# CHECKLISTA FÖR ATT UTVÄRDERA LEVERANTÖRER AV KONSULTINKÖPSSYSTEM (VMS) MED FOKUS PÅ SÄKERHET OCH DATALAGRING:

## Åtkomstkontroll:

Kontrollera att konsultinköpssystemet erbjuder robusta åtkomstkontroller som möjliggör definiering av roller och behörigheter för olika användare.

## Spårbarhet och transparens:

Efterfråga information från leverantören om hur spårbarhet på transaktioner i systemet följas och hur leverantören arbetar för att säkerställa datans pålitlighet.

## Autentisering och auktorisering:

Bekräfta att systemet stödjer starka autentiseringsmetoder (t.ex. multifaktorautentisering för leverantörer eller SSO för anställda) och erbjuder detaljerade auktoriseringsinställningar.

## Efterlevnad av dataskyddslagar:

Säkerställ att leverantören följer relevanta dataskyddsföreskrifter såsom GDPR eller branschspecifika standarder.

## Databackuper och återställning:

Kontrollera att leverantören har pålitliga procedurer för databackuper och återställning för att skydda mot dataförlust.

## Incidenthantering och övervakning:

Ta reda på om leverantören har en plan för incidenthantering och övervakningsförmåga för att upptäcka och svara på säkerhetsincidenter i realtid.

## Nätverkssäkerhet:

Bedöm vilka åtgärder som är vidtagna för att skydda mot nätverksbaserade attacker, inklusive brandväggar, intrångsdetektering/ -förebyggande system och nätverkssegmentering.

## Fysisk säkerhet av datacenter:

Säkerställ att leverantörens datacenter har ordentliga åtgärder för fysisk säkerhet, såsom åtkomstkontroller, övervakning och katastrofåterhämtningsplaner.

## Leverantörens säkerhetscertifikat och revisioner:

Kontrollera att leverantören har branscherkända säkerhetscertifikat och genomgår regelbundna säkerhetsrevisioner.

## Säker programvaruutvecklingslivscykel (SDLC):

Fråga om processer och praxis som leverantören följer för att säkerställa att säkerhet integreras i utvecklingen av deras programvara.

## Hantering av programuppdateringar:

Förstå hur leverantören hanterar programuppdateringar och patchar för att snabbt åtgärda säkerhetssvårigheter.

## Katastrofhantering och redundans:

Bekräfta att konsultinköpssystemet har robusta planer för katastrofhantering och redundanta system för att säkerställa oavbruten service vid eventuella driftstopp.

## Dataskydd och äganderätt:

Klargör dataskyddspolicys och äganderättsliga rättigheter för att säkerställa att de är i linje med din organisations krav.

## Kontraktsliga säkerhetsavtal:

Granska kontraktet för att säkerställa att säkerhetsansvar, ansvar och förpliktelser är tydligt definierade.

## Datakryptering:

Se till att data är krypterad både under överföring (användande av protokoll som HTTPS) och vid lagring (säker förvaring).

## Referenser och rykte:

Efterfråga referenser från befintliga kunder för att bedöma deras nöjdhet med leverantörens säkerhetsåtgärder.

## Säkerhetsträning och medvetenhet:

Fråga om utbildnings- och medvetenhetsprogram som finns för anställda för att säkerställa att de förstår och följer säkerhetsbästa praxis.

## Efterlevnad av branschstandarder:

Kontrollera om leverantören följer branschspecifika säkerhetsstandarder och certifieringar som är relevanta för din organisation.

**Kom ihåg, noggrann due diligence inom säkerhets- och hosting aspekter är avgörande för att säkerställa skyddet för känsliga data och den övergripande integriteten i din VMS-lösning.**

---

Inkopio AB
Mäster Samuelsgatan 36
111 57 Stockholm, Sweden
Org: 556974-2108