INFORMATIONSSIKKERHEDSPOLITIK FOR HERLUFSHOLM SKOLE OG GODS

Formål

Formål med denne sikkerhedspolitik er at definere rammerne for styring af informationssikkerhed på Herlufsholm Skole og Gods (HSOG).

Gyldighed

Sikkerhedspolitikken gælder for alle ansatte, al anvendelse og al adgang til de af HSOGs godkendte informationssystemer i henhold til HSOGs *Persondatahåndbog (PDH)* samt Persondataforordningen (GDPR) og gældende dansk lovgivning.

Målsætning

HSOG arbejder aktivt med styring af informationssikkerhed med det formål at sikre tilgængelighed, integritet og fortrolighed af HSOGs informationsaktiver, systemer og data.

HSOG anvender en risikobaseret tilgang. Særligt for behandling af personfølsomme data, som kræver ekstraordinært højt beskyttelsesniveauet, udarbejdes særlig risikoanalyse.

HSOG tilstræber at overholde de indgåede aftaler med eksterne parter, herunder databehandleraftaler.

Denne håndbog gennemgår løbende vedligeholdelse, og indeholder beskrivelser af implementerede tiltag ift. informationssikkerhed samt henvisninger til relevante politikker, retningslinjer og procedurer beskrevet i HSOGs *Persondatahåndbog*.

Organisation og ansvar:

Bestyrelsen har det ultimative ansvar for informationssikkerheden på HSOG.

HSOGs IT-styregruppe – bestående af direktionen (rektor, vicerektor og direktør), regnskabschef, IT-chef og HSOGs Compliance Officer (CO) - er ansvarlig for styringsprincipperne og delegerer specifikke ansvarsområder for beskyttelsesforanstaltninger, herunder anvendelse af informationssystemer.

Ejerskab fastsættes for hvert kritisk informationssystem. Ejeren fastlægger hvorledes sikringsforanstaltninger anvendes og administreres i overensstemmelse med sikkerhedspolitikken og i samarbejde med HSOGs Compliance Officer.

IT-afdelingen rådgiver, koordinerer, kontrollerer og rapporterer om status på IT-sikkerheden ud fra understøttende retningslinjer og procedurer som angivet i nærværende dokument.

Den enkelte medarbejder er ansvarlig for at overholde Informationssikkerhedspolitikken og er informeret herom i denne skrivelse, "Retningslinjer for medarbejdernes IT-anvendelse gældende for HSOG" (internt) samt i HSOGs "*Persondatahåndbog*".

Dispensationer

Dispensationer til HSOGs Informationssikkerhedspolitik og retningslinjer kan i sjældne tilfælde forekomme og skal godkendes af IT-afdelingen ud fra retningslinjer udstukket af IT-styregruppen.

Der kan forekomme enkelte situationer, hvor det er nødvendigt at dispensere for de fastlagte politikker. I sådanne tilfælde skal IT-styregruppen underrettes, og dispensationen skal gives skriftligt og tidsbegrænset.

Omfatter dispensationen behandling af følsomme personoplysninger, skal dette ledsages af en risikoanalyse, og tilladelse skal indhentes fra IT-styregruppen, før dispensationen gives.

Oversigt over tilladte dispensationer skal forefindes i "Persondatamappen for Herlufsholm Skole og Gods", og de enkelte dispensationer skal som minimum indeholde følgende oplysninger:

- Hvilke data er berørt af dispenseringen
- Hvem berør dispensationen
- Konsekvens af dispenseringen (risikovurdering)
- Hvor længe kan dispensation tillades

Rapportering

IT-afdelingen og medarbejdere på Herlufsholm skal informere IT-styregruppen ved mistanke om muligt sikkerhedsbrud uden unødig forsinkelse (ref. HSOGs *Persondatahåndbog)*.

HSOG fører en samlet oversigt over alle forekomne datasikkerhedsbrud, og IT-chefen fører status over dispensationer i en rapport, som forelægges IT-styregruppen ved hvert af de 4 årlige møder i IT-styregruppen. Rapporterne arkiveres i persondatamappen.

IT-styregruppen behandler årligt HSOGs sikkerhedsstatus og aflægger rapport til bestyrelsen.

Overtrædelse

Forsætlig overtrædelse og misbrug af reglerne i dette dokument rapporteres øjeblikkeligt af IT- chefen til IT-styregruppen uden unødig forsinkelse.

Overtrædelse af informationssikkerhedspolitikken eller understøttende retningslinjer kan få ansættelsesretlige konsekvenser.