SjekkIT Sikkerhet av tele- og data-utstyr (11/5-2010)

Datautstyr og teleutstyr er i økende grad en kritisk del av infrastrukturen vi stoler på. Sikkerhet og sikring av slikt utstyr er avhengig av menneskets kunnskap og holdninger og ikke minst organisering og ansvarsforhold. Denne undersøkelsen, SjekkIT, fokuserer på menneskets kunnskap og holdninger som enkeltindivider og i grupper. Vi ønsker å kartlegge og videreutvikle atferd, holdninger og kultur som er relatert til sikkerhet generelt og sikring av tele- og data--utstyr. Dette verktøyet SjekkIT er utviklet som et samarbeid mellom Nasjonal Sikkerhetsmyndighet, Statoil, Hydro, Telenor, NTNU og SINTEF.

Sentrale definisjoner

Sikkerhet: Med sikkerhet mener vi en tilstand hvor vi kontinuerlig tilstreber oversikt, kontroll og styring i forhold til mulige hendelser som kan føre til skade på eller tap av menneskeliv, miljø, materiell, tilgjengelighet, integritet eller konfidensialitet.

Risiko er et uttrykk for kombinasjon av sannsynlighet (frekvens) for skade på menneske, miljø eller materiell og alvorlighetsgraden av denne skaden (konsekvens).

Uønsket hendelse: en hendelse som *har* eller *kan ha* forårsaket materielle, immaterielle, miljømessige eller menneskelige tap, eller brudd på sikkerhet..

Informasjons- og prosess-sikkerhet (IPS): Beskyttelse mot mulige hendelser som kan føre til skade på eller tap av menneskeliv, miljø, materiell, tilgjengelighet, integritet eller konfidensialitet. IPS presiseres via nedenstående:

- **Tilgjengelighet;** sikring av at autoriserte brukere har tilgang til informasjon og tilknyttet utstyr når det er påkrevd.
- **Integritet;** verning av nøyaktigheten og full-stendigheten av informasjon og behandlingsmetoder.
- **Konfidensialitet;** sikring av at bare de som er autorisert til å ha tilgang til informasjon har tilgang til den.

I det følgende bruker vi sikkerhet som det samlende begrepet som også omfatter informasjons- og prosess-sikkerhet (IPS):

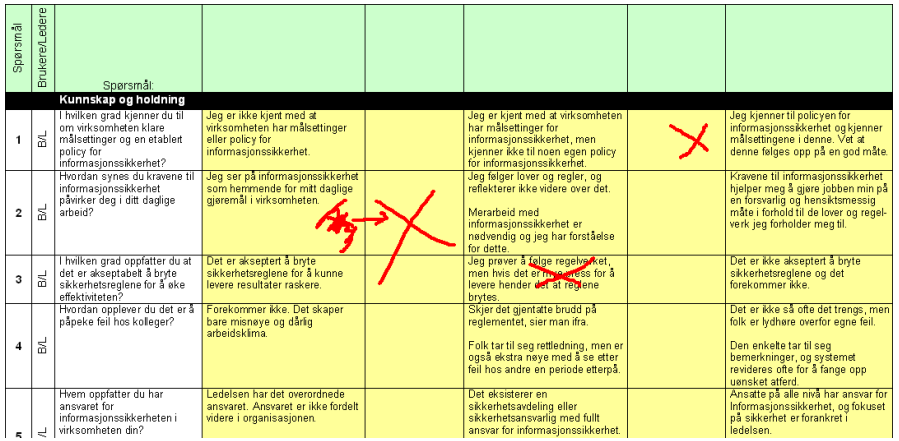
SjekkIT Sikkerhet av tele- og data-utstyr

Legg merke til følgende!

Besvarelsen skal være anonym, men vi ber om at deltakerne krysser av her om de er fra følgende tre områder:

☐ (1)Ledergruppen (& administrasjon),
☐ (2) Drift eller
☐ (3)Servicesenter.

Alle spørsmålene må besvares.
For hvert spørsmål kan det kun krysses av i en rute.
Hensikten er at du skal svare det som du <u>føler og tror</u> 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.:

1. Les spørsmålet og gjør deg opp en mening om virksomheten er bra eller dårlig på dette punktet.
2. Start og lese der du mener virksomheten befinner seg.
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 inn.
Helt til slutt er det laget et åpent tekstfelt for kommentarer.

Nr	Spørsmål:	1 (Unngå skyld)	2	3 (Viktigst at regler finnes)	4	5 (Lærende organisasjon)
	Kunnskap og holdning					
1	**Vet du hva som kan gå galt ved feil eller uønskede hendelser i tele eller datautstyret?**	Jeg er ikke kjent med at det kan skje noen vesentlige ulykker ved uønskede hendelser knyttet til tele eller datautstyret.		Jeg er kjent med at virksomheten har målsettinger for sikkerhet generelt og knyttet til tele- og datautstyr, men kjenner ikke at alvorlige feil kan skje.		Jeg er kjent med risiko- og sårbarhetsanalyser for utstyret, og har oversikt over viktige uønskede hendelser. Uønskede hendelser deles og diskuteres internt og med leverandører og konsulenter.
2	**Vet du hvilket ansvar du har, dvs i hvilken grad kjenner du til om virksomheten har klare målsettinger og en etablert policy for sikkerhet?**	Jeg er ikke kjent med at virksomheten har målsettinger eller policy for sikkerhet knyttet til mitt eget område.		Jeg er kjent med at virksomheten har målsettinger for sikkerhet, men kjenner ikke til noen egen policy eller plan for sikkerhet knyttet til mitt eget område.		Jeg kjenner til policyen (plan) for sikkerhet og kjenner målsettingene i denne. Vet at planene følges opp på en god måte.
3	**Vet du hva du skal gjøre for å hindre uønskede feil eller hva du skal gjøre når du skal håndtere en uønsket hendelse?**	Jeg er ikke kjent med hvem jeg skal kontakte eller hva jeg skal gjøre		Jeg er kjent med at det finnes regler, men jeg bruker de sjelden og trener ikke på uønskede hendelser.		Jeg har trent jevnlig på uønskede hendelser og jeg vet hva jeg skal gjøre ved en uønsket hendelse.
4	**Hvordan synes du kravene til sikkerhet påvirker deg i ditt daglige arbeid?**	Jeg ser på sikkerhet som hemmende eller ikke relevant for mitt daglige gjøremål i virksomheten.		Jeg følger lover og regler, og reflekterer ikke videre over det. Merarbeid med sikkerhet er nødvendig og jeg har forståelse for dette.		Kravene til sikkerhet hjelper meg å gjøre jobben min på en forsvarlig og hensiktsmessig måte i forhold til de lover og regelverk jeg forholder meg til.
5	**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.
6	**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.

Nr	Spørsmål:	1 (Unngå skyld)	2	3 (Viktigst at regler finnes)	4	5 (Lærende organisasjon)
7	**Hvem oppfatter du har ansvaret for sikkerheten 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 sikkerhet (inklusive informasjons-sikkerhet). Fokuset på sikkerhet er forankret i ledelsen. Oppgavene løses og følges opp lokalt.
8	**Opplever du at du har fått tilstrekkelig opplæring rundt sikkerhet og sikker bruk av tele- og data-systemer?**	Jeg har ikke fått opplæring i sikker bruk av tele og data-systemer.		Jeg har fått opplæring i gjeldende regelverk og rutiner for sikker bruk av virksomhetens systemer. Opplæringen dekker tiltak og beredskap mot uønskede hendelser.		Ledelsen følger opp gjennom kontinuerlig informasjon og opplæring blant alle brukergrupper. Alle bidrar aktivt i opplæringen.
9	**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 sikkerhetsproblemene.		Verken personer eller samarbeidende virksomheter blir syndebukker. Beskyldninger er sjelden noe tema – det viktigste er å lære av hendelsen slik at den ikke skjer igjen, og sjekke at vi kan takle den igjen.
10	**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.

Nr	Spørsmål:	1 (Unngå skyld)	2	3 (Viktigst at regler finnes)	4	5 (Lærende organisasjon)
	Atferd					
11	**Hvilke vaner har du for valg og bruk av brukernavn og passord?**	Skifter aldri passord. Enkelhet prioriteres framfor sikkerhet.		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.
12	**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.		Oppgir bare sensitiv opplysning på web-adresser jeg har kontrollert eller hvor sertifikater benyttes.
13	**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. 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.

Nr	Spørsmål:	1 (Unngå skyld)	2	3 (Viktigst at regler finnes)	4	5 (Lærende organisasjon)
	Policy og ledelse					
14	**I hvilken grad er ledelsen opptatt av å kommunisere sikkerhet til ansatte og samarbeidspartnere?**	Ledelsen synes ikke å være spesielt opptatt av sikkerhet, ansatte får lite informasjon om sikkerhet 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 sikkerhet og gir ut relevant informasjon (gode eksempler på sikkerhetsbrudd) til medarbeidere og samarbeidspartnere, samtidig som det er god dialog.
15	**I hvilken grad oppfatter du at lederne i virksomheten går foran som gode eksempler når det gjelder sikkerhet?**	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.
16	**I hvilken grad oppfatter du at ansatte inkluderes i arbeidet med sikkerhet?**	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 sikkerhet. Enkelte ansatte får konkrete oppgaver innen sikkerhet.
17	**Hvordan håndteres sikkerhet (og informasjonssikkerhet) i prosjekter?**	Sikkerhet er ikke et tema når nye prosjekter planlegges. Eventuelle problemer knyttet til sikkerhet blir utsatt til gjennomføringsfasene av prosjekter og løses etter hvert.		Sikkerhet 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 sikkerhet vurdert i startfasen. Risiko- og sårbarhetsanalyser gjennomføres og sikkerhet testes løpende underveis. Prosjektgruppene har forståelse for at sikkerhet er av kritisk betydning.
18	**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 varsler alltid dersom jeg opplever en uønsket hendelse. Jeg kjenner til hvem i virksomheten jeg skal rapportere 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.

Nr	Spørsmål:	1 (Unngå skyld)	2	3 (Viktigst at regler finnes)	4	5 (Lærende organisasjon)
19	**I hvor stor grad er fysiske sikkerhetstiltak etablert for systemer?**	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. PCer med sensitivt materiell er låst fast.
20	**I hvilken grad er det gode kriterier eller rutiner for å velge ut hvilke systemer som skal beskyttes?**	Det er ikke etablerte rutiner for å velge ut hvilke systemer som skal beskyttes.		Sikkerhetsavdelingen har ansvaret for utvelgelse av hvilke systemer som skal beskyttes.		Det eksisterer gode rutiner for å fange opp hvilke systemer som skal beskyttes, og hovedansvaret ligger på eier av systemene i samarbeid med fagmiljøet.
21	**I hvilken grad har virksomheten beredskapsplaner, dvs 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. En trener systematisk, hvert år, på uønskede hendelser hvor en må benytte beredskapsplaner 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.

Nr	Spørsmål:	1 (Unngå skyld)	2	3 (Viktigst at regler finnes)	4	5 (Lærende organisasjon)
	Revisjon/Analyse					
22	**Hvordan revideres sikkerhet?**	Revisjon av sikkerhet skjer kun ved eksternt press og større hendelser.		Det gjennomføres årlige eller sjeldnere revisjoner for å påse at regler og prosedyrer for sikkerhet eksisterer og blir fulgt.		Jevnlige revisjoner fokuserer både på kunnskap, atferd og holdninger. Revisjon brukes aktivt for å forbedre virksomhetens rutiner og prosedyrer.
23	**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 og ansatte (også hos underleverandører) kan lære og unngå tilsvarende hendelser og ringvirkninger av slike.
24	**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. (Ca hvert 3 år) Det settes grenser og eventuelle minimumsstandarder for akseptabel risiko, og tiltak settes i verk der risikoen er større enn de fastsatte grensene.		Det gjennomføres periodiske risiko- og sårbarhetsanalyser, når det er behov, og virksomheten har løpende fokus på risiko og sårbarheter. Tiltak settes i verk med det samme behovet oppstår.

Nr	Spørsmål:	1 (Unngå skyld)	2	3 (Viktigst at regler finnes)	4	5 (Lærende organisasjon)
	Tillegg					
25	**Hvor god kunnskap har du om spy-ware, virus og ormer? (Vet du at ex virus kan spres fra minnepinne?)**	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, og er i stand til å beskytte systemer og nettverket den er tilkoblet.
26	**Hvordan ivaretar du sikkerheten ved bruk av mobilt utstyr som eksempelvis telefon, lomme-PC eller minnepinne?**	Enkelhet prioriteres framfor sikkerhet. Lagrer sensitiv informasjon på mobilt utstyr som minnepinne 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, 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.
27	**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.
28	**Hvordan håndteres sikkerhet når oppgaver utføres av leverandør?**	Sikkerhet er ikke et tema. 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 sikkerhet. Leverandøren skal følge virksomhetens prosedyrer, regler og relevant lovverk og dette er kontraktsfestet.		Sikkerhet er et fokusområde og er kontraktsfestet. Virksomheten samarbeider med leverandørene. Leverandøren får bare tilgang til den informasjonen som er nødvendig og har god forståelse for dette.
29	**I hvilken grad kjenner du til rutiner for håndtering av hendelser/feil knyttet til tele eller data systemer ?**	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/feil som er integrert med det vanlige rapporteringssystem.
	Evaluering					
30	**Hvordan oppfattet du denne undersøkelsen?**	Tidkrevende og unødvendig, ikke relevant.		Helt OK.		Spennende, tilførte meg ny kunnskap.

Svarkortet – siste side

NR:	Spørsmål:	1	2	3	4	5
1	Vet du hva som kan gå galt					
2	Vet du hvilket ansvar du har					
3	Vet du hva du skal gjøre					
4	Krav til sikkerhet påvirker daglig arbeid					
5	Bryte reglene for å øke effektiviteten					
6	Påpeke feil ovenfor kolleger					
7	Ansvar for sikkerhet i virksomheten					
8	Tilstrekkelig opplæring i bruk av systemene					
9	Skyldspørsmål ved hendelser					
10	Behandling av sensitiv informasjon					
11	Brukernavn og Passordvaner					
12	Sikkerhet ved surfing på Internett					
13	Arbeid hjemmefra på egen PC					
14	Kommunisere sikkerhet					
15	Ledere går foran som gode eksempler					
16	Ansatte inkluderes i arbeid med informasjonssikkerhet					
17	Håndtering av sikkerhet i prosjekter					
18	Verdsetting av rapportering i virksomheten					
19	Fysiske sikkerhetstiltak					
20	Rutiner for valg av systemer som skal beskyttes					
21	Rutiner mht beredskapsplaner					
22	Revisjon av informasjonssikkerhet					
23	Analyse av inntrufne hendelser					
24	Gjennomføring av risiko og sårbarhetsanalyser					
25	Kunnskap har du om ad-ware, spy-ware og virus					
26	Sikkerheten ved bruk av mobilt utstyr					
27	Arbeider bevisst for å unngå uønskede hendelser					
28	Sikkerhet når leverandør utfører					
29	Rutiner for håndtering av uønskede hendelser					
	(Summer antall enere, toere, osv..) SUM					
		*	*	*	*	*
		1	2	3	4	5
		=	=	=	=	=
	Score pr svar nummer					

SUM

/ 29

Gjennomsnittscore =

30	Hva synes du om undersøkelsen (summeres ikke med)					

Helt til slutt har vi en tekstboks hvor du kan gi egne synspunkter relatert til denne undersøkelsen, som du ikke har fått gitt uttrykk for.

Egne kommentarer /synspunkter