| | |
|---|---|
| Ämne:<br>Säkerhetspolicy | Datum:<br>2019-12-02 |
| Ansvarig:<br>Säkerhetsskyddschef | Revision:<br>1.0 |
| Godkänd av:<br>Styrelsen | Säkerhet<br>Publik |

## Definition och utgångspunkter

Policyn beskriver den strategiska betydelsen för Nacka Energi AB och Nacka Energi Försäljning AB säkerhet och ska styra aktiviteterna i organisationen. Samhället idag är beroende av ett fungerande informationssystem och störningar i drift får stora inverkan. Säkerhetsskydd delas enligt lagen upp i de tre områdena informationssäkerhet, fysisk säkerhet och personalsäkerhet.

**Informationssäkerhet** har en central roll när det handlar om att hantera den information som bolaget upprättar, tar emot eller förvarar. Som ett kommunägt bolag har vi även skyldighet att bevara och tillgängliggöra allmänna handlingar samtidigt som vi ska skydda dem. Bolaget ska behandla uppgifter i enlighet med lagar och föreskrifter som skyddar personlig integritet.

**Fysisk säkerhet**, ska säkerställas genom att bolaget ska vidta säkerhetsskyddsåtgärder för att upptäcka, försvåra, hantera och minimera obehörigt tillträde eller skadlig inverkan. Bolaget ska på olika sätt kontrollera att alla personer som ska få tillträde till en plats där säkerhetskänslig verksamhet bedrivs, har behörighet till det.

**Personalsäkerhet** sker i samband med anställning eller annat deltagande i säkerhetskänslig del av verksamheten genom säkerhetsprövning. Bolaget ska med utgångspunkt i säkerhetsskyddsanalysen föra förteckning över vilka anställningar eller annat deltagande i den säkerhetskänsliga verksamheten som placerats i säkerhetsklass eller som ska föregås av registerkontroll.

Bolaget ska hantera säkerhetsaspekterna så att vi uppnår krav på:

- Tillgänglighet - att informationen ska kunna nyttjas efter behov, i förväntad utsträckning samt av rätt person med rätt behörighet.
- Riktighet - att informationen är tillförlitlig, korrekt och fullständig.
- Konfidentialitet - att begränsa åtkomsten för informationen där det behövs.
- Spårbarhet - att specifik informationen ska kunna spåras, viktigt i verksamheten då personuppgifter ingår i informationshanteringen.

Samtliga informationstillgångar ska vara identifierade och förtecknade. Av förteckningen ska framgå vem som är informationsägare eller systemägare. Alla verksamheter och system är utsatta för risker, så informationsklassningar, säkerhetsklassningar och riskanalyser ska finnas.

Alla som hanterar informationstillgångar i bolaget har ett ansvar att säkerheten upprätthålls. Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten. Policyn ska vara förankrad hos både interna och externa aktörer som verkar i och med bolaget. För detta ska riktlinjer och instruktioner finnas tillgängliga.

### Mål

Bolaget, som utpekad leverantör av samhällsviktiga tjänster enligt Nis-direktivet ska uppfylla krav i lagar, förordningar och föreskrifter. Bolaget ska hålla överenskommelser i avtal samt ge medarbetare en rimlig arbetsmiljö avseende tillgång till information. Skador genom påverkan på leveranser, tjänster och funktioner som är nödvändiga för samhället på nationell nivå ur ett säkerhetsskyddsperspektiv ska vara identifierade och hanteras enligt föreskrifter.
Bolaget ska bedriva ett systematiskt och riskbaserat säkerhetsarbete avseende nätverk och

informationssystem. Lämpliga åtgärder ska förebygga och minimera incidenter som påverkar nätverk och informationssystem. Åtgärderna ska syfta till att säkerställa kontinuiteten i tjänsterna.

## Arbetet med säkerhet

Riskanalyser och klassningar för information och säkerhetsskydd ska ligga till grund för val av säkerhetsåtgärder och åtgärdsplaner. Analyser och klassningar ska dokumenteras och uppdateras årligen. Utifrån policyn ska bolaget säkerställa riktlinjer och instruktioner samt säkra IT-system för kontinuerligt säkerhetsarbete. Det är av vikt att tydligt påvisa hur godkännande och granskning av IT-system som är knutna till säkerhetskänslig verksamhet sker på bolaget. Dessa dokument ska uppdateras och behandlas ur olika ansvarsnivåer i organisationen, som också ska vara väl förankrade. Utbildning av personal ska ske regelbundet och fokus kring riktlinjer och instruktioner ska ha en central roll vid introduktion av nyanställda. Incidenthantering ska vara välförankrade och tydliga processer. Handlingsplan för kortsiktiga mål och prioriteringar med grund i säkerhetspolicyns mål ska framställas och arbetas utifrån på avdelningsnivå.

## Roller och ansvar

- **Koncernen (kommunen)** är ägare av bolaget.
- **Styrelsen** beslutar om policyn och står bakom dess viljeriktning.
- **VD** har det övergripande ansvaret för bolagets informationssäkerhet och dess riktlinjer.
- **Säkerhetskyddschefen** är en viktig kravställare på medarbetare när det gäller. informationssäkerhet och dess riktlinjer och styrning.

## Hantering av incidenter

Personuppgiftsincidenter ska utifrån dataskyddsförordningen (GDPR) och i samråd med bolagets dataskyddsombud anmälas till datainspektionen med hjälp av deras riktlinjer. Detta ska normalt ske inom 72 timmar från upptäckt.

Bolaget ska utan onödigt dröjsmål rapportera incidenter till organisationer som bedriver tillsyn för samhällsskydd och beredskap. Styrande är i de fall incidenten har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänst som vi tillhandahåller enligt Nis-direktivet.

Då bolaget bedriver säkerhetskänslig verksamhet så finns även skyldighet att anmäla incidenten enligt säkerhetsskyddslagstiftningen.