebet. Kontakt evt. SOLID-IT.	Kontakt evt. relevant leverandør og interessenter fra kontaktliste.	Start: Slut:
4	Skift adgangskoder Vurder, om adgangskoder bør skiftes.	Kontakt evt. relevant leverandør og interessenter fra kontaktliste.	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 kontaktliste.	Start: Slut:
6	Kontakt leverandører Kontakt leverandørerne, hvis de ramte områder driftes eksternt.	Kontakt evt. relevant leverandør og interessenter fra kontaktliste.	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 kontaktliste.	Start: Slut:
8	Informer interessenter Eventuelle øvrige interessenter informeres.	Kontakt interessenter fra kontaktliste.	Start: Slut: