Sikkerhetsmål og -strategi

1 Innledning

Sikkerhetsmål og strategi er Tappin ASs overordnet styrende dokument for informasjonssikkerhet.

Ledelsen i Tappin AS har det overordnede ansvaret for all informasjonssikkerhet hos Tappin AS. Sikkerhetsansvarlig har ansvar for utarbeidelse av mål og strategi for informasjonssikkerhet, utarbeidelse av rutiner samt kontroll med at rutinene følges.

Sikkerhetsmålene beskriver hva som ønskes oppnådd sikkerhetsmessig, mens sikkerhetsstrategien beskriver hvilke tiltak som skal gjennomføres for å oppnå sikkerhetsmålene.

2 Sikkerhetsmål

Sikkerhetsmålene skal understøtte og sikre virksomhetens drift, allmenne tillit og omdømme i det offentlige rom, ved å forebygge og begrense konsekvensene av uønskede hendelser. Sikkerhetsmålene beskriver Tappin ASs overordnete mål for beskyttelse av virksomhetens informasjonsbehandling mot interne og eksterne trusler av tilsiktet og utilsiktet art.
Det overordnede formålet med Tappin ASs behandling av personopplysninger er *Drift av arrangementsapper og tilhørende systemer for kunder og partnere.*

Følgende sikkerhetsmål er definert:

1. Tappin AS skal sikre at informasjon behandles iht krav i relevante lover og forskrifter.
2. Sikkerheten ved Tappin AS skal ha forankring i ledelsen ved Tappin AS.
3. Sikkerheten skal ivaretas som en integrert del av hele Tappin ASs organisasjon.
4. Den fysiske sikkerhet ved Tappin AS skal hindre at uautoriserte får adgang til lokaler der beskyttelsesverdig informasjon og sensitive personopplysninger lagres og behandles.
5. Tilgang til systemer og informasjon gis kun til medarbeidere etter behov (Need to Know).
6. Tilgang til systemer og informasjon for uvedkommende skal forhindres.
7. Tappin AS skal sikre at informasjonsbehandling er korrekt og at informasjon ikke forandres uten lovlig tilgang.
8. Tappin AS skal sikre tilgjengelighet til systemer, tjenester og informasjon til rett tid for de personer som er autorisert.
9. Det skal være mulig å spore uønskede hendelser.
10. Det skal være tatt i bruk rutiner for å håndtere uønskede inkludert virksomhetskritiske hendelser.
11. Det skal være tatt i bruk systematiske læreprosesser ved uønskede hendelser slik at sannsynlighet for tilsvarende eller gjentatte hendelser reduseres

12. Forhindre at personer eller systemer hos Tappin AS bevisst eller ubevisst er årsak til sikkerhetsmessig uønskede hendelser mot egen eller andre virksomheter eller privatpersoner.
13. Tappin AS skal sikre at medarbeidere som bruker Tappin ASs informasjonssystemer har en tilstrekkelig kompetanse for å ivareta virksomhetens sikkerhetsbehov/krav.

Regelverk

- Personopplysningsloven
- Personopplysningsforskriften

Andre relevante lover/forskrifter

- Sikkerhetsloven
- Straffeloven
- Arbeidsmiljøloven

Mer informasjon om lovene og forskrifter finnes på www.lovdata.no.

3 Sikkerhetsstrategi

3.1 Organisering av sikkerheten

Sikkerhetsansvarlig

Sikkerhetsansvarlig ved Tappin AS har et overordnet utøvende ansvar for informasjonssikkerheten i Tappin AS. Ansvaret innebærer å organisere, koordinere og styre sikkerhetsarbeidet, utarbeide retningslinjer, iverksette egenkontroll, gjennomføre forbedringsprosesser samt følge opp at sikkerheten vedlikeholdes i alle ledd. Sikkerhetsansvarlig har videre myndighet og ansvar til blant annet å kunne gjennomføre opplæring i informasjonssikkerhet, risikovurderinger, sikkerhetstester, avvikshåndtering, iverksette korrigerende og andre sikkerhetsrelaterte tiltak. Sikkerhetsansvarlig rapporterer til Ledelsen i Tappin AS i sikkerhetssaker. Ansvarsområdet reguleres av stillingsbeskrivelse.

Organisering

Deler av operativt sikkerhetsansvar vil normalt delegeres til personer i ulike avdelinger. Sikkerhetsorganiseringen skal til enhver tid fremgå av egen beskrivelse der roller og personer (inkludert kontaktinformasjon) inngår.

Kontrakter Alle formaliteter mellom Tappin AS og leverandører skal være formulert i formelle kontrakter (SLA - Service Level Agreement) og skal inkludere relevante sikkerhetskrav. Tappin AS skal alltid ha rett til innsyn og måling av hvorvidt sikkerhetskrav etterleves av en leverandør.

Egenkontroll

- Egenkontroll/måling av sikkerhetsnivå ved Tappin AS skal utføres regelmessig iht. systematiserte rutiner.
- Avvik fra sikkerhetsmål og strategi samt vedtatte rutiner og styrende dokumenter skal håndteres som en del av avvikshåndtering, se 3.9.

3.2 Personell og sikkerhet

Generell taushetserklæring

Alle som får tilgang til beskyttelsesverdig opplysninger om Tappin AS skal underskrive en taushetserklæring. Dette gjelder Tappin ASs ansatte, leverandørers ansatte eller andre som måtte komme i kontakt med slik informasjon.

Sikkerhetsinstruks

Alt personell med tilgang til informasjonssystemene skal underskrive ”Sikkerhetsinstruks bruker".

Kompetanse

Ansatte hos Tappin AS skal gjennom opplæring og rutiner oppnå tilstrekkelig kunnskap til å forvalte informasjon og systemer på en sikker måte. Endringer i konfigurasjon av systemer og nettverk skal bare utføres av kvalifisert personell, og etter godkjenning fra Tappin AS.

Konsekvenser ved sikkerhetsbrudd

Brudd på sikkerhetsreglene beskrevet i sikkerhetsinstrukser, taushetserklæring og eventuell konfidensialitetserklæring, vil bli vurdert i henhold til de lover som står beskrevet i kap. 2.1 og kan få følger for ansettelsesforholdet.

3.3 Fysisk sikkerhet

Soneinndeling og adgangskontroll

- Adgang til Tappin ASs lokaler for eksternt (og internt) personell skal godkjennes av aktuell linjeleder og følge retningslinjer for tildeling av adgang. Adgang skal begrenses til det minimum av lokaler som vedkommende har behov for.
- Adgangskontroll med bruk av adgangskort med personlig kode utenfor arbeidstid eller nøkkel skal være montert.
- Arkiv, serverrom og rom med annet sentralt IT-utstyr skal sikres og plasseres slik at det er mulig å begrense adgangen til området. Dør til slike områder skal alltid være låst. Dette gjelder også rom med sensitive personopplysninger og opplysninger gradert etter sikkerhetsloven.
- Utrangerte harddisker beskyttes tilsvarende servere.
- Ytterdører skal være låst etter arbeidstidens slutt.
- Når kontor forlates skal kontordør låses .
- Reserve besøkskort, adgangskort, nøkler og passord skal lagres i safe eller på annen sikker måte.

Alarmsystemer

- Tappin ASs adgangskontrollsystem skal gi alarm ved forsøk på uautorisert adgang til vaktselskap.
- Tappin ASs døgnkontinuerlig innbruddsovervåking skal gi automatisk alarm til egen vakt.

3.4 Tilgang til informasjonssystem

- Nærmeste linjeleder er ansvarlig for å klarlegge og autorisere en ansatts behov for tilgang og formidle dette til IT-avdelingen ved ansettelse eller endringer i ansvar.
- Informasjonseier har ansvaret for å godkjenne tilgang til egen forvaltet informasjon.

- Nærmeste linjeleder er ansvarlig for å melde til IT-avdelingen at personell slutter slik at tilgangsrettigheter fjernes.
- IT-avdelingen eller den IT-avdelingen bemyndiger er ansvarlig for å vedlikeholde tilgangsrettigheter samt holde oversikt over de tilgangsrettigheter som er gitt.
- Linjeleder er ansvarlig for at verifikasjon av tilgangsrettigheter gjøres.

3.5 Dokumentsikkerhet

Alle dokumenter og lagringsmedia som inneholder beskyttelsesverdig informasjon, skal oppbevares, forsendes og destrueres på en slik måte at det ikke kommer uvedkommende i hende.

3.6 Konfigurasjonskontroll

Oversikt over gyldig sikkerhetsdokumentasjon, utstyr, programvare og systemkonfigurasjon skal utarbeides og vedlikeholdes.

- IT-avdelingen har ansvaret for å utarbeide og vedlikeholde oversikt over utstyr, programvare og systemkonfigurasjon.
- Sikkerhetsansvarlig har ansvaret for å utarbeide og vedlikeholde oversikt over sikkerhetsdokumentasjon.

3.7 Endringskontroll

- Ved endringer i Tappin ASs informasjonssystemer skal alltid beskyttelsesbehov vurderes, og om endring kan ha konsekvenser for sikkerheten.
- Endringer som kan ha konsekvenser for informasjonssikkerheten, skal godkjennes av sikkerhetsansvarlig.
- For endringer som kan ha sikkerhetsmessig konsekvens, skal IT-avdelingen utarbeide en risikovurdering inkludert forslag til tiltak som oversendes sikkerhetsansvarlig som en del av endringsforespørsel.
- Sikkerhet skal være et vurderingspunkt gjennom alle faser av en endring.
- Krav til sikkerhet og overordnet vurdering av risiko skal inngå i eventuelle forprosjekt.
- Ved en eventuell kontrakt med tredjepart skal krav til sikkerhet inngå i kontrakten.
- Produksjonsdata som inneholder sensitive personopplysninger skal anonymiseres før de benyttes ved tester knyttet til endringer.
- Sikkerhetsnivå skal verifiseres før endringer idriftsettes.

3.8 Beredskap

Det skal etableres en beredskapsplan som dekker:

- Ansvar og vaktordning for håndtering av hendelser.
- Effektiv håndtering sikres gjennom rutiner som er tilgjengelig for relevante personer.
- Hendelser skal håndteres i henhold til hendelsens alvorlighet.
- Varslingsrutiner skal eksistere der både relevant personell hos Tappin AS og partnere inngår.
- Drift og kontinuitetsplan for å gjenopprette normaldrift skal finnes.

Tiltak for å hindre uhell/kriser

- Brann: Det skal være automatisk branndeteksjon, og varsling til brannvesen
  - for tekniske rom, serverrom, operasjonsrom, fortrinnsvis med automatisk brannslukningsutstyr.
  - i kontorer og korridorer.
- Vann: Sikring mot vannlekkasje i relevante rom (der servere er plassert).
- Tyveri/innbrudd: Skal detektere og forhindre innbrudd. Innbruddsalarm tilknyttet vaktsentral med utrykning ved alarm.
- Brann eller andre uhell skal ikke slette eller ødelegge virksomhetskritisk informasjon.
- Strømsvikt og -ustabilitet: informasjonssystemene skal sikres mot overspenninger, servere skal beskyttes mot utilsiktet strømbrudd og separat strømforsyning skal være tilgjengelig.

3.9 Avvikshåndtering

- Alvorlige hendelser av sikkerhetsmessig betydning skal alltid rapporteres til sikkerhetsansvarlig.
- Ved alvorlige hendelser skal sikkerhetsansvarlig involveres i oppfølging og beslutning av korrigerende tiltak knyttet til hendelsen.
  - Sikkerhetsansvarlig har ansvar for oppfølging og beslutning av korrigerende tiltak som gjelder hendelser ved brudd på konfidensialitet eller integritet samt enkeltpersoners brudd på sikkerhetsreglene.
  - Hvis personopplysninger er kommet på avveie eller det er mistanke om det samme, skal Datatilsynet orienteres.
  - IT driftsansvarlig har ansvar for oppfølging og beslutning av korrigerende tiltak som gjelder hendelser relatert til tilgjengelighet på systemer og tjenester

3.10 Systemteknisk sikkerhet

3.10.1 Nødvendig sikkerhetsnivå – høy, middels, lav

Avhengig av det aktuelle system og informasjonen som behandles, vil de ulike aspektene ved sikkerhet (tilgjengelighet, konfidensialitet og integritet) ha ulik betydning. Følgende kategorisering benyttes for beskyttelsesbehov:

- Høy - gis bare systemer og informasjon med virksomhetskritisk beskyttelsesbehov.
- Middels - gis systemer og informasjon med beskyttelsesbehov.
- Lav, (lave krav til sikkerhet) kan gjelde alle systemer og informasjon med lite eller ingen beskyttelsesbehov.

Ulike delsystemer kan ha ulike beskyttelsesbehov.

3.10.2 Krav til dokumentasjon av beskyttelsesbehov

- Tappin AS skal vedlikeholde en oversikt over personopplysninger og andre digitale verdier som informasjonssystemer og eksterne kommunikasjonsgrensesnitt med faktisk beskyttelsesbehov.
- Tappin AS skal vedlikeholde kriterier for valg av beskyttelsesbehov.
- Sikkerhetstiltak skal vurderes og iverksettes i henhold til definert beskyttelsesbehov.

- Vurdering av beskyttelsesbehov skal inngå i alle system- eller infrastruktur endringer som kan påvirke informasjonssikkerheten.

3.10.3 Strategi for systemteknisk sikkerhet

Generelt

- Sikkerhetstiltak for Tappin ASs nettverk og systemer skal aldri basere seg på at system, person, eller virksomhet det kommuniseres med har en "sikker" infrastruktur, Tappin ASs lokale tiltak skal alltid iverksettes for å minimalisere risiko.
- Sikkerhetsbehov skal alltid vurderes relatert til hvor virksomhetskritiske systemene er (se over "Nødvendig sikkerhetsnivå").

Datakommunikasjon

- Tappin ASs nett skal inndeles i soner der hver sone bare utveksler relevant trafikk med andre interne/eksterne soner. Eksempler kan være driftsnett, server- sone og lignende.
- Brannmurer og tilsvarende sikkerhetsbarrierer skal benyttes for å oppnå et sikkert skille mellom Tappin AS og eksterne nett.
- All ekstern kommunikasjon skal rutes via sikkerhetsbarrierer som filtrerer ulovlige tjenester, uønsket informasjon, adresser og trafikkretning.
- Det skal benyttes to sikkerhetsbarrierer mellom sikret sone og eksternt nettverk for behandling av sensitive personopplysninger.
- Det skal være elektronisk overvåking av ekstern nettverkstrafikk/kommunikasjon mot virksomhetskritiske systemer og nettverk ved Tappin AS.
- Support fra leverandører over eksterne linjer skal benytte VPN-løsning med kryptering. Tilkoplingen i Tappin ASs nettverk skal aktivt åpnes/lukkes etter behov. Dersom det likevel etter en risiko/nyttevurdering anses som påkrevd med kontinuerlig forbindelse skal tilkobling skje i egen nettverkssone der trafikk overvåkes og kontrolleres.

Infrastruktur

- Mekanismer i underliggende nettverkskomponenter, operativsystem og annen programvare skal benyttes for å oppnå at brukere bare har tilgang til relevant informasjon.
- Autentiseringsmekanismer skal alltid være integrert med og bygge på underliggende autentiseringsmekanismer i operativsystem og nettverk.
- Antall passord eller tilsvarende som en bruker må kunne skal minimaliseres
- Automatisk passordbeskyttet skjermsparer skal benyttes.
- Systemene skal regelmessig oppdateres med relevante sikkerhetspatcher.
- Server og klienter skal være herdet mot innbrudd og nedetid.
- To-nivå automatisk viruskontroll og med automatisk oppdatering av signaturer skal være iverksatt. Med to-nivå menes intern viruskontroll og viruskontroll på ytre barriere.
- PC som ikke eies av Tappin AS, skal ikke tilkobles Tappin ASs nettverk. Dersom det likevel etter en risiko/nyttevurdering anses som påkrevd skal tilkobling skje i egen nettverkssone der trafikk overvåkes og kontrolleres.

- Alle PC'er tilknyttet Tappin ASs nettverk skal være innkjøpt, forvaltet og konfigurert av IT-avdelingen.
- På bærbare PC'er som benyttes til å lagre sensitive personopplysninger og eller annen sensitiv informasjon, skal harddisk (eller relevante deler av denne) krypteres, samt at beskyttelse mot endringer ved oppstart skal iverksettes.
- Bærbare PC'er kan bare koples direkte til eksternt nett dersom de er konfigurert og godkjent av IT-avdelingen.
- Informasjonssystemer skal være konfigurert til å logge uautorisert tilgang eller forsøk på uautorisert tilgang.
- Tilgang relatert til brukere skal være sporbart til brukernavn/-identifikasjon
- Utførelse av rutiner for egenkontroll og drift, samt håndtering av sikkerhetsrelaterte hendelser eller hendelser knyttet til manglende stabil drift, skal logges.
- Programvare- og maskinvare-plattformer benyttet i Tappin ASs informasjonssystem skal være standardisert. Det er ikke tillatt å installere egen programvare, all installasjon skal utføres av IT-avdelingen eller de som IT-avdelingen delegerer dette til.
- Tappin AS systemer og nettverk skal ha synkroniserte klokker.
- IT-avdelingen skal vedlikeholde en oversikt over beskyttelsesbehov for et gitt system, dette kan inkludere oversikt over hvilke informasjonsfelter som må beskyttes med indikasjon av nødvendig sikkerhetsnivå.

3.10.4 Tappin ASs spesifikke applikasjoner

For Tappin ASs spesifikke applikasjoner, dvs applikasjoner som utvikles spesielt for Tappin ASs, gjelder følgende:

- Ansvaret for håndtering av sikkerhetsbehov i Tappin ASs spesifikke applikasjoner ligger hos systemeier. Utøvende ansvar kan delegeres til prosjektleder eller andre navngitte personer.
- All programvare skal utvikles på bakgrunn av detaljerte kravspesifikasjoner der også krav til sikkerhet inngår.
- Teknisk sikkerhetsnivå skal verifiseres i alle prosjektets faser ved utvikling.
- Før programvaren/systemer settes i produksjon, skal teknisk sikkerhetsnivå verifiseres. Ved feil eller mangler skal retting av eventuelle feil/mangler gjennomføres før systemet settes i produksjon. Rettelser av feil og mangler skal verifiseres.
- Før programmer eller systemer settes i produksjon skal rutiner for drift, proaktiv overvåkning og beredskap være iverksatt.
- Verifikasjon av sikkerhet gjennom test skal utføres av andre personer enn de som har vært med på å utvikle systemet eller personer som drifter systemer.

Sikkerhetsansvarlig har ansvaret for selve gjennomføringen av testen og formidler resultatene tilbake til prosjektet.