Stansomatic Informationssikkerhedspolitik

Introduktion

Informationssikkerhed er en vigtig komponent i vores overordnede forretningsstrategi og er afgørende for at beskytte vores informationsaktiver, sikre forretningskontinuitet og opretholde tilliden hos vores kunder og forretningspartnere. Vi forpligter os til at overholde alle relevante bestemmelser vedrørende informationssikkerhed. Vi vil regelmæssigt gennemgå og opdatere vores informationssikkerhedspolitikker og -kontroller for at sikre overholdelse af disse retningslinjer og bestemmelser. Derudover vil vi overvåge ændringer i retningslinjer vedrørende informationssikkerhed og justere vores politikker og kontroller i overensstemmelse for at opretholde compliance.

Formålet med denne informationssikkerhedspolitik er at skitsere kravene til og ansvaret for at beskytte fortroligheden, integriteten og tilgængeligheden af oplysninger og informationssystemer i virksomheden. Politikken fastlægger også en ramme for implementering og gennemgang af kontroller.

Denne politik gælder for alle medarbejdere, samarbejdspartnere og tredjepartsleverandører, der har adgang til virksomhedens informationssystemer og data. Leverandører eller andre forretningspartnere, der overtræder informationssikkerhedspolitikker og -kontroller, kan modtage en advarsel eller i værste fald få kontrakten med Stansomatic suspenderet eller ophævet. Stansomatic kan anlægge sag mod medarbejdere, leverandører eller andre forretningspartnere, der overtræder informationssikkerhedspolitikker og -kontroller på en måde, der skader virksomheden, dens kunder eller dens partnere.

Det er alle medarbejdere, samarbejdspartnere og tredjepartsleverandørers ansvar at overholde denne politik for at sikre virksomhedens informationsaktiver.

Informationssikkerhedskontroller

Følgende informationssikkerhedskontroller er forpligtelser, der skal implementeres for at beskytte virksomhedens informationssystemer og data:

a) Adgangskontrol: Adgang til informationssystemer og data må kun gives til autoriseret personale efter behov. Adgangskontroller skal gennemgås regelmæssigt, og eventuelle ændringer skal dokumenteres og godkendes af ledelsen.

b) Fortrolighed: Fortroligheden af virksomhedsoplysninger skal altid opretholdes. Medarbejdere, samarbejdspartnere og tredjepartsleverandører skal underskrive en fortrolighedsaftale, før de får adgang til virksomhedsoplysninger.

c) Databeskyttelse: Virksomhedsdata skal beskyttes mod uautoriseret adgang, videregivelse, ændring eller destruktion. Datakryptering og backupprocedurer skal implementeres for at beskytte mod tab eller tyveri af data. Det er vores mål at sikre, at alle kritiske data krypteres, både ved overførsel og opbevaring.

d) Hændelsesstyring: Virksomheden skal have en hændelsesstyringsproces på plads til at opdage og reagere på hændelser samt genoprette sikkerheden. Alle sikkerhedshændelser skal straks rapporteres til den informationssikkerhedsansvarlige. Vi ønsker at reducere den gennemsnitlige tid, det tager at opdage og reagere på sikkerhedshændelser med 50 % i løbet af det næste år.

e) Fysisk sikkerhed: Fysisk adgang til informationssystemer og datalagringssteder skal kontrolleres, overvåges og beskyttes mod uautoriseret adgang.

f) Systemovervågning: Informationssystemer skal overvåges for at opdage forsøg på uautoriseret adgang, unormal systemadfærd og sikkerhedsbrud.

g) Uddannelse og forståelse: Alle medarbejdere, samarbejdspartnere og tredjepartsleverandører skal modtage uddannelse i og information om informationssikkerhed for at sikre, at de forstår deres ansvar og forpligtelser vedrørende emnet. Det er vores mål at øge procentdelen af medarbejdere, der gennemfører uddannelse i informationssikkerhed årligt til 100 %.

Risikovurdering

Risikovurderinger af informationssikkerheden er en nøglekomponent i vores politik for informationssikkerhedsstyring. Vi vil foretage regelmæssige risikovurderinger for at identificere potentielle trusler og sårbarheder i forhold til vores informationsaktiver og vurdere sandsynligheden for og den potentielle indvirkning af disse risici. Resultaterne af disse vurderinger vil danne grundlag for udviklingen og gennemførelsen af passende og reviderede informationssikkerhedskontroller og -foranstaltninger for at mindske identificerede risici.

Vi vil sikre, at vores risikovurderinger udføres på en systematisk og omfattende måde ved hjælp af anerkendte rammer og metoder. Vores risikovurderinger vil tage højde for en række faktorer, herunder hvor følsomme og kritiske vores informationsaktiver er, den potentielle indvirkning af et brud eller en kompromittering og sandsynligheden for og hyppigheden af potentielle trusler. Vi vil også sikre, at vores risikovurderinger udføres regelmæssigt med den hyppighed af vurderinger, der er bestemt af vores

informationsaktivers risikoniveau. Vores informationssikkerhedsansvarlige vil være ansvarlig for at koordinere og føre tilsyn med risikovurderinger, og resultaterne af disse vurderinger vil blive dokumenteret og kommunikeret til relevante interessenter efter behov.

Gennem vores risikovurderinger af informationssikkerheden vil vi proaktivt identificere og håndtere risici for vores informationsaktiver og sikre fortsat beskyttelse, fortrolighed og tilgængelighed af vores data og systemer.

Evalueringsproces

Informationssikkerhedspolitikken skal evalueres årligt for at sikre, at den forbliver relevant og effektiv. Evalueringsprocessen skal omfatte følgende trin:

a) Den informationssikkerhedsansvarliges evaluering af politikken for at sikre, at den er opdateret og i overensstemmelse med relevante standarder og bestemmelser.
b) Konsultation med vigtige interessenter, herunder IT og HR, for at identificere eventuelle nødvendige ændringer eller opdateringer.
c) Evaluering og opdatering af informationssikkerhedskontroller og -procedurer.
d) Godkendelse af den opdaterede politik af den øverste ledelse.

Dedikerede ansvarsområder

Følgende personer har et dedikeret ansvar for informationssikkerheden i virksomheden:

a) Informationssikkerhedsansvarlig: Den informationssikkerhedsansvarlige er ansvarlig for at føre tilsyn med implementering og styring af informationssikkerhedskontroller.
b) IT-afdeling: IT-afdelingen er ansvarlig for at implementere og vedligeholde informationssikkerhedskontroller for virksomhedens informationssystemer.
c) HR-afdeling: HR-afdelingen er ansvarlig for at sikre, at alle medarbejdere, samarbejdspartnere og tredjepartsleverandører modtager uddannelse i og information om informationssikkerhed.

Stansomatic d. 24-04-2023

_____

Søren Bahnsen
CEO