HUDEVAD
RADIATOR DESIGN

Informations-sikkerhedspolitik

Indhold

1. Indledning

Vi er forpligtet til at håndtere information sikkert. Det er et ansvar, vi tager alvorligt, når vi bliver betroet vores interessenters persondata, og vi er optaget af at beskytte alle data med det absolut højeste sikkerhedsniveau.

Derudover er informationssikkerheden afgørende for både vores selskabs bæredygtighed og konkurrenceevne. Det er samtidig en central del af vores ansvar over for kunder, kolleger, leverandører, samarbejdspartnere og investorer.

2. Formål

Formålet med denne politik er at angive en ramme for beskyttelse af fortrolighed, integritet og tilgængelighed af de informationsaktiver, der ejes eller behandles af Stelrad Group plc og dets datterselskaber ("koncernen").

3. Anvendelsesområde

Informationssikkerhedspolitikken og dens understøttende kontroller, processer og procedurer gælder for al information, som koncernen anvender, uanset format. Det omfatter også information, der behandles af andre organisationer i forbindelse med deres samarbejde med koncernen.

Informationssikkerhedspolitikken og dens understøttende kontroller, processer og procedurer gælder for alle personer, som har adgang til koncernens information, informationssystemer eller -tjenester. Det inkluderer alle medarbejdere, leverandører, entreprenører og samarbejdspartnere, der har adgang til koncernens information, samt eksterne parter, der leverer informationsbehandlingstjenester til koncernen.

4. Principper og mål

Det er koncernens politik at sikre, at information beskyttes mod tab af:

- Fortrolighed – Information er kun tilgængelig for bemyndigede personer, og vi udviser den højeste grad af omhu for at beskytte den.
- Integritet – Vores robuste systemer og processer sikrer, at informationens nøjagtighed og fuldstændighed opretholdes.
- Tilgængelighed – Information vil være tilgængelig for autoriserede brugere og processer, når det er nødvendigt.

Derfor er koncernens sikkerhedsmål følgende:

- Vores informationsrisici identificeres, håndteres og behandles i overensstemmelse med en aftalt risikotolerance.
- Vores autoriserede brugere kan sikkert tilgå og dele information for at udføre deres opgaver.
- Vores fysiske, proceduremæssige og tekniske kontroller afbalancerer brugeroplevelse og sikkerhed.
- Vores kontraktuelle og juridiske forpligtelser vedrørende informationssikkerhed overholdes.

- Informationssikkerhed indtænkes i alle koncernens aktiviteter og forretningsområder.
- Personer med adgang til vores information er bevidste om deres ansvar for informationssikkerhed.

5. Ledelse og ansvar for informationssikkerhed

Ansvaret for informationssikkerhed ligger hos koncernens økonomidirektør (Chief Financial Officer), som rapporterer direkte til koncernens bestyrelse.

Derfor er koncernens sikkerhedsmål følgende:
Derudover modtager bestyrelsen og det øverste ledelseslag detaljerede orienteringer om vores risikostyring og afbødningsaktiviteter fra koncernens revisions- og risikoudvalg.

En styregruppe for informationssikkerhed påvirker, overvåger og fremmer en effektiv håndtering af koncernens information og formidler udviklinger inden for informationsrisici til økonomidirektøren.

6. Informationssikkerhedspolitikker og risikostyring

For at leve op til vores forpligtelse og dokumentere vores indsats har vi udviklet politikker, der fastsætter vores ambitioner, samt implementeret kontroller til at forebygge, opdage og begrænse risici. Vi har vedtaget en risikobaseret tilgang, hvor vi prioriterer indsatsen på de områder, der udgør den største risiko for selskabet.

Vi har desuden etableret rapporteringsprocesser og en styregruppe for informationssikkerhed for at sikre synlighed på ledelsesniveau og på tværs af koncernen. Risikoregistre og oversigter over informationsaktiver gennemgås regelmæssigt af styregruppen for informationssikkerhed. Vi opfordrer løbende til kritisk vurdering qua uafhængige informationssikkerhedsgennemgange og revisioner.

7. Systemsikkerhed

For at sikre, at vores teknologiske systemer er beskyttet mod nye sikkerhedssårbarheder, tester og installerer vi regelmæssigt opdateringer og sikkerhedsrettelser.

Derudover styrker vi løbende vores netværk for at beskytte os mod uautoriseret trafik og skadeligt indhold. Samtidig har vi implementeret værktøjer til at beskytte os mod malware-infektioner.
Vi gennemfører årlige uafhængige angrebstests for proaktivt at identificere sårbarheder.
Systemer og programmer, der udvikles, er genstand for en grundig sikkerhedskontrol for fejl og svagheder i hele udviklingsprocessen, før de tages i brug. Vores informationssikkerhedsinfrastruktur er desuden underlagt omfattende overvågning.

Vi har en fast procedure for identifikation og eskalering af sikkerhedshændelser. Faktiske eller formodede brud på informationssikkerheden registreres og undersøges. De nødvendige tiltag for at afhjælpe bruddet iværksættes, og eventuelle læringspunkter indarbejdes i vores sikkerhedsprotokoller.

8. Medarbejderbevidsthed og uddannelse

Vi sikrer, at vores medarbejdere modtager uddannelse i sikkerhedsbevidsthed, så de forstår vigtigheden af fortrolighed, integritet og tilgængelighed – samt deres ansvar for at opretholde disse principper. Løbende uddannelse gennemføres for yderligere at beskytte vores kunde-, medarbejder- og selskabsdata.

Uddannelse i informationssikkerhed er obligatorisk for alle medarbejdere. Vi afholder regelmæssige opfølgningskurser for at sikre, at viden og bevidsthed altid er opdateret hos alle.

9. Leverandørrelationer og gennemgange

Vi forventer, at vores leverandører udviser samme høje grad af omhu som os, når det gælder beskyttelse af den information, vi deler med dem. Koncernens krav til informationssikkerhed indgår som en central faktor ved etablering af leverandørrelationer for at sikre, at de aktiver, leverandører har adgang til, er beskyttet.

Leverandøraktiviteter overvåges og gennemgås i forhold til værdien af de pågældende aktiver samt de tilknyttede risici.

10. Forretningskontinuitet

For at sikre en stabil og uafbrudt drift af vores virksomhed gennemfører vi regelmæssige forretnings¬påvirknings¬analyser af vores funktioner for at identificere kapaciteter, behov og kritiske elementer for vores forretning. På baggrund af dette implementerer vi beredskabs-planer, kontroller og afbødnings¬tiltag for at beskytte disse vigtige processer.

Vores beredskabs¬planer vedligeholdes, gennemgås og testes løbende.

Vi har desuden etableret passende backuprutiner og indbygget robusthed i vores it-systemer, som vi regelmæssigt tester for at sikre deres pålidelighed.

11. Håndtering af cyberrisici

Hver af koncernens forretningsenheder skal implementere følgende procedurer for at håndtere cyberrisici:

- Gennemføre regelmæssige sårbarhedsvurderinger og angrebstests.
- Implementere et uddannelsesprogram i sikkerhedsbevidsthed for alle medarbejdere.
- Anvende stærke adgangskoder og flerfaktorgodkendelse.
- Implementere en plan for data¬sikkerhedskopiering og gendannelse.
- Have en beredskabsplan for håndtering af cyberhændelser.

Ved en cyberhændelse vil koncernen iværksætte følgende tiltag:

- Omgående undersøge hændelsen.
- Inddæmme hændelsen og forhindre yderligere skade i samarbejde med SOC (Security Operations Center) [red.: Sikkerhedscenter]

- Gendanne eventuelt tabte eller beskadigede data.
- Anmelde hændelsen til relevante myndigheder.
- Kommunikere med berørte parter.

Koncernen overholder alle gældende love og regler vedrørende cybersikkerhed.

12. Overholdelse

Design, drift, anvendelse og administration af vores informationssystemer overholder alle regulatoriske og kontraktuelle sikkerhedskrav, herunder:

- Lovgivning om databeskyttelse – Hvis persondata overføres, skal det ske i overensstemmelse med kravene i databeskyttelsesforordningen (GDPR), hvor det er relevant.
- Payment Card Industry Standard (PCI-DSS) – Hvis en tredjepart behandler kortbetalinger, skal det ske i overensstemmelse med Payment Card Industry Data Security Standard (PCI DSS), hvor det er relevant.
- Koncernens kontraktuelle forpligtelser.

Vi anvender en kombination af interne og eksterne gennemgange for at dokumentere overholdelsen af udvalgte standarder og best practices, herunder vores interne politikker og protokoller. Det omfatter it-sundhedstjek, gap-analyser i forhold til dokumenterede standarder samt interne kontroller af medarbejderes overholdelse af sikkerhedskrav.

Vi opfordrer alle, der har mistanke om overtrædelser af denne politik, til at sige fra ved at kontakte deres nærmeste leder, personalechef (hr) eller ved at rapportere deres bekymringer via koncernens whistleblowerpolitik. Kontaktoplysningerne er: compliance@srgl.com eller +44 191 261 3306.

Politikgennemgang

Denne politik vil blive gennemgået af koncernens økonomiafdeling og godkendt af bestyrelsen.
.

Dokumentansvar:	Koncernøkonomi
Ikrafttrædelse:	Oktober 2023
Frekvens:	Hvert andet år
Næste gennemgang:	Oktober 2025

Versionskontrol

Dato	Version	Årsag til ændring	Forfatter
Oktober 2023	1.0	Første udgivelse	Koncern-økonomi