Informasjonssikkerhet

Informasjonssikkerhet (infoSEC)

Andvord Grafisk bedriver informasjonssikkerhet av to årsaker. Den ene er superenkel, våre kunder krever og forventer det. Våre kunder er humanitære organisasjoner, bank, finans, stat og helse som krever sikkerhet. Den andre årsaken er fordi vi vil beskytte oss selv mot trusler, vi driver en 24/7/365 bedrift uten muligheter til å ta pauser utover noen timer på julaften og 1. påskedag. Vi vil ikke at uvennlige aktører skal stenge bedriften vår via datakablene.

For Andvord Grafisk har informasjonssikkerhet vært en del av hverdagen i årevis men ble aktualisert ytterligere da vi i 2014 begynte å bli revidert etter ISO27001:2013. For mange av våre kunder har InfoSEC vært dagligdags siden 2014, men GDPR aktualiserte det ytterligere for nye kundegrupper som kommuniserer med forbrukere gjennom papir eller på digitale kanaler. Kravene var nesten identisk tidligere, men GDPR tydeliggjorde noen av dem. GDPR er nå iverksatt som «Personopplysningsloven» forkortet POL. Det gir derfor størst mening å bruke begrepet POL i Norge. I tillegg til POL finnes det en rekke regler, forordninger, rutiner og bransjenormer som Andvord Grafisk forholder seg til avhengig av hvilke kundetyper vi er databehandler for. NORMEN for helsevesenet er et eksempel.

Ledelse, ansvar og styringssystemet

InfoSEC drives fremover fra toppen, men gjennomføres i alle prosesser. Prosesser som du som kunde er avhengig av for at det du vil at vi skal gjøre for deg blir gjort. For å sikre at infoSEC gjøres korrekt bruker AG et styringssystem som inneholder en styrende del, en gjennomførende del og en kontrollerende del. Den styrende delen inneholder informasjonssikkerhetsmål, oversikter over hva vi behandler, nivåer for akseptabel risiko, organiseringen av InfoSEC samt instrukser iht. organiseringen. Den gjennomførende delen inneholder oversikter, policyer, prosedyrer, prosessbeskrivelser, planer, annen dokumentasjon og rutinebeskrivelser. Den kontrollerende delen inneholder planer for revisjoner, oppfølginger, gjennomgang på ulike nivåer, avvikshåndtering, testing av prosedyrer og årsrapporteringer.

Risikostyring

Risikostyring drives tradisjonelt etter CIAs metode. Konfidensialitet (C) som skal sikre at kun de som må ha det får tilgang til opplysningene. Integritet (I) skal sikre at opplysningene forblir riktige. Tilgjengelighet (A) betyr at opplysningene må være tilgjengelige når de behøves. I tillegg er det lagt på en R for robusthet. Robusthet betyr at det bør finnes systemer og organisering for å ivareta de tre kravene samt håndtere hendelser hvis noen av dem ikke tilfredsstilles. Under dette punktet gjøres også risikovurderinger og konsekvensvurderinger.

FORTSETTER NESTE SIDE

ISO 27001:2013

«Vi leverer informasjons-sikkerhet, 24/7/365. Du har trygghet for dine og dine kunders sensitive opplysninger»

Pål A. Gaure
Informasjonssikkerhets-ansvarlig

ANDVORD
grafisk

Personvern

Taushetsplikt for våre ansatte er essensielt her. Alle ansatte har skrevet under på dette og drilles flere ganger årlig på hvorfor de har skrevet under denne erklæringen. Ellers er vår virksomhet av en slik art at vi normalt behandler personopplysninger på vegne av kunder og sletter opplysningene etter hver behandling. Krav om innsyn og utlevering av opplysninger treffer derfor ikke den nåværende produksjonen.

Informasjonssikkerhet

Består av en rekke komponenter som virker sammen. De ansattes ryggmargsreflekser og holdninger betyr alt i den daglige produksjonen og opplæring er derfor vesentlig. Vi praktiserer streng tilgangsstyring slikt at kun de som er autorisert, har tilgang. Våre lokaler er fysisk sikret på flere nivåer og fysiske tilganger er begrenset. Vi håndterer teknisk utstyr etter strenge krav og policies. Sikker IT-drift er en kritisk komponent som inneholder konfigurasjonskontroll, endringsstyring, sikkerhetskopiering og logging. Vi har ulike nivåer av drift avhengig av krav fra våre kunder. Styring av sårbarheter og sikkerhetsrevisjoner gjøres kontinuerlig. Kontinuitetstester ligger i grenseland mellom kvalitet og informasjonssikkerhet men for å kunne tilby kontinuitet, altså produksjon uten nedetid må informasjonssikkerheten mellom oss og vår alternative leverandør være på plass. Alternativ leverandør er vårt eierselskap og er således på plass.

Kommunikasjonssikkerhet internt, eksternt og mellom egne fysiske avdelinger skjer etter strenge krav og henger tett sammen med IT-drift og fysisk sikring. Digital kommunikasjon med kunder utover administrativ kommunikasjon skjer via krypterte linjer, via https, sFTP eller andre sikrede kommunikasjonsformer. Vi sørger for at dine ansatte følger retningslinjene i kommunikasjonen med oss.

Leverandørforhold og avtaler

AG bruker ikke underleverandører uten at vi minimum har en databehandleravtale, der dette er påkrevet. Vi har normalt en skriftlig, oppdatert avtale med viktige underleverandører.
Vi sørger også alltid for at vi har en databehandleravtale med våre kunder før vi igangsetter produksjon som krever en slik avtale.

Håndtering av informasjonssikkerhetsbrudd

Våre prosjektledere og Service Managers er trent på hendelseshåndtering, hendelsesvarslinger og kjenner konsekvensen av å ikke varsle. Vi sier fra hvis du ikke følger reglene, vi sier fra hvis vi ikke følger reglene.

ANDVORD
grafisk

Andvord Grafisk AS
– Et selskap i Parajett-gruppen
Brennaveien 20B, 1481 Hagan
22 72 66 00 / ag@andvord.no
andvordgrafisk.no