SjekkIT – Informasjonssikkerhet

Mennesker, som enkeltpersoner eller i grupper, har stor betydning for informasjonssikkerhet. Holdninger og organisasjonskultur er noe av grunnlaget for hvordan man forholder seg til sensitiv informasjon. Dette verktøyet forsøker å gi et bilde av atferd, holdninger og kultur som er relatert til informasjonssikkerhet. Verktøyet er utviklet som et samarbeid mellom Nasjonal Sikkerhetsmyndighet, NTNU og SINTEF.

Sentrale definisjoner

Informasjonssikkerhet (IS): Beskyttelse mot brudd på konfidensialitet, integritet og tilgjengelighet. Informasjonen kan finnes muntlig, skriftlig eller på elektronisk form.

Konfidensialitet: sikring av at bare de som er autorisert til å ha tilgang til informasjon har tilgang til den.

Integritet: verning av nøyaktigheten og fullstendigheten av informasjon og behandlingsmetoder.

Tilgjengelighet: sikring av at autoriserte brukere har tilgang til informasjon og tilknyttet utstyr når det er påkrevd.
I tillegg nevnes ofte **autentisering**, som dreier seg om å få visshet om at en part virkelig er den han utgir seg for. Når man bruker et passord eller en PIN-kode, er dette en del av en autentisering.

Uønsket hendelse: en hendelse som *har* eller *kan ha* forårsaket materielle, immaterielle eller menneskelige tap, eller brudd på informasjonssikkerhet, dvs. brudd på konfidensialitet, integritet eller tilgjengelighet.

Risiko: en funksjon av *Sannsynlighet* og *Konsekvens*.

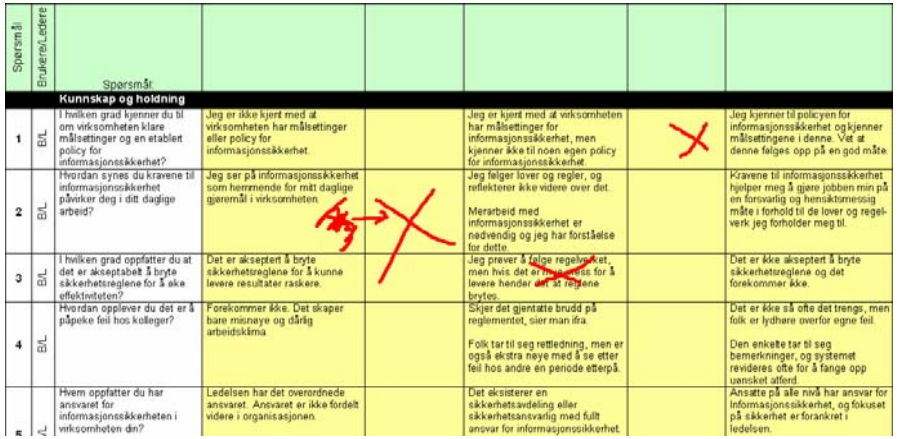
Sårbarhet: et uttrykk for de problemer et system vil få med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med
å gjenoppta sin virksomhet etter at hendelsen har inntruffet.

Gradering: Påføring av en beskyttelsesgrad eller sikkerhets-grad i henhold til sikkerhetsloven og/eller påføring av en beskyttelsesgrad eller sikkerhetsgrad i henhold til andre lover og instrukser, som eksempelvis beskyttelsesinstruksen eller på bakgrunn av en vurdering av virksomhetskritisk informasjon. Uttrykket *gradering* brukes gjennomgående for å dekke disse aspektene i verktøyet.

SjekkIT – informasjonssikkerhet

Legg merke til følgende!

Besvarelsen skal være anonym.
Når vi bruker ordet sikkerhet, så mener vi det som er definert som under informasjonssikkerhet på foregående side.
Alle spørsmålene må besvares.
For hvert spørsmål kan det kun krysses av i én rute.
Hensikten er at du skal svare det som du føler er riktig.



Spørsmål	Brukere/Ledere	Spørsmål					
		Kunnskap og holdning					
1	B/L	I hvilken grad kjenner du til om virksomheten klare målsettinger og en etablert policy for informasjonssikkerhet?	Jeg er ikke kjent med at virksomheten har målsettinger eller policy for informasjonssikkerhet.		Jeg er kjent med at virksomheten har målsettinger for informasjonssikkerhet, men kjenner ikke til noen egen policy for informasjonssikkerhet.	X	Jeg kjenner til policyen for informasjonssikkerhet og kjenner målsettingene i denne. Vet at denne følges opp på en god måte.
2	B/L	Hvordan synes du kravene til informasjonssikkerhet påvirker deg i ditt daglige arbeid?	Jeg ser på informasjonssikkerhet som hemmende for mitt daglige gjøremål i virksomheten.	X	Jeg følger lover og regler, og reflekterer ikke videre over det. Merarbeid med informasjonssikkerhet er nødvendig og jeg har forståelse for dette.		Kravene til informasjonssikkerhet hjelper meg å gjøre jobben min på en forsvarlig og hensiktsmessig måte i forhold til de lover og regelverk jeg forholder meg til.
3	B/L	I hvilken grad oppfatter du at det er akseptabelt å bryte sikkerhetsreglene for å øke effektiviteten?	Det er akseptert å bryte sikkerhetsreglene for å kunne levere resultater raskere.		Jeg prøver å følge regelverket, men hvis det er nødvendig for å levere hender det at reglene brytes.		Det er ikke akseptert å bryte sikkerhetsreglene og det forekommer ikke.
4	B/L	Hvordan opplever du det er å påpeke feil hos kolleger?	Forekommer ikke. Det skaper bare misnøye og dårlig arbeidsklima.		Skjer det gjentatte brudd på reglementet, sier man ifra. Folk tar til seg rettledning, men er også ekstra nøye med å se etter feil hos andre en periode etterpå.		Det er ikke så ofte det trengs, men folk er lydhøre overfor egne feil. Den enkelte tar til seg bemerkninger, og systemet revideres ofte for å fange opp uønsket atferd.
5	L	Hvem oppfatter du har ansvaret for informasjonssikkerheten i virksomheten din?	Ledelsen har det overordnede ansvaret. Ansvaret er ikke fordelt videre i organisasjonen.		Det eksisterer en sikkerhetsavdeling eller sikkerhetsansvarlig med fullt ansvar for informasjonssikkerhet.		Ansatte på alle nivå har ansvar for informasjonssikkerhet, og fokuset på sikkerhet er forankret i ledelsen.

Hvordan skal skjemaet besvares?

For hver kategori skal du sette kryss for det svaralternativet som du synes best beskriver situasjonen i virksomheten. Det er ikke meningen at du skal lese alle rutene – det tar fort for lang tid! Gjør i stedet følgende:

1. Les spørsmålet og gjør deg opp en mening om virksomheten er bra eller dårlig på dette punktet.
2. Begynn og les der du mener virksomheten befinner seg. (Skalaen er forsøkt laget slik at de ”beste”/ideelle svaralternativene er lengst til høyre.)
3. Juster svaret ditt til høyre eller venstre for å finne den beskrivelsen som passer best.

Hver kategori måles på en femtrinns skala, der tre av alternativene er beskrevet. Du vil kanskje ikke finne en rute/beskrivelse som stemmer 100 % overens med det du mener er situasjonen i virksomheten. I så fall velger du den som du mener passer best, eller krysser midt imellom (på rute 2 eller 4) der du mener at dette er riktig.

Når du er ferdig med undersøkelsen, skal svarkortet på siste side fylles ut.

Personlige opplysninger og opplysninger om forholdet til virksomheten

Alder:
- ☐ Under 18
- ☐ 18 - 25
- ☐ 26 - 35
- ☐ 36 - 50
- ☐ 51 - 60
- ☐ Over 60

Kjønn:
- ☐ Mann
- ☐ Kvinne

Nivå i organisasjonen:
- ☐ Leder
- ☐ Medarbeider

Fagområde:
- ☐ Administrasjon
- ☐ Teknisk/drift
- ☐ Sikkerhet
- ☐ Sentralt kontrollrom
- ☐ Ledelse
- ☐ Annet

Ansettelsesforhold?
- ☐ Fast ansatt
- ☐ Deltidsansatt
- ☐ Innleid

Hvor mange virksomheter har du jobbet i, inkludert denne?
- ☐ 1
- ☐ 2
- ☐ 3 - 5
- ☐ 6 eller flere

Høyeste utdannelse:
- ☐ Universitet
- ☐ Høyskole
- ☐ Videregående
- ☐ Annet

Totalt antall år i virksomheten:
- ☐ 0 - 1 år
- ☐ 1 - 5 år
- ☐ 6 - 10 år
- ☐ 11 - 25 år
- ☐ Over 25 år

Trives du i jobben din og med arbeidsoppgavene?
- ☐ Ja
- ☐ Nei

Hva slags erfaring har du med bruk av datamaskiner:
- ☐ Lang erfaring med bruk og programmering av datamaskiner
- ☐ Erfaren, avansert bruker
- ☐ Kan de programmene jeg bruker oftest, men ikke så mye mer

Spørsmål	For Ledere	Spørsmål:	**Patologisk** (Unngå skyld)		**Regelorientert** (Viktigst at regler finnes)		**Ideell** (Lærende organisasjon)
		Kunnskap og holdning					
1		**I hvilken grad kjenner du til om virksomheten har klare målsettinger og en etablert policy for informasjons-sikkerhet?**	Jeg er ikke kjent med at virksomheten har målsettinger eller policy for informasjonssikkerhet.		Jeg er kjent med at virksomheten har målsettinger for informasjonssikkerhet, men kjenner ikke til noen egen policy for informasjonssikkerhet.		Jeg kjenner til policyen for informasjonssikkerhet og kjenner målsettingene i denne. Vet at denne følges opp på en god måte.
2		**Hvordan synes du kravene til informasjonssikkerhet påvirker deg i ditt daglige arbeid?**	Jeg ser på informasjonssikkerhet som hemmende eller ikke relevant for mitt daglige gjøremål i virksomheten.		Jeg følger lover og regler, og reflekterer ikke videre over det. Merarbeid med informasjons-sikkerhet er nødvendig og jeg har forståelse for dette.		Kravene til informasjonssikkerhet hjelper meg å gjøre jobben min på en forsvarlig og hensiktsmessig måte i forhold til de lover og regel-verk jeg forholder meg til.
3		**I hvilken grad oppfatter du at det er akseptabelt å bryte sikkerhetsreglene for å øke effektiviteten?**	Det er akseptert å bryte sikkerhetsreglene for å kunne levere resultater raskere.		Jeg prøver å følge regelverket, men hvis det er mye press for å levere hender det at reglene brytes.		Det er ikke akseptert å bryte sikkerhetsreglene og det forekommer ikke.
4		**Hvordan opplever du det er å påpeke feil hos kolleger?**	Forekommer ikke. Det skaper bare misnøye og dårlig arbeidsklima.		Skjer det gjentatte brudd på reglementet, sier man ifra. Folk tar til seg rettledning, men er også ekstra nøye med å se etter feil hos andre en periode etterpå.		Det er ikke så ofte det trengs, men folk er lydhøre overfor egne feil. Den enkelte tar til seg bemerkninger, og systemet revideres ofte for å fange opp uønsket atferd.
5		**Hvem oppfatter du har ansvaret for informasjonssikkerheten i virksomheten din?**	Ledelsen har det overordnede ansvaret. Ansvaret er ikke fordelt videre i organisasjonen.		Det eksisterer en sikkerhetsavdeling eller sikkerhetsansvarlig med fullt ansvar for informasjonssikkerhet. Ansatte får pålegg og retningslinjer fra sikkerhetsavdelingen.		Ansatte på alle nivå har ansvar for Informasjonssikkerhet, og fokuset på sikkerhet er forankret i ledelsen. Oppgavene løses og følges opp lokalt.

6		**Opplever du at du har fått tilstrekkelig opplæring rundt informasjonssikkerhet og sikker bruk av IT-systemer?**	Jeg har ikke fått opplæring i sikker bruk av IT.		Jeg har fått opplæring i gjeldende regelverk og rutiner for sikker bruk av virksomhetens informasjonssystemer. Opplæringen dekker tiltak og beredskap mot uønskede hendelser.		Ledelsen følger opp gjennom kontinuerlig informasjon og opplæring blant alle brukergrupper. Alle bidrar aktivt i opplæringen.
7		**I hvilken grad får noen skylden dersom en uønsket hendelse inntreffer?**	Enkeltansatte eller samarbeidspartnere blir trukket fram som syndebukker dersom det skjer et sikkerhetsbrudd.		En kombinasjon av tekniske eller personlige feil sees på som årsaker til at hendelser skjer. Systemet i seg selv får ofte skylden for sikkerhets-problemene.		Verken personer eller samarbeidende virksomheter blir syndebukker. Beskyldninger er sjelden noe tema.
8		**Hvordan oppfatter du at informasjon i virksomheten graderes?**	Det finnes ikke, eller jeg kjenner ikke, rutiner for å skille sensitiv og åpen informasjon. Det gjøres ingen verdivurdering av informasjonen.		Det finnes regelverk for å skille mellom sensitiv og åpen informasjon, men jeg kjenner ikke til hvordan de fungerer.		Det finnes graderingssystemer og de ansatte kjenner disse godt slik at ikke informasjon blir feilgradert. Kriterier og rutiner for verdi-vurdering av informasjon følges av de ansatte og videreutvikles og tilpasses løpende.
9		**Hvordan behandler du sensitiv informasjon?**	Tenker sjelden over at sensitiv informasjon skal behandles med forsiktighet.		Er klar over restriksjonene knyttet til sensitivt og sikkerhetsgradert materiale.		Er kjent med utstederen av informasjonen (eierskapet), kjenner hvem som har tilgang og forstår hvorfor informasjonen er sensitiv. Er ”føre var” når jeg kommer i kontakt med sensitiv informasjon.
10		**Hvor god kunnskap har du om spy-ware, virus og ormer?**	Jeg har liten eller ingen kjennskap til dette, og har i liten grad en formening om hvilken skade disse kan forårsake.		Vet hva de vanligste truslene representerer, og er i stand til å beskytte meg mot disse.		Har inngående kunnskap på området, kjenner til de vanligste sikkerhetshullene truslene benytter seg av, og er i stand til å beskytte min PC og nettverket den er tilkoblet.
11		**I hvilken grad har du oversikt over virksomhetens arbeidsprosesser, informasjonssystemer og samspillet mellom disse?**	Jeg har liten oversikt over hvordan rutiner og systemer påvirker hverandre, og vet lite om hvilke konsekvenser en feil i en rutine eller system kan ha for andre systemer.		Jeg har en viss forståelse av sammenhengen mellom rutinene og systemene i virksomheten. Stort sett kan jeg si hvilke konsekvenser mine handlinger har for enkeltsystemer, men har liten oversikt over konsekvenser for tilstøtende systemer.		Jeg kjenner sammenhengen mellom rutiner og systemer godt, og har god forståelse for hvordan feil kan forårsake sikkerhets-brister i andre systemer.

12		**I hvilken grad kjenner du til rutiner for håndtering av IKT-relaterte hendelser i virksomheten?**	Kjenner ikke til at det er rutiner for dette i bedriften.		Vi har etablert rutiner som er gjort kjent.		Det er etablert rutiner for IKT hendelser som er integrert med det vanlige rapporteringssystem.
		Atferd					
13		**Hvilke vaner har du for valg og bruk av brukernavn og passord?**	Skifter aldri passord. Enkelhet prioriteres framfor sikkerhet når du er 2 uker på jobb og 4 uker borte fra jobb.		Bruker samme passord på forskjellige tjenester. Skifter passord av og til.		Skifter passord ut fra en risikovurdering. Benytter passord som er en kombinasjon av tall og store/små bokstaver som er over 7 tegn. Det er laget gode rutiner for å ivareta sikkerheten ifbm offshorearbeid (2 uker på og 4 uker av).
14		**Hvilke e-postvaner har du?**	Åpner og videresender e-post med vedlegg uten å tenke på sikkerheten. Tenker aldri over at e-post kan komme uvedkommende i hende.		Det er laget regler for god e- post skikk som beskriver hvordan e-post skal benyttes.		Er klar over at e-post er et usikkert medium. Avsender kan forfalskes, og vedlegg og lenker kan være skadelige eller feilaktige. Det er laget regler som beskriver hvordan e-post kan brukes sikkert for å sikre at bare rett person får korrekt informasjon uten at andre får innsyn i det.
15		**Hvordan ivaretar du sikkerheten når du surfer på internett?**	Klikker som regel ”OK” på spørsmål. Synes det er vanskelig å vite hva som er rett. Oppgir sensitiv informasjon ukritisk uten å sjekke at nettadressen er ufarlig.		Forsøker å være forsiktig, kontrollerer web-adresser jeg benytter. Det vil si, oppgir ikke personlige opplysninger som brukeridentitet, passord eller annen informasjon uten å være sikker på at web-adressen er ekte. Klikker etter mageføelsen.		Oppgir bare sensitiv opplysning på web-adresser jeg har kontrollert eller hvor sertifikater benyttes.
16		**Hvordan ivaretar du sikkerheten ved arbeid hjemmefra på egen PC?**	Tenker lite på informasjonssikkerhet. Andre personer (f.eks. familie), har full tilgang til min PC. Lagrer arbeidet på egen PC uten å kryptere. Enkelhet prioriteres framfor sikkerhet.		Følger etablerte rutiner. Er klar over restriksjonene knyttet til gradert materiale. Det er etablert gode rutiner for å arbeide sikkert med PC som skal koples opp utenfra i virksomhetens interne nett.		Tar alle forholdsregler og er oppmerksom på at å arbeide på denne måten øker faren for virus og lekkasje av informasjon. Hjemme-PC har samme sikkerhetsnivå som jobb-PC. Bruker kryptert forbindelse til jobben, og lagrer filene mine på en sikker server på jobb.

17		**Hvordan forholder du deg til lovpålagte regler, som for eksempel Sikkerhetsloven og Personopplysningsloven i virksomheten?**	Relevant lovverk er ikke kommunisert ut i virksomheten. Ledelsen eller sikkerhetsansvarlige har noe kjennskap til lovverket. Det er sannsynlig at virksomheten ikke oppfyller alle kravene fordi disse ikke er godt kjent.		Interne prosedyrer blir periodisk sammenlignet med kravene i loven slik at lovverket blir oppfylt.		Vi har jevnlig intern opplæring, og interne rutiner blir løpende oppdatert når lovverket justeres og oppdateres. Det er god forståelse for lovverket, og alle ser nødvendigheten av et lovpålagt regelverk i virksomheten
18		**Hvordan vil du beskrive kontorplassen din når du går fra den?**	Fortrolige papirer ligger åpent og tilgjengelig for hvem som helst. Jeg låser eller stenger PCen sjelden når jeg forlater den.		Følger de etablerte reglene, fortrolige papirer gjøres utilgjengelig for ikke autoriserte. Låser/stenger som regel PCen, men ikke når jeg skal ta en kjapp tur bort fra den (ca 5-15 minutter).		Fortrolige papirer gjøres utilgjengelig for ikke autoriserte personer, og jeg låser alltid PCen når jeg forlater den.
19		**Hvordan ivaretar du sikkerheten ved bruk av mobilt utstyr som eksempelvis bærbar PC, telefon, lomme-PC eller minnepinne?**	Enkelhet prioriteres framfor sikkerhet. Lagrer sensitiv informasjon på mobilt utstyr uten å kryptere eller å ta sikkerhetskopi. Tenker lite på informasjonssikkerhet. Andre personer har tilgang til mitt mobile utstyr.		Jeg følger etablerte rutiner og er klar over restriksjonene knyttet til sensitiv informasjon på mobilt utstyr. Utstyret er beskyttet med passord og informasjon er kryptert.		Informasjon på mobilt utstyr er alltid kryptert og jeg har sikkerhetskopi. Informasjon lagres i utgangspunktet på en sikker server på jobben. Bruker kryptert forbindelse med autentisering ved utveksling av data. Hva man får tilgang på ved arbeid utenfra, er bestemt ut fra en risikovurdering.
20		**I hvilken grad oppfatter du at det er akseptabelt å laste ned og dele opphavsrettslig beskyttet materiale (musikk, film, dokumenter, programvare, bøker, lyd) eller pornografi?**	Fildeling er akseptert og det forekommer. Materiale lagres av og til på lokale filtjenere og på egen PC. Når materiale er tilgjengelig, så kopieres og spres det. Det er en utbredt holdning at dette er helt greit.		Det er etablert regler som forbyr lagring og bruk av opphavsrettslig beskyttet materiale, men det forekommer.		Det er god forståelse for at man ikke kopierer og videreformidler opphavsrettslig beskyttet materiale, og det forekommer heller ikke. Det er god forståelse for at pornografisk materiale kan inneholde virus og at det kan innebære en sikkerhetsrisiko.

21		**I hvilken grad arbeider alle bevisst for å unngå uønskede sikkerhetsrelaterte hendelser?**	Vi ligger i etterkant. Det repareres når hendelser har inntruffet.		Vi prøver å ta vare på sikkerheten, men kommer av og til på etterskudd, for eksempel ved innføring av ny teknologi.		Vi forsøker alltid å ligge i forkant, og jobber systematisk for å forhindre uønskede hendelser. Målet er at det aldri skal forekomme feil i forbindelse med informasjonssikkerhet.
22		**Hvordan vil du reagere når IKT-systemene ikke oppfører seg som forventet?**	Antar at dette går over, slår maskinen av og på.		Rapporterer hendelsen inn i Synergi – og glemmer hendelsen.		Antar at dette kan være ett virus eller IKT uønsket hendelse og rapporterer hendelsen til rette vedkommende.
		Policy og ledelse					
23		**I hvilken grad er ledelsen opptatt av å kommunisere informasjonssikkerhet til ansatte og samarbeidspartnere?**	Ledelsen synes ikke å være spesielt opptatt av informasjons-sikkerhet, ansatte får lite informasjon om informasjonssikkerhet og relevante hendelser.		Ledelsen bryr seg når det har vært en hendelse. Ledelsen informerer om relevante hendelser, men det er mye enveiskommunikasjon.		Ledelsen er løpende opptatt av informasjonssikkerhet og gir ut relevant informasjon (gode eksempler på sikkerhetsbrudd) til medarbeidere og samarbeids-partnere, samtidig som det er god dialog.
24		**I hvilken grad oppfatter du at lederne i virksomheten går foran som gode eksempler når det gjelder informasjonssikkerhet?**	Oppfatter ikke at lederne går foran som gode eksempler.		Lederne går til en viss grad foran som gode eksempler, men i enkelte situasjoner, som f.eks for å nå tidsfrister, bryter de reglene for å nå målene		Lederne går alltid foran som gode eksempler og viser hvordan ting bør gjøres.
25		**I hvilken grad oppfatter du at ansatte inkluderes i arbeidet med informasjonssikkerhet?**	Ledelsen og sikkerhetsansvarlige utreder og kommer med retningslinjer og generelle tiltak uten innspill fra ansatte.		Rapporter og erfaringer fra de ansatte relatert til uønskede hendelser benyttes i utformingen av prosedyrer og regler.		Ansatte blir rådført og deltar i utforming av tiltak, og blir sett på som en viktig ressurs i arbeidet for informasjonssikkerhet. Enkelte ansatte får konkrete oppgaver innen informasjons-sikkerhet.
26		**I hvilken grad utveksles erfaringer med informasjonssikkerhet med andre virksomheter?**	Det hentes lite erfaringer fra andre. Sikkerhetsarbeidet er lukket og internt.		Det fokuseres på å måle informasjonssikkerhet for å kunne sammenligne med andre virksomheter.		Virksomheten deltar aktivt i fagnettverk relatert til informasjonssikkerhet. Virksomheten undersøker stadig hvordan samarbeidspartnere og andre virksomheter, også i andre bransjer og sektorer, jobber med informasjonssikkerhet.
27		**I hvilken grad oppfatter du at samarbeidspartnere og leverandører inkluderes i arbeidet med informasjonssikkerhet?**	Samarbeidspartnere er ikke involvert i utarbeidelse av retningslinjer.		Samarbeidspartnere skal følge virksomhetens prosedyrer, regler og relevant lovverk.		Samarbeidspartnere skal følge virksomhetens prosedyrer, regler og relevant lovverk, men blir også rådført og deltar aktivt i arbeidet for å sikre god informasjonssikkerhet.

28		**Blir informasjonssikkerhet prioritert i forhold til de vanlige daglige gjøremål?**	Det fokuseres kun på å få unna virksomhetens primæroppgaver. Informasjonssikkerhet sees utelukkende på som en ekstra belastning og utgiftspost.		Primæroppgavene er i fokus, men det settes av tilstrekkelige ressurser til å imøtekomme pålegg, bestemmelser og kjente trusler. Det settes av nok ressurser til å gjøre regler kjent. Ved hendelser settes det inn nok ressurser til å opprette stabil drift.		Ressurser prioriteres ut fra en risikovurdering og en kost-/nyttevurdering. Man forsøker å ligge i forkant for å unngå uønskede hendelser. Informasjonssikkerhet er integrert i daglig drift og i utvikling av primæroppgavene.
29		**Hvordan håndteres informasjonssikkerhet i prosjekter?**	Informasjonssikkerhet er ikke et tema når nye prosjekter planlegges. Eventuelle problemer knyttet til informasjonssikkerhet blir utsatt til gjennomføringsfasene av prosjekter og løses etter hvert.		Informasjonssikkerhet blir tatt hensyn til i prosjekter, og deltakerne er alle autoriserte til å kunne gjøre jobben. Prosjektene skal følge etablerte prosedyrer, regler og relevant lovverk.		Når nye prosjekter planlegges blir informasjonssikkerhet vurdert i startfasen. Risiko- og sårbarhetsanalyser gjennomføres og informasjons-sikkerhet testes løpende underveis. Prosjektgruppene har forståelse for at informasjonssikkerhet er av kritisk betydning.
30		**I hvilken grad verdsettes rapportering av uønskede hendelser i virksomheten?**	Jeg får ingen tilbakemelding fra noen om hvordan det går med saken når jeg rapportere videre internt. Jeg velger heller å prøve å løse problemet selv.		Dersom hendelsen er av såpass omfang at den har direkte konsekvenser for mitt daglige arbeid, rapporterer jeg den. Min nærmeste overordnede er den jeg rapporterer til og jeg får tilbakemelding om at min rapportering er mottatt og at noen vil se på saken.		Jeg rapporterer/varsler alltid dersom jeg opplever en sikkerhetsrelatert, uønsket hendelse. Jeg kjenner til hvem i virksomheten jeg skal rapportere ulike typer hendelser til. Jeg opplever at henvendelsen blir tatt på alvor og at det skjer noe. Jeg blir informert om løsningen dersom det er nødvendig og/eller relevant.
31		**I hvilken grad oppfatter du at virksomheten prioriterer sikkerheten ved fjernarbeid, for eksempel ved oppkopling mot virksomhetens nett?**	Enkelhet prioriteres framfor sikkerhet. Det er viktigste er å kunne koble opp utstyr til virksomhetens nett på en enkel måte.		Det er etablert regler for sikkert arbeid med PC som skal kobles opp utenfra i virksomhetens interne nett.		Virksomheten har gode rutiner for fjernarbeid. Jeg er likevel oppmerksom på at fjernarbeid øker faren for virus og lekkasje av informasjon. Tilgang til produksjonsnett gjøres systematisk via sikkerhets-løsninger som eksempelvis Sikker Operasjonsløsning (SOL).

