POLICY FÖR IT- OCH INFORMATIONSSÄKERHET

Syfte och bakgrund

Amnesty Sverige hanterar information för att kunna bedriva vårt arbete med insamling, opinionsbildning och påverkan. Tillgång till information är en grundläggande del i detta arbete och är därmed att ses som en verksamhetskritisk del av verksamheten. Amnesty arbetar med ett modernt informationsstöd med hög tillgänglighet och flexibilitet, vilket är viktiga egenskaper för att på ett effektivt sätt kunna bedriva insamlingsverksamhet, samt att ge medarbetare, medlemmar och givare en god service och upplevelse.

Väl förvaltade informationstillgångar är en förutsättning för att erhålla en god utveckling för verksamheten, motsatsen kan bli till förfång för både förtroende och intäkter.

Egenskaper såsom en väl förankrad säkerhetsmedvetenhet inom hela organisationen är grunden för god informationssäkerhet. Alla medarbetare ska vara väl informerade om vilka riktlinjer och rutiner som gäller runt IT-säkerhet samt vikten av att förhålla sig därtill.

IT- och informationssäkerhetspolicyn framställer mål och inriktning för IT- och informationssäkerhetsarbetet och vänder sig till alla som på något sätt arbetar med Amnestys informationstillgångar, såsom anställda, externa resurser och ideellt arbetande personer.

Syftet med IT- och informationssäkerhetspolicyn är att fungera som ett övergripande styrdokument som anger ramar för säkerhetsarbetet, med målsättning att förebygga bristande funktionsduglighet inom organisationens IT-verksamhet, samt att rätt information ska vara tillgänglig för behörig vid ett specifikt tillfälle.

Att etablera en god nivå av systematiskt IT- och informationssäkerhetsarbete gör det möjligt att lagstadgade och interna krav kan efterlevas, att verksamhet av kritisk art har hög tillgänglighet, att brister i säkerheten minimeras, att kostnader för säkerhetsbrister begränsas, samt bidrar till att förtroendet för Amnestys varumärke och dess verksamhet upprätthålls.

Säkerhetsaspekter

IT- och Informationssäkerhetsarbetet ska bedrivas systematiskt och långsiktigt utifrån följande punkter;

- Riktighet
  Informationstillgångar ska inte kunna förändras och förvanskas av misstag eller av någon obehörig. De ska vara tillförlitliga, korrekta och fullständiga. Skyddet av IT- och informationstillgångar ska vara utformat så att verksamhetens krav på säkerhetsaspekter uppfylls.

- Sekretess
  Informationstillgångar ska följa lagstiftade krav, samt ska följa interna etiska regler, delges endast den eller de personer som har behörighet att ta del därav.

- Spårbarhet
  Betydande händelser i informationsbehandlingen i väsentliga informationssystem ska kunna spåras. Det ska vara möjligt att härleda specifika aktiviteter eller händelser till ett identifierat objekt, till exempel dokument, användare, komponent, fysisk plats eller IT-system. Det ska gå att se vilka förändringar som har utförts och av vem dessa har utförts.

- Tillgänglighet
  IT-systemen ska vara tillgängliga för behöriga användare i beslutad omfattning på bestämda tider.

Ansvar

Amnesty Sveriges IT- och informationssäkerhetspolicy beslutas av Amnesty Sveriges styrelse. IT-gruppen ansvara för implementeringen av policyn. Policyn omfattar hela Amnesty Sveriges verksamhet och all information utan undantag oavsett om den hanteras på internet, i datorer, mobila enheter eller i dokumentform.

Det innebär;

Amnesty Sverige, föreskrifter och arbetssätt

- Amnesty Sverige följer god sed inom IT- och informationssäkerhet och lagstadgade krav, såsom integritetsskydds lagstiftning GDPR, säkerhetsstandarden för kortbetalningar (PCI DSS) "Payment Card Industry Data Security Standard".
- Amnesty Sverige klassificerar, värderar och prioriterar dess IT- och informationstillgångar genom förvaltningsorganisation utifrån verksamhetens krav på riktighet, sekretess, spårbarhet och tillgänglighet.
- Amnesty Sverige har beredskap för att kritiska verksamheter ska upprätthållas på överenskommen nivå vid olika typer av störningar, avbrott eller krissituationer.
- Amnesty Sverige ställer säkerhetskrav i upphandlingar och vid utveckling, användning och avveckling av IT-system.
- Amnesty Sverige ska uppmärksamma och rapportera händelser som kan misstänkas påverka informationssäkerheten.
- Amnesty Sverige säkerställer att interna och externa revisorer kontinuerligt genomför uppföljningar av efterlevnaden av reglerande krav.

Amnesty Sverige, medarbetare

- Amnesty Sveriges alla medarbetare och externa resurser, det vill säga alla anställda, externa resurser och ideellt arbetande personer ska känna till vad det egna ansvaret omfattar och ha god kunskap om vilka säkerhetsregler som gäller. Det gäller både för fast- och tillfälligt anställda, samt externt anlitad personal.
- Medarbetare som berörs ska regelbundet få och förväntas deltaga i den utbildning som krävs för att IT- och informationssäkerheten ska kunna upprätthållas.

IT- och informationsägare

- Alla IT-system har en utsedd systemägare (som inom ramen för Amnesty Sveriges förvaltningsmodell ansvarar för att säkerhetskraven på IT-systemet uppfylls).
- Systemägaren ansvarar för att klassificera informationen och ställa de säkerhetskrav som krävs för informationshantering.
- IT- och informationsägare ska genom återkommande risk- och sårbarhetsanalyser och inträffade incidenter vidta nödvändiga åtgärder för att säkerställa att Amnesty Sveriges informationstillgångar har ett ändamålsenligt skydd.

Årlig omprövning

- IT- och informationssäkerhetspolicyn omprövas årligen av IT-gruppen. Vid omfattande förändring föreslås revideringar som antas av styrelsen.