Göteborgs Stad

Riskanalys för informationssäkerhet

Copilot chatt

2025-04-11

Versionshantering

Datum	Version	Beskrivning	Ändrat av
2025-04-02	1.0	Rapport efter riskanalys	Marcus Broman
2025-04-11	1.01	Uppdaterat med kategorier av risker	Marcus Broman

Innehållsförteckning

Deltagande

Namn	Roll
Marcus Broman	Expertstöd informationssäkerhet och dataskydd, Enheten för informationssäkerhet
Maria Dahlgren	Enhetschef Samarbetsplattform, Digital arbetsplats
Mikael Schou Maegaard	Domänarkitekt, Digital arbetsplats
Fredrik Andersson	Enheten för informationssäkerhet
Razvan Nutu	Verksamhetschef Digital arbetsplats, Beställare
Robert Hansson	Förvaltningsledare Digital arbetsplats: Office 365
Emelie Arnell	Verksamhetsutvecklare, Digital arbetsplats
Katarina Kokolj	Verksamhetsutvecklare, Digital arbetsplats

1 Bakgrund

Bakgrunden till att genomföra en hot- och riskanalys för Copilot chatt grundar sig i behovet av att förstå och reducera potentiella säkerhetsrisker. Det är avgörande att identifiera säkerhetshot och sårbarheter som skulle kunna leda till oönskade händelser.

En hot- och riskanalys ger en inledande systematisk översyn av vilka informationssäkerhetsrisker som finns med användningen av Copilot chatt, inklusive risker för dataläckage eller otillräckligt dataskydd. Denna analys är nödvändig för att:

- Identifiera och hantera potentiella hot mot konfidentialitet, riktighet och tillgänglighet av information som skulle komma hanteras genom Copilot chatt.
- Föreslå tekniska och administrativa åtgärder som är effektiva för att hantera identifierade risker.
- Skapa en grund för fortsatt hantering av risker för andra intressenter och i olika verksamheter, som kravställningar.
- Skapa en grund för kunna hantera nya funktioner som utvecklas och implementeras för hur Copilot chatt skulle integreras i staden.

Verksamhetschefen för digital arbetsplats har därför beställt denna analys av enheten för informationssäkerhet vid Intraservice.

1.1 Kontexten för riskanalysen

Riskanalyser inom informationssäkerhet sker i ett sammanhang och detta kräver en tydlig förståelse av omfattningen, grundläggande krav från intressenter, risk- och acceptenskriterier samt målen med analysen.

En effektiv riskanalys inom informationssäkerhet måste omfatta både interna och externa faktorer. Interna faktorer inkluderar identifiering av intressenter, förståelse för interna regelverk, klassning av information baserat på känslighet, granskning av informationssystem och deras sårbarheter, samt ekonomiska och tidsmässiga aspekter av säkerhetsåtgärder. Externa faktorer som måste beaktas är lagar och författningar, avtal och förpliktelser, krav mot interna tjänster som Intraservice, tillämpning av säkerhetsstandarder, leverantörers pålitlighet, samt omvärldshot och andra externa risker. En genomtänkt analys av dessa faktorer bidrar till robustare riskhantering och stärker organisationens informationssäkerhet.

Metoder som workshops och omvärldsbevakning används för att säkerställa att analysen är aktuell och baserad på relevant kunskap.

Riskanalysen avser Microsofts Copilot chatt och har tagits fram som underlag för att kunna fatta beslut om att åter aktivera tjänsten i stadens O365-miljö. Tjänsten har tidigare stoppats på grund av osäkerheter kring informationssäkerhet, integritet och brist på tydliga riskbedömningar. Analysen syftar därför till att identifiera konkreta risker med hur Copilot chatt hanterar data, exempelvis åtkomst till känslig information, AI-genererