Behovsbeskrivning digitalisering inför nyproduktion vård och omsorgsboende mall

Generell beskrivning

Avser de digitala tekniska lösningar som exempelvis; yttre och inre skalskydd, passersystem, brandlarm, digital läkemedelshantering, trygghetslarm, trygghetskamera, dörröppnare, digitala lås, porttelefon, utgångskontroll, GPS-larm, belysningsstyrning, rörelselarm och digitala aktiviteter som lätthanterliga fjärrkontroller till TV/medialösningar. Tekniken ska installeras så att den bidrar till ökad livskvalitet och ger mer tid för umgänge. Inriktningen för den digitala tekniken är att den ska underlätta självständighet, aktivitet, och delaktighet hos hyresgästen samt effektivare arbetssätt som bidrar till bättre arbetsmiljön för medarbetare.

Vård- och omsorgsboendet ska vara nyckelfritt och bygger på att hyresgästen har ett armband som fungerar som ”nyckel” till boendet, den enskilda lägenheten, läkemedels- och värdeskåp samt integreras med det trygghetslarm som Göteborgs Stad upphandlat via ramavtal. Målet med varje fastighet där det bedrivs vård- och omsorgsboende är att de ska vara robust rustade för att klara av eventuella avbrott gällande fiber och el. Tanken är att varje fastighet ska ha en redundant fiber med diversitet och backupsystem. Arbete pågår med att ta fram lösningar för att hantera elavbrott.

Medarbetaren har tillgång till tagg/passerkort för passage samt nyckelskåp utifrån olika behörighetsgrupper som följer funktion. Utöver detta har medarbetarna en handenhet (mobil) som möjliggör en överblick av all information via aviseringar/notiser på aktuella app:ar genom en överblick/yta (Surface) för att kunna genomföra sitt uppdrag. Genom att ha aktuell information tillgänglig skapas möjligheter för medarbetarna att arbeta mer mobilt.

Samtliga system ska kunna samspela med varandra för att möjliggöra att medarbetarna får tillgång till aktuell och relevant information för att kunna genomföra sitt arbete mobilt. Med det avses att systemen ”pratar” med varandra eller att samlad information via aviseringar/notiser synliggörs i realtid genom app:ar på handenheten via gemensam överblick/yta (Surface). För samtliga system krävs det

att ansvarig inom verksamheten ska kunna ta ut loggar för att följa behörighet och tidpunkt för användande av specifik tjänst.

Övergripande krav som gäller genomgående

Ledningssystem för informationssäkerhet

Leverantören ska vara certifierad enligt ISO/IEC 27001 eller likvärdig certifiering som är motsvarande i ett informationssäkerhetsperspektiv. Certifikat ska lämnas in på begäran.

1. Om Leverantören inte är certifierad enligt ovan ska Leverantören på begäran redovisa rutiner för ett systematiskt informationssäkerhetsarbete, för de delar av verksamheten som berörs i leveransen, genom att beskriva hur nedan punkter kommer hanteras:
2. Organisationen har ett ledningssystem som uppfyller kraven i den standard som ska tillämpas.
3. Systemet är en naturlig del av organisationens dagliga verksamhet.
4. Systemet är beskrivet och tillgängligt.
5. System och beskrivning underhålls löpande.
6. Leverantören ska ha dokumenterade rutiner för övervakning, detektering, analys, rapportering, eskalering och hantering av säkerhetshändelser och säkerhetsincidenter. Leverantören ska ha rutiner för att hantera säkerhetsincidenter enligt gällande lagar och förordningar.
7. Det ska finnas en dokumenterad och formell process för hur användaridentiteter utfärdas och hanteras. De digitala identiteterna ska vara personliga och unika över tid.
8. Interna Informationssäkerhetsincidenter och IT säkerhetsincidenter hos leverantören ska rapporteras enligt en definierad incidentprocess för tjänsten,
9. Leverantören ska vidta nödvändiga tekniska och administrativ säkerhets- och skyddsåtgärder för att

förhindra it-säkerhetsincidenter som kan påverka Göteborgs Stad direkt eller indirekt.

10. Leverantören ska ha förmåga att identifiera och hantera IT-säkerhetsincidenter i sin egen IT-miljö som direkt eller indirekt kan påverka Göteborgs Stad.
11. Leverantören ska ha riktlinjer för informationssäkerhet inom sina systemutvecklingsprocesser. Vid större ändringar ska leverantören identifiera och hantera risker som säkerställer att säkerhetskraven i systemet är uppfyllda.

Tredjelandsöverföring – text från INK

All eventuell extern lagring, överföring eller bearbetning av personuppgifter, oberoende typ av data, som krävs för tjänstens utförande ska ske inom EU/EES eller i land som EU-kommissionen har beslutat har en adekvat skyddsnivå i enlighet med artikel 44-46 dataskyddsförordningen.

Observera att kravet också omfattar eventuella företag vars kapacitet Leverantören åberopar och eventuella Underleverantörer. Även om extern lagring, överföring eller bearbetning av personuppgifter, oberoende typ av data, som krävs för tjänstens utförande sker inom EU/ESS kan det förekomma en förhöjd risk för överföring av personuppgifter till tredjeland i de fall det finns någon annan än Leverantören som kan påverka tillgången till personuppgifterna, till exempel ett moderbolag inom en koncern eller liknande. Även vid en sådan situation måste kontroll genomföras för att säkerställa att det vidtagits tillräckliga åtgärder för kravuppfyllnad/efterlevnad enligt ovan.

Leverantören ska till sitt anbud bifoga dokumentation så att kontroll och verifiering av kravuppfyllnad/efterlevnad vad gäller hantering av personuppgifter kan genomföras. Inköp och upphandling har för det fall det bedöms nödvändig möjlighet att begära in ytterligare dokumentation för att kunna genomföra kontroll

Utifrån respektive system om köps in till ett VoB behöver hänsyn tas till informationssäkerhetskrav utifrån respektive lösnings informationsklassning och konsekvensbedömning.

Krav enlig nedan rubriker kommer att ställas på respektive system.

Informationssäkerhet

Systematiskt informationssäkerhetsarbete
- Informationssäkerhetspolicy
- Organisation av informationssäkerhetsarbetet
- Personalsäkerhet

Hantering av tillgångar
- Policy
- Användning
- Gallring
- Hantering
-

Styrning av åtkomst – autentisering i Webbapplikation

Kryptering

Fysisk och miljörelaterad säkerhet

Driftsäkerhet
- Säkerhetskopiering och återställning
- Hantering av tekniska sårbarheter
- Loggning och spårbarhet

Kommunikationssäkerhet

Anskaffning, utveckling och underhåll

Leverantörsrelationer

Hantering av informationssäkerhetsincidenter

Informationssäkerhetsaspekter avseende hantering av verksamhetens kontinuitet

Efterlevnad

Dataskydd
Leverantören ska iaktta följsamhet gentemot Dataskyddsförordningen på det sätt som exempelvis beskrivs i ISO 27701:2019. Kapitel 8 samt bilaga B.

Icke funktionella It-krav:

- Webbläsare
- Användbarhet

- Integration
- Kontorsprogram
- Dokumentation
- Skalbarhet
- Responstid

Autentisering

Drift & Support

- Felanmälan
- Tillgänglighet
- Tillåtna avbrott
- Redundans
- Uppdateringar
- Uppföljning
- Tillägg och ändringar

Utbildning

Tröskelanalys/Konsekvensbeskrivning

En konsekvensbedömning är en process för att beskriva behandlingen, bedöma om den är nödvändig och proportionell och hjälpa till att hantera risker. Dataskyddskontakterna och generell IT-säkerhet tillhandahåller i nuläget stöd för genomförande av de olika analyserna i projekt och förvaltning.

- Tröskelanalys genomförs av Intraservice i egenskap av PUA för att avgöra om en konsekvensbedömning behöver genomföras.
- Konsekvensbedömning – (Data Protection Impact Assessment, DPIA) är den mest kompletta analysen och används att skapa och påvisa efterlevnad.

Digitala tekniska/system lösningar -

- Passersystem
- Digital läkemedelshantering
- Värdeskåp
- Trygghetslarm –Trygghetskamera- GPS-larm- Digitala lås
- Porttelefon

- Informationsskärmar
- Nyckelskåp
- ...

Funktionsbeskrivning för respektive system ska finnas med som bilagor. För trygghetslam hänvisa till Ramavtal för Trygghetslarm VoB och Bmss.