European Union Agency
for Cybersecurity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

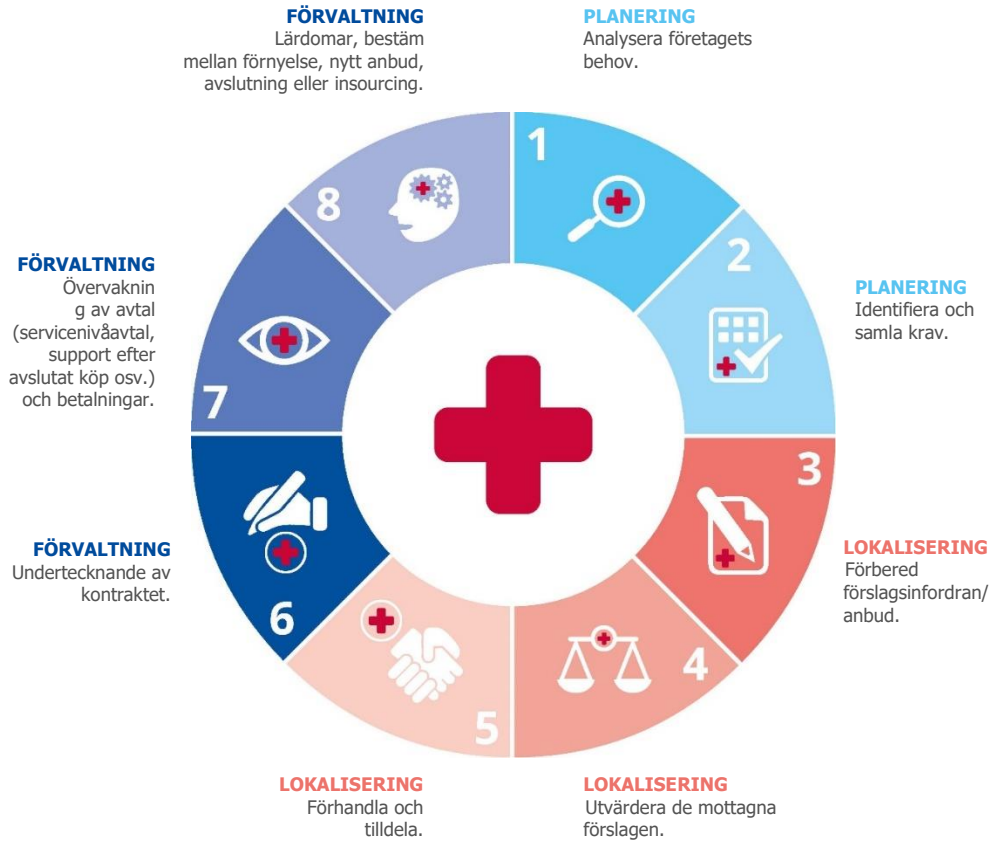
UPPHANDLINGSRIKTLINJER FÖR CYBERSÄKERHET PÅ SJUKHUS

Rapporten syftar till att vara en ”vägledning” för hälso- och sjukvårdspersonal. Många av metoderna och rekommendationerna kommer också att vara användbara för andra hälso- och sjukvårdsorganisationer, eftersom upphandlingsprocesserna kan vara mycket lika. Den är användbar för hälso- och sjukvårdspersonal med tekniska tjänster på sjukhus, dvs. chefer: säkerhetsansvariga, säkerhetsansvariga för de centrala datasystemen, teknikansvariga, IT-team samt upphandlingstjänstemän inom hälso- och sjukvårdsorganisationer. Detta korta dokument tar upp de viktigaste punkterna i rapporten – mer detaljerad information kan läsaren hitta i ENISA-publikationen: ENISA Goda rutiner för säkerhet för hälso- och sjukvårdstjänster som publicerades i februari 2020.

UPPHANDLINGSPROCESS

Eftersom sjukhusets ekosystem består av flera IT-komponenter bör cybersäkerheten granskas separat i alla dessa olika komponenter. Cybersäkerhet bör ingå i alla olika skeden i upphandlingsprocessen. I detta avsnitt presenterar vi de gemensamma stadierna i upphandlingsprocessen för att erhålla produkter och tjänster inklusive medicintekniska produkter, informationssystem och infrastrukturer.

Figur 1: Upphandlingsprocessens livscykel för sjukhus



- Planeringsfasen: Inledningsvis analyserar sjukhuset sina behov och samlar in krav från flera avdelningar internt. Till exempel, när det gäller att få en ny molntjänst, bör den teknikansvariga identifiera behoven och förstå vilken typ av användbarhet denna tjänst kommer att erbjuda.

- Lokaliseringsfasen: Därefter översätts kraven till tekniska specifikationer och lokaliseringsprocessen inleds tillsammans med upphandlingstjänstemannen (t.ex. en anbudsinfordran offentliggörs). Sjukhuset mottar de utsedda buden, kommittén (inklusive den teknikansvariga/säkerhetsansvariga för de centrala datasystemen eller/och en medlem av IT-teamet) utvärderar buden och väljer de mest lämpliga produkterna. Förhandlingar genomförs med anbudsgivaren och avtalet tilldelas.

- Förvaltningsfasen: Slutligen tilldelas avtalet (förvaltning och övervakning) till företagets ägare inom sjukhuset. Den utsedda tjänstemannen är ansvarig för att avsluta anbudet och ta emot feedback från användarna om utrustningens/systemets/tjänstens faktiska prestanda.

TYPER AV UPPHANDLING PÅ SJUKHUS

Tabell 1: Typer av upphandling (tillgångstaxonomi)

Typ av upphandling	Typ av beskrivning
Kliniska informationssystem	Inbegriper upphandling av någon form av programvara som är inriktad på medicinsk vård
Medicintekniska produkter	All maskinvara som är avsedd för behandling, kontroll eller diagnos av sjukdomar
Nätutrustning	Nätverkslinjer (koaxiala, optiska), nätportar, routrar, omkopplare, brandväggar, VPN:er, IPS, IDS osv.
Vårdsystem på distans	Faciliteter eller anordningar som ger vård utanför sjukhusmiljön, särskilt vad som i dag kallas ”sjukhusbaserade hemvårdstjänster”.
Mobila klientanordningar	All programvara som avser vårdrelaterad eller medicinsk datainsamling som inte är direkt ansluten till sjukhusnätverket, till exempel, appar för telemedicin
Identifieringssystem	System för att unikt identifiera patienter eller medicinsk personal (biometriska skannrar, kortläsare osv.) och garantera identifiering och/eller behörighet att komma åt IT-systemen.
System för fastighetsdrift	Alla typer av konstruktioner som kan rymma medicinska anläggningar.
Industriella styrsystem	System som styr alla fysiska aspekter av centren, såsom effektregleringssystem, dörrlåssystem, säkerhetssystem för nära kretsar.
Professionella tjänster	Alla typer av tjänster som har lagts ut på entreprenad eller inte, tillhandahållna av personal eller företag: medicinska tjänster, transport, redovisning, ingenjörskonst, IT, juridiska tjänster, underhåll, städning, catering osv.
Molntjänster	Alla kommunikations- och informationssystem eller andra informationssystem som inte finns i den medicinska byggnaden eller i en datacentral under fullständig kontroll av IT-avdelningen för vårdenheten.

HOTTAXONOMI

Olika typer av upphandling är förknippade med olika hot mot sjukhusets IKT-miljö. Konsultera hottaxonomin som presenteras i detta avsnitt tillsammans med din IT-, säkerhets- eller riskavdelning för att identifiera vilka hot som är mest relevanta för din organisation. Denna aktivitet bör vara en del av IT-uppgifterna på sjukhuset oavsett upphandlingspotentialen.

Tabell 2: Typer av hot (hottaxonomi)

Hot	Exempel
Naturkatastrofer	Eldsvåda, översvämningar eller jordbävningar
Fel i leveranskedjan	Fel hos leverantör av molntjänster, fel hos nätleverantör, fel i kraftförsörjning, fel hos tillverkare av medicintekniska produkter/ansvarsfrihet
Mänskliga fel	Konfigurationsfel för medicinska system, frånvaro av logginformation, obehörig åtkomstkontroll/brist i processen, bristande efterlevnad (BYOD), fel av sjukvårdspersonal/patient
Illvilliga handlingar	Sabotageprogram (virus, utpressningsprogram, BYOD), kapning (kryptokapning, kapning av medicintekniska produkter), social manipulering (nätfiske, lockbete, kloning av enheter), stöld (av uppgifter, enheter), manipulering av medicintekniska produkter, skimning, tillgänglighetsförlust, webbaserade attacker, webbapplikationsattacker, internt hot, fysisk manipulering/skada, identitetsstöld, cyberspionage, störningar för mekaniska komponenter
Systemfel	Programvarufel, föråldrad fast programvara, enhetsfel, nätverkskomponentfel, otillräckligt underhåll

GODA RUTINER FÖR CYBERSÄKERHET INOM UPPHANDLING

Listan över goda rutiner nedan är inte uttömmande, den ger dock en solid fördel för IT-personal inom sjukvård som ansvarar för inköp av utrustning på ett sjukhus. Uppsättningen av goda rutiner är det kollektiva resultatet av alla synpunkter från intervjuad vårdpersonal. Läsaren kan anpassa listan baserat på prioriteringarna i sin organisation.

GR 1. Engagera IT-avdelningen i olika skeden av upphandlingen för att säkerställa att expertis inom cybersäkerhetsaspekter beaktas.

Upphandlingsfaser: Samtliga

Relaterade typer av upphandling: Samtliga

Relaterade hot: Samtliga

GR 2. Implementera en identifierings- och hanteringsprocess för sårbarheter för att säkerställa att sårbarheter beaktas innan nya produkter eller tjänster upphandlas och att sårbarheter hos befintliga produkter/tjänster övervakas under hela deras livscykel.

Upphandlingsfaser: Samtliga

Relaterade typer av upphandling: Kliniska informationssystem, medicintekniska produkter, nätutrustning, vårdsystem på distans, mobila klientanordningar, identifieringssystem, industriella styrsystem, molntjänster

Relaterade hot: Samtliga

GR 3. Utveckla en policy för maskinvaru- och programvaruuppdateringar för att säkerställa att de senaste patcherna för ditt operativsystem och programvara tillämpas och att antivirusprogrammet uppdateras.

Upphandlingsfaser: Samtliga

Relaterade typer av upphandling: Medicintekniska produkter, kliniska informationssystem, nätutrustning, vårdsystem på distans, mobila klientanordningar, identifieringssystem, industriella styrsystem, molntjänster

Relaterade hot: Illvilliga handlingar, fel i leveranskedjan, systemfel

GR 4. Förbättra säkerhetskontrollerna för trådlös kommunikation för att säkerställa att tillgången till sjukhusets wifi-nätverk är begränsad och strikt kontrollerad.

Upphandlingsfaser: Samtliga

Relaterade typer av upphandling: Medicintekniska produkter, klientanordningar på distans, identifieringssystem, molntjänster

Relaterade hot: Illvilliga handlingar, mänskliga fel

GR 5. Fastställa testpolicy för att säkerställa att nyligen förvärvade eller nykonfigurerade produkter genomgår ett penetrationstest och att de avhjälpande åtgärderna som vidtas är i linje med de operativa parametrarna för den faktiska miljön.

Upphandlingsfaser: Samtliga

Relaterade typer av upphandling: Kliniska informationssystem, medicintekniska produkter, nätutrustning, vårdsystem på distans, mobila klientanordningar, identifieringssystem, system för fastighetsdrift, industriella styrsystem, molntjänster

Relaterade hot: Illvilliga handlingar, systemfel, mänskliga fel

GR 6. Fastställa driftskontinuitetsplaner för att säkerställa att ett systems fel inte kommer att störa sjukhusets kärntjänster och att leverantörens roll är väl definierad.

Upphandlingsfaser: Samtliga

Relaterade typer av upphandling: Medicintekniska produkter, kliniska informationssystem, nätutrustning, vårdsystem på distans, mobila klientanordningar, identifieringssystem, industriella styrsystem, molntjänster

Relaterade hot: Illvilliga handlingar, fel i leveranskedjan, systemfel

GR 7. Ta hänsyn till interoperabilitetsproblem för att säkerställa att det inte finns några säkerhetsluckor med de komponenter som redan finns (befintlig IT).

Upphandlingsfaser: Samtliga

Relaterade typer av upphandling: Kliniska informationssystem, medicintekniska produkter, vårdsystem på distans, mobila klientanordningar, identifieringssystem, industriella styrsystem, molntjänster

Relaterade hot: Systemfel, mänskliga fel, illvilliga handlingar

GR 8. Göra testning av alla komponenter möjlig för att garantera att de levererar vad som lovats: Verifiera användarvänlighet, kontrollera korrektheten av resultat under belastning och kontrollera säkerhetsbrister (policy för svaga lösenord, SQL-injektion).

Upphandlingsfaser: Samtliga

Relaterade typer av upphandling: Kliniska informationssystem, medicintekniska produkter, klientanordningar på distans, identifieringssystem, molntjänster, industriella styrsystem, vårdsystem på distans, system för fastighetsdrift, mobila klientanordningar

Relaterade hot: Illvilliga handlingar, mänskliga fel, systemfel, fel i leveranskedjan

GR 9. Tillåta granskning och loggning för att spåra angripare och hur mycket information som förlorades/stulits när systemet äventyras.

Upphandlingsfaser: Samtliga

Relaterade typer av upphandling: Medicintekniska produkter, vårdsystem på distans, mobila klientanordningar, identifieringssystem, industriella styrsystem

Relaterade hot: Illvilliga handlingar, fel i leveranskedjan, systemfel

GR 10. Kryptera känsliga personuppgifter i vila och i transit genom att definiera en policy för system, tjänster eller anordningar som behandlar de särskilda kategorierna av personuppgifter som anges i artikel 9 i dataskyddsförordningen.

Upphandlingsfaser: Samtliga

Relaterade typer av upphandling: Medicintekniska produkter, kliniska informationssystem, nätutrustning, vårdsystem på distans, mobila klientanordningar, identifieringssystem, industriella styrsystem, molntjänster

Relaterade hot: Illvilliga handlingar, fel i leveranskedjan, systemfel

GR 11. Genomföra en riskbedömning som en del av upphandlingsprocessen.

Upphandlingsfaser: Planering

Relaterade typer av upphandling: Samtliga

Relaterade hot: Samtliga

GR 12. Planera nät-, maskinvaru- och licenskrav i förväg för att avgöra om ytterligare uppgraderingar och/eller inköp måste göras innan installationen för att tillgodose det nya systemet.

Upphandlingsfaser: Planering

Relaterade typer av upphandling: Kliniska informationssystem, nätutrustning, identifieringssystem, industriella styrsystem.

Relaterade hot: Fel i leveranskedjan, systemfel, naturkatastrofer, mänskliga fel

GR 13. Identifiera hot relaterade till upphandlingsprodukter eller -tjänster och säkerställa att hotidentifieringen är kontinuerlig under upphandlingens livscykel.

Upphandlingsfaser: Planering, förvaltning

Relaterade typer av upphandling: Samtliga

Relaterade hot: Samtliga

GR 14. Segregera ditt nätverk för att säkerställa att nätverkstrafik kan isoleras och/eller filtreras för att begränsa och/eller förhindra åtkomst mellan nätverkszoner.

Upphandlingsfaser: Planering, lokalisering

Relaterade typer av upphandling: Medicintekniska produkter, kliniska informationssystem, nätutrustning, vårdsystem på distans, mobila klientanordningar, identifieringssystem, industriella styrsystem, molntjänster

Relaterade hot: Illvilliga handlingar, fel i leveranskedjan, systemfel

GR 15. Bestämma nätverkskrav för att säkerställa interoperabilitet och undvika luckor efter att ha skapat nättopologi och komponenttopologi.

Upphandlingsfaser: Planering

Relaterade typer av upphandling: Kliniska informationssystem, nätutrustning, identifieringssystem, industriella styrsystem., molntjänster, vårdsystem på distans, mobila klientanordningar.

Relaterade hot: Fel i leveranskedjan, systemfel, naturkatastrofer

GR 16. Fastställa grundläggande säkerhetskrav och översätta dem till urvalskriterier vid val av leverantör.

Upphandlingsfaser: Planering, lokalisering

Relaterade typer av upphandling: Medicintekniska produkter, kliniska informationssystem, nätutrustning, vårdsystem på distans, mobila klientanordningar, identifieringssystem, industriella styrsystem, molntjänster

Relaterade hot: Illvilliga handlingar, fel i leveranskedjan, systemfel

GR 17. Skapa en dedikerad förslagsinfordran för upphandling av molntjänster som tar hänsyn till rättsliga och policymässiga krav.

Upphandlingsfaser: Planering, lokalisering

Relaterade typer av upphandling: Molntjänster

Relaterade hot: Illvilliga handlingar, fel i leveranskedjan

GR 18. Prioritera upphandling av tillgångar som är certifierade mot cybersäkerhetssystem/-standarder.

Upphandlingsfaser: Lokalisering

Relaterade typer av upphandling: Medicintekniska produkter, kliniska informationssystem, nätutrustning, vårdsystem på distans, mobila klientanordningar, identifieringssystem, industriella styrsystem, molntjänster

Relaterade hot: Illvilliga handlingar, fel i leveranskedjan, systemfel

GR 19. Genomföra konsekvensbedömning avseende dataskydd vid planering av upphandling av ett nytt system eller tjänst.

Upphandlingsfaser: Lokalisering

Relaterade typer av upphandling: Kliniska informationssystem, medicintekniska produkter, nätutrustning, vårdsystem på distans, mobila klientanordningar, identifieringssystem, professionella tjänster, molntjänster

Relaterade hot: Illvilliga handlingar, mänskliga fel

GR 20. Ställa in nätportar som håller befintliga system/maskiner anslutna och som ger gränskontroll vid problem inom dessa grupper.

Upphandlingsfaser: Lokalisering, förvaltning

Relaterade typer av upphandling: Medicintekniska produkter, vårdsystem på distans, mobila klientanordningar, identifieringssystem, industriella styrsystem

Relaterade hot: Illvilliga handlingar, fel i leveranskedjan, systemfel

GR 21. Ge cybersäkerhetsutbildning om organisationens säkerhetsrutiner för att säkerställa att intern personal eller externa entreprenörer/konsulter som arbetar på plats är lämpligt utbildade.

Upphandlingsfaser: Lokalisering, förvaltning

Relaterade typer av upphandling: Samtliga

Relaterade hot: Illvilliga handlingar, mänskliga fel

GR 22. Utveckla incidenthanteringsplaner som omfattar nyligen förvärvade produkter eller system.

Upphandlingsfaser: Lokalisering, förvaltning

Relaterade typer av upphandling: Medicintekniska produkter, kliniska informationssystem, nätutrustning, vårdsystem på distans, mobila klientanordningar, identifieringssystem, industriella styrsystem, molntjänster

Relaterade hot: Illvilliga handlingar, fel i leveranskedjan, systemfel

GR 23. Engagera leverantörer/tillverkare i incidenthanteringen och ange tydliga villkor i förslagsinfordran.

Upphandlingsfaser: Lokalisering, förvaltning

Relaterade typer av upphandling: Medicintekniska produkter, kliniska informationssystem, nätutrustning, vårdsystem på distans, mobila klientanordningar, identifieringssystem, industriella styrsystem, molntjänster

Relaterade hot: Illvilliga handlingar, fel i leveranskedjan, systemfel

GR 24. Planera och övervaka underhållsoperationer för all utrustning för att säkerställa en lämplig funktionsnivå och besluta om uppdateringar/patcher osv.

Upphandlingsfaser: Lokalisering, förvaltning

Relaterade typer av upphandling: Kliniska informationssystem, nätutrustning, medicintekniska produkter, system för fastighetsdrift, vårdsystem på distans, mobila klientanordningar, identifieringssystem, industriella styrsystem, molntjänster

Relaterade hot: Mänskliga fel, systemfel, naturkatastrofer

GR 25. Fjärråtkomst bör minimeras och administreras på ett sådant sätt att extern kommunikation med leverantören begränsas till endast den enhet som de måste kontrollera.

Upphandlingsfaser: Lokalisering, förvaltning

Relaterade typer av upphandling: Medicintekniska produkter, kliniska informationssystem, nätutrustning, vårdsystem på distans, mobila klientanordningar, identifieringssystem, industriella styrsystem, molntjänster

Relaterade hot: Illvilliga handlingar, fel i leveranskedjan, systemfel, mänskliga fel

GR 26. Kräva patchning för alla komponenter och inkludera information i förslagsinfordran.

Upphandlingsfaser: Lokalisering, förvaltning

Relaterade typer av upphandling: Medicintekniska produkter, kliniska informationssystem, nätutrustning, vårdsystem på distans, mobila klientanordningar, identifieringssystem, industriella styrsystem, molntjänster

Relaterade hot: Illvilliga handlingar, fel i leveranskedjan, systemfel

GR 27. Öka medvetenheten om cybersäkerhet bland personalen för att säkerställa att den är medveten om riskerna med nyligen förvärvade produkter eller tjänster.

Upphandlingsfaser: Förvaltning

Relaterade typer av upphandling: Samtliga

Relaterade hot: Samtliga

GR 28. Genomföra tillgångsinventering och konfigureringshantering för att säkerställa att inventariet uppdateras på lämpligt sätt när någon komponent läggs till eller tas bort från IKT-miljön och att grundläggande säkerhetskonfigurationer för IKT-komponenter finns och hanteras på lämpligt sätt.

Upphandlingsfaser: Förvaltning

Relaterade typer av upphandling: Kliniska informationssystem, medicintekniska produkter, nätutrustning, vårdsystem på distans, mobila klientanordningar, identifieringssystem

Relaterade hot: Illvilliga handlingar, mänskliga fel, systemfel

GR 29. Inrätta särskilda åtkomstkontrollmekanismer för medicintekniska produkter som också bör vara fysiskt skyddade och endast tillgängliga för specialiserad personal.

Upphandlingsfaser: Förvaltning

Relaterade typer av upphandling: Medicintekniska produkter, system för fastighetsdrift, identifieringssystem

Relaterade hot: Illvilliga handlingar, mänskliga fel

GR 30. Planera penetrationstester ofta eller efter en förändring i arkitekturen/systemet och inkludera villkoren i förslagsinfordran.

Upphandlingsfaser: Lokalisering, förvaltning

Relaterade typer av upphandling: Medicintekniska produkter, kliniska informationssystem, nätutrustning, vårdsystem på distans, mobila klientanordningar, identifieringssystem, industriella styrsystem, molntjänster

Relaterade hot: Illvilliga handlingar, fel i leveranskedjan, systemfel