

Risikovurdering

#	Trussel	Sandsynlighed	Konsekvens	Samlet risikobillede	Kommentarer og forslag til yderligere sikkerhedstiltag for at imødegå de konstaterede trusler
1	Uautoriseret adgang til it-systemer	MIDDEL	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	LAV	ACCEPTABEL	Der foretages løbende kontrol af, at brugerrettigheder er korrekte. Følgende programmer og data ligger kun på administratorens pc: <ul style="list-style-type: none"> • Rambøll vandværksprogram • Målerdata • Office 365 <ul style="list-style-type: none"> ○ Korrespondance med andelshavere Data ligger i Cloud, hvor der er lavet adgangskoder, som kun kendes af administrator og formand: <ul style="list-style-type: none"> • Sms/e-mail service • Målerdata • Løndata
3	Fyrede/fratrådte medarbejdere får ikke frataget adgangsrettigheder	LAV	HØJ	ACCEPTABEL	Fratrådte ansættelser afleverer pc, og der ændres kodeord på pc, interne programmer og eksterne programmer
4	Vandværket rammes af et ransomware eller virusangreb	MIDDEL	HØJ	MIDDEL	Der er installeret antivirus-software på alle pc'ere og pc'erne er opsat til automatisk opdatering af installerede programmer Vandværket har ikke et fælles netværk
5	Samme login og password bruges af flere	MIDDEL	MIDDEL	MIDDEL	Vores SRO styring styres af eksternt firma Der er lavet aftale med leverandøren om styring af adgang til systemet
6	Datamedier, diske eller dokumenter med fortrolige data bliver stjålet/tabt/glemt, f.eks. under transport	MIDDEL	HØJ	KRITISK	Der er etableret kryptering af harddiske, både interne og eksterne
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 10 minutter (pauseskærm)
8	Brugere skifter ikke adgangskode løbende	MIDDEL	MIDDEL	MIDDEL	Der indføres passwordpolitik, så der skiftes password efter 60 dage

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 Backup testes hver 14 dag
10	En medarbejder modtager og aktiverer virus eller trojansk hest via e-mail, browser eller usb-nøgle	MIDDEL	HØJ	MIDDEL	Der er installeret antivirus-software på alle pc'ere og pc'erne er opsat til automatisk opdatering af installerede programmer Der må ikke benyttes "fremmede usb-nøgler, eksterne harddiske o. lign. Vandværket har ikke et fælles netværk
11	Brug af privat computer eller brug af firmacomputer til private formål åbner for misbrug eller hacker/virusangreb	LAV	MIDDEL	ACCEPTABEL	Der er installeret antivirus software på alle pc'ere og pc'erne er opsat til automatiskopdatering af installerede programmer Vandværket har ikke et fælles netværk
12	En ansat lokkes til at udlevere fortrolig/kritisk information til uvedkommende (social engineering)	LAV	MIDDEL	ACCEPTABEL	Fortrolighed er behandlet i ansættelsesaftaler

Revisionshistorik

Version	Note	Dato	Redigeret af
V1.00	Dokument oprettet	25-05-2018	Lil Sørensen & Martin Carlsen