

Nordstadens informationssäkerhetspolicy

Övergripande målbild och viljeriktning:

Konsekvensen av bristande informationssäkerhet kan medföra stora problem för enskilda personer och föreningar om information skulle gå förlorad, förvanskas, utnyttjas eller stjälas. Det kan även medföra ekonomiska förluster och att förtroendet för Nordstaden AB påverkas negativt.

Informationssäkerhet omfattar hela Nordstadens verksamhet i allmänhet och all information där personuppgifter är en del av i synnerhet, oavsett om informationen hanteras på datorer, i telefonsamtal eller på papper.

Med informationssäkerhet säkerställs följande

- **Riktighet** – Att information inte kan förändras av obehöriga, av misstag eller på grund av störningar i funktion/system. Informationen ska vara tillförlitlig, korrekt och fullständig.
- **Sekretess** – Att information i dokument, system och handlingar etc. med lagkrav om sekretess eller motsvarande inte görs tillgängliga eller avslöjas för obehörig.
- **Spårbarhet** – Att i efterhand kunna härleda specifika aktiviteter eller händelser till ett identifierat objekt ex. handling, användare, dator, skrivare eller system/program.
- **Tillgänglighet** – Att information är tillgänglig i skäligen och förväntad utsträckning och inom rimlig tid.

Den fysiska säkerheten är utformad för att förebygga obehörig åtkomst till servers. Vi har implementerade elektroniska säkerhetsåtgärder, såsom brandväggar, tillträdesbegränsningar i form av upprättade behörighetsnivåer som motsvarar behoven för respektive anställd på Nordstaden för att kunna utföra vårt arbete. Vi har även erforderlig kryptering som ger skydd mot dataintrång och annan obehörig åtkomst. NS reglerar via sekretessavtal åtkomst till personuppgifter för de personer i vår organisation, eller hos våra ombud, som har ett specifikt affärssyfte att bevara och behandla personuppgifter.

Rutin för incidenthantering:

Enligt datainspektionen så är den riktiga benämningen "*Personuppgiftsincidenter*" och det är detta som denna hantering avser.

Varje medarbetare på Nordstaden samt underentreprenörer kontrakterade av Nordstaden ansvarar för att all information som denne hanterar skall förvaras och hanteras på ett sådant sätt att ingen obehörig får tillgång till informationen, detta avser information såväl digitalt som i pappersform.

Om något skulle inträffa som innebär att information har gått förlorad så skall detta omedelbart rapporteras till ledningen på Nordstaden.

Nordstadens ledning säkerställer sedan att incidenten rapporteras till **Datainspektionen** inom 72 timmar efter överträdelsen upptäckts.