Systemförvaltning - kamerabevakning

Lägga till och ta bort användare, åtkomstbegränsningar

Systemägare ska lägga beställning till leverantör/entreprenör och likadant för oss som leverantör/entreprenör.

I beställning ska det tydligt framgå vilka rättigheter användaren ska ha (objektsindelning, granskning, uthämtning av material, livevy etc.).

Avbeställning av behörighet ska göras av närmaste chef till säkerhetssamordnare på teknik- och fastighetsförvaltningen, som därefter begär att borttagandet utförs av leverantör/entreprenör.

Ändringar i system och systemdokumentation

Change Acceptance Boards (CAB), styrelse för beslut om förändring, beslutar om förfrågningar innan de slutförs. Dessa möten leds av säkerhetssamordnare på teknik- och fastighetsförvaltningen och genomförs varje kvartal. I gruppen ingår utsedd person från Digital utveckling, objekt- och systemförvaltare, leverantör/entreprenör. Alla bör ha teknisk kompetens.

Teknisk riskanalys måste göras innan beslut fattas och implementering genomförs. Detta för att säkerställa att vi uppfyller kraven enligt GDPR och dataskyddsriktlinjer.

Rutin larmcentral algoritmer vid automatisk detektering samt beslut om att titta på kameror

Vid rörelse/aktivitet under tidsintervall klockan 19 – 06 aktiveras ett larmschema. För att larmet ska lösas ut krävs klassificering ”person som uppehåller sig i ett angivet område under en viss tid (20 – 60 sek)”. Larm visas per automatik på larmcentralen och där görs bedömningen av åtgärd (påkalla väktare eller polis).

Granskningsprocess för att se bilder är taget av videoanalysen var på bedömning görs av larmoperatör.

Alla loggar skall sparas i minst 12 månader. Efter fem dagar så är videomaterialet automatiskt raderat men logghändelserna finns kvar.

Larmcentralen kan också spela upp ett meddelande att personen befinner sig på ett bevakat område, där man ber personen att lämna området och att väktare är tillkallad.

Vi utlöst brandlarm/inbrottslarm kan larmcentralen ta beslut om att verifiera med hjälp av kamerorna om de finns en synlig brandhärd eller liknande. När beslut om att titta i kamerorna görs, så skall detta loggas i larmsystemet.

Larmcentralen ska alltid verifiera och skriva in orsak till granskning.

Destruktion

Vid avvecklande av server ska lagringsmedia förstöras. Detta görs av två personer som båda kvitterar att detta har utförts samt bevittnats.
Exempel: Anställda på Botkyrka tar server och åker till en anläggning som har som specialitet att destruera ovan, tillser att lagringsmedia är förstört och kvitterar därefter detta.

Årlig revision av kameror, servrar etc.

Enligt avtal mellan Botkyrka Kommun och leverantör/entreprenör ska följas.

- Årligt underhåll CCTV SSF1060 aktuell utgåva.
- Kontroll av bildlagring på lagrat material.
- Kontroll av filexport, att den fungerar.
- Kamerornas bildkvalitet och inställning enligt leverantörens krav samt tillståndsmyndighet.

Provbilder ska tas utifrån storleken på anläggning. Är anläggningen stor tas prover från cirka 25 % av totalt antal kameror. Om de finns kameror på platser där det är dåligt ljus ska dessa alltid prioriteras först och bilderna ska tas under sämsta förhållandet.

Videoanalysen måste kontrolleras att den fungerar enligt överenskommelse.

Årlig riskanalys

Systemägare och informationsansvarig ska varje år göra en riskanalys av verksamheten och utgå från projekteringsunderlag. Varje kameraplacering ska ifrågasättas; uppfylls det som angivits i tillståndet? Kvarstår behovet av kameran, eller ska den flyttas eller demonteras?

Systemägaren ska också genomföra riskanalys på systemet.