32		**I hvor stor grad er fysiske sikkerhetstiltak etablert for informasjonssystemer?**	Det er få fysiske tiltak for å sikre sensitiv informasjon og systemer. Utenforstående har fri adgang til lokalene.		Virksomheten har adgangskontroll i bygget og virksomhetskritiske informasjonssystemer er fysisk sikret.		Virksomheten er godt sikret med flere nivåer av adgangskontroll på forskjellige områder og lokaler. Ingen besøkende går uten følge uten at dette er avklart med sikkerhetsansvarlig. Kontorer låses, PCer med sensitivt materiell er låst fast og lagringsenhet fjernes og låses vekk.
33	Ledere	**I hvilken grad er det gode kriterier eller rutiner for å velge ut hvilke IT-systemer som skal beskyttes?**	Det er ikke etablerte rutiner for å velge ut hvilke IT-systemer som skal beskyttes.		Sikkerhetsavdelingen har ansvaret for utvelgelse av hvilke IT-systemer som skal beskyttes.		Det eksisterer gode rutiner for å fange opp hvilke IT-systemer som skal beskyttes, og hovedansvaret ligger på sikkerhetsavdelingen.
34	Ledere	**I hvilken grad har virksomheten gode rutiner for å sikre kontinuerlig drift?**	Det er ikke etablert beredskapsplaner. Det fokuseres ikke mye på å unngå uønskede hendelser.		Virksomheten har regler, rutiner og løsninger som trer i kraft ved alvorlige hendelser. Rutinene sikrer kontinuitet ved forventede uønskede hendelser.		Man kjører ofte risiko- og sårbarhetsanalyser, slik at virksomheten til enhver tid har et oppdatert risikobilde. Ved hendelser trer et beredskapsapparat med nødvendige tiltak i kraft, slik at driften kan opprettholdes mens feilen rettes. I ettertid analyseres hendelsen for å kunne unngå tilsvarende hendelser i fremtiden.
35	Ledere	**I hvilken grad er informasjonssystemene, produksjonsnettet og nødsystemer (NAS, B&G) godt sikret mot feil?**	Robusthet og redundans for systemene vurderes sjelden. Enkeltfeil i ett system kan føre til følgefeil i andre systemer.		Det hender informasjonssystemene går ned, men bare i korte perioder. Vanlig drift kan gjenopptas etter kort tid.		Informasjonssystemene er satt opp etter beste praksis og er testet for robusthet. Kritiske komponenter er satt opp med redundans, slik at nedetiden på systemene er neglisjerbar og har ingen innvirkning på drift.

36	Ledere	**Hvordan håndteres informasjonssikkerhet ved outsourcing?**	Informasjonssikkerhet er ikke et tema ved outsourcing. Det legges kun vekt på at jobben gjøres til lavest mulig pris. Ved feil eller hendelser skyves skyld over på tjeneste- eller underleverandør.		Potensielle tjeneste- eller under-leverandører vurderes i forhold til hvordan de ivaretar informasjons-sikkerhet. Leverandøren skal følge virksomhetens prosedyrer, regler og relevant lovverk og dette er kontraktsfestet.		Informasjonssikkerhet er et fokusområde ved outsourcing og er kontraktsfestet. Virksomheten samarbeider med leverandørene for å sikre god informasjonssikkerhet på den outsourcede oppgaven. Leverandøren får bare tilgang til den informasjonen som er nødvendig og har god forståelse for dette.
37		**I hvilken grad mener du det gis gode tilbud for å heve kompetansen på informasjonssikkerhet?**	Kurs og opplæring ses på som nødvendig, men det stjeler tid fra det vi egentlig jobber med.		Systematisk opplæring blir gitt. Det lages systematiske kursplaner. Opplæringen dekker tiltak og beredskap mot uønskede hendelser.		Utvikling av kompetanse blir sett på som en kontinuerlig prosess. Opplæring tilpasses risikobildet og virksomhetens behov.
		Revisjon/Analyse					
38	Ledere	**Hvordan revideres informasjonssikkerhet?**	Revisjon av informasjonssikkerhet skjer kun ved eksternt press og større hendelser.		Det gjennomføres revisjoner for å påse at regler og prosedyrer for informasjonssikkerhet eksisterer og blir fulgt.		Jevnlige revisjoner fokuserer både på kunnskap, atferd og holdninger. Revisjon brukes aktivt for å forbedre virksomhetens rutiner og prosedyrer.
39		**I hvilken grad analyseres inntrufne uønskede hendelser?**	Det gjøres lite analyser av hendelser. Kun større hendelser som rammer betydelige deler av virksomheten følges opp.		Hendelsen analyseres med fokus på etablere en rutine for å unngå samme hendelse igjen. Det gjøres lite oppfølgingsarbeid for å se sammenhenger og få oversikt.		Hendelsen analyseres slik at organisasjonen kan lære og unngå tilsvarende hendelser og ringvirkninger av slike.
40	Ledere	**I hvilken grad gjennomføres risiko- og sårbarhets-analyser?**	De eneste analysene som foregår, er de sikkerhetsansvarliges egne vurderinger som gjøres i det daglige arbeidet. Ledelsen har liten oversikt over risiko.		Det gjennomføres til tider risiko- og sårbarhetsanalyser. Det settes grenser og eventuelle minimumsstandarder for akseptabel risiko, og tiltak settes i verk der risikoen er større enn de fastsatte grensene.		Det gjennomføres ofte risiko- og sårbarhetsanalyser, og virksomheten har løpende fokus på risiko og sårbarheter. Tiltak settes i verk med det samme behovet oppstår.
		Evaluering					
41	B/L	**Hvordan oppfattet du denne undersøkelsen?**	Tidkrevende og unødvendig, ikke relevant.		Helt OK.		Spennende, satte ny fokus og tilførte meg ny kunnskap.

NR:	Spørsmål:	1	2	3	4	5
	Kunnskap og holdning					
1	Klare målsettinger og etablert sikkerhetspolicy					
2	Krav til informasjonssikkerhet påvirker daglig arbeid					
3	Bryte reglene for å øke effektiviteten					
4	Påpeke feil ovenfor kolleger					
5	Ansvar for informasjonssikkerhet i virksomheten					
6	Tilstrekkelig opplæring i bruk av IT-systemene					
7	Skyldspørsmål ved hendelser					
8	Gradering av informasjon					
9	Behandling av sensitiv informasjon					
10	Kunnskaper om ad-ware, spy-ware og virus					
11	Oversikt over arbeidsprosesser og informasjonssystemer					
12	Rutiner for håndtering av IKT-relaterte hendelser					
	Atferd					
13	Brukernavn og passordvaner					
14	E-postvaner					
15	Sikkerhet ved surfing					
16	Arbeid hjemmefra på egen PC					
17	Lovpålagte regler					
18	Kontorplassen din					
19	Sikkerheten ved bruk av mobilt utstyr					
20	Akseptabelt å laste ned og dele materiale					
21	Arbeider bevisst for å unngå uønskede hendelser					
22	IKT-systemene ikke oppfører seg som forventet?					
	Policy og ledelse					
23	Kommunisere sikkerhet					
24	Ledere går foran som gode eksempler					
25	Ansatte inkluderes i arbeid med informasjonssikkerhet					
26	Utveksling av erfaring med andre virksomheter					
27	Inkludering av samarbeidspartnere i arbeid med i.s.					
28	Prioritering av informasjonssikkerhet					
29	Håndtering av informasjonssikkerhet i prosjekter					
30	Verdsetting av rapportering i virksomheten					
31	Prioritering av sikkerhet ved fjernarbeid					
32	Fysiske sikkerhetstiltak					
33	Rutiner for valg av IT-systemer som skal beskyttes					
34	Rutiner for å sikre kontinuerlig drift					
35	Informasjonssystemene godt sikret mot feil					
36	Informasjonssikkerhet ved outsourcing					
37	Tilbud for å heve kompetansen på informasjonssikkerhet					
	Revisjon/Analyse					
38	Revisjon av informasjonssikkerhet					
39	Analyse av inntrufne hendelser					
40	Gjennomføring av risiko og sårbarhetsanalyser					
41	Hva synes du om undersøkelsen (summeres ikke med)					
	(Summer antall enere, toere, osv..) SUM					
		*	*	*	*	*
		1 =	2 =	3 =	4 =	5 =
	Score pr svar nummer					

SUM

/ 40

Gjennomsnittscore =