Praecom tietoturvakäytännöt

Praecomin Tietohallinto ja tietoturvahenkilöstö huolehtivat Praecomin tietojärjestelmien eheydestä ja turvallisuudesta.

Tietoturvalla tarkoitetaan kaikkien tietojen turvallista käsittelyä niiden muodosta riippumatta. Tietoturva on tietojen luottamuksellisuuden, eheyden ja käytettävyyden varmistamista.

Praecomin liiketoiminta edellyttää tietojärjestelmiä, jotka toimivat virheettömästi ja turvallisesti. Tämän varmistamiseksi tietoturvaa seurataan aktiivisesti ja poikkeamiin puututaan ennalta määrättyjen menettelyjen mukaisesti.

Tietoturvaa toteutetaan ja kehitetään ratkaisuilla, jotka ovat riskien kannalta tarkoituksenmukaisia ja kustannustehokkaita. Sopimukset työntekijöiden, asiakkaiden ja kumppaneiden kanssa, yksityisyyden suoja ja muut lakisääteiset vaatimukset otetaan huomioon toiminnassa. Tietoturvakäytännöillä hallitaan uusien prosessien, teknologioiden ja tietojärjestelmien käyttöönottoon liittyviä riskejä.

Praecom rekisteröi tietoja prospekti- ja asiakasrekisteri rekisteriseloste mukaan ja käsittelee tietoja henkilötietojen käsittely sopimuksen mukaisesti.

Vastuut ja organisaatio

Yrityksen johto vastaa toiminnan jatkuvuussuunnitelmien laatimisesta, joita ylläpidetään säännöllisesti.

Tietohallinto vastaa operatiivisten vaatimusten mukaisten tietojärjestelmien toteuttamisesta ja tietoturvallisuudesta. Tietohallinto vastaa keskitettyjen tietoturvapalvelujen tarjoamisesta.

Tietoturvahenkilöstö varmistaa, että tunnistettujen tietoturvariskien edellyttämät toimenpiteet on toteutettu ajantasaisen tietoturvatason ylläpitämiseksi. Tietoturvahenkilöstö vastaa tietoturvan teknisestä valvonnasta. Tietoturvahenkilöstö huolehtii myös työntekijöiden tietoturvatietoisuudesta, jotta he tunnistavat mahdolliset turvallisuusuhat ja toimivat asianmukaisesti tällaisia uhkia kohdatessaan.

Kaikki työntekijät perehtyvät annettuihin ohjeisiin ja heitä vaaditaan toimimaan niiden mukaisesti. Työntekijän on ilmoitettava havaitsemistaan turvallisuusuhkista ja -riskeistä. Esihenkilöiden tehtävänä on seurata työntekijöidensä perehtyneisyyttä mainittuihin ohjeisiin ja puuttua tietoturvapolitiikkaa ja -ohjeita rikkoviin toimiin.

Tietoturvariskien arviointi

Tietoturvariskejä arvioidaan ja analysoidaan niiden liiketoimintavaikutusten perusteella. Arvioinnit on tehtävä uusien järjestelmien määrittelyvaiheessa ja sellaisten muutosten yhteydessä, joilla on merkittävä vaikutus toiminnan kriittisyyteen.

Keskitetty käyttöoikeuksien hallinta

Praecom tietojärjestelmien käyttöoikeudet ja käyttöoikeuksien hallinta on keskitetty tietohallinnolle. Järjestelmän omistajat hyväksyvät käyttöoikeuksien myöntämisen. Ulkoisten käyttäjien oikeuksia Tietohallinto valvoo keskitetysti.

Tietoverkon käyttäminen

Pääsy Praecomin tietoverkkoon ja palveluihin myönnetään vain Tietohallinnon valvomien tai hyväksymien järjestelmien ja ohjelmistojen kautta. Tiedonhallinta valvoo ja tarvittaessa rajoittaa käytettäviä ohjelmistoja tietoturvan varmistamiseksi. Ulkoisille kumppaneille on luotu erillinen turvallinen kytkentämenettely.

Tietoturvakoulutus

Praecom työntekijät osallistuvat säännöllisesti tietoturvallisuus koulutukseen.

Seuranta ja valvonta

Tietoturvan tason parantaminen ja ylläpitäminen edellyttää tietojärjestelmien systemaattista ja jatkuvaa valvontaa. Tarkastuksista vastaa tietoturvahenkilöstö ja heitä sitoo käsittelemiensä tietojen salassapitovelvollisuus. He allekirjoittavat salassapitosopimuksen riippumatta siitä, ovatko he Praecomin työntekijäitä tai ulkopuolisia kumppaneita.

Teknistä tietoturvaa arvioidaan jatkuvasti ja tietoturvan tilasta raportoidaan normaalissa sisäisessä valvonnassa. Kriittisiltä palveluilta vaaditaan ennen käyttöönottoa tehtävät tietoturvatarkastukset.

Tietoturvapoikkeamien käsittely

Tietoturvahenkilöstöllä on käytössä menettelytavat ja välineet tietoturvapoikkeamien havaitsemiseksi.

Yhteistyökumppanit

Kaikkien Praecomin yhteistyökumppaneiden on sitouduttava palvelusopimusten tietoturvaliitteissä sovittuihin tietoturvavaatimuksiin, joita valvotaan säännöllisesti.

Tietoturvaloukkaukset

Tietoturvaloukkauksiin kuuluvat kaikki toimet, jotka ovat ristiriidassa tietoturvakäytäntöjen ja -ohjeiden kanssa. Tietoturvaa valvotaan kaikkien hyväksyttyjen seurantaperiaatteiden mukaisesti. Seuranta on toteutettava myös lain ja sopimusten mukaisilla teknisillä ratkaisuilla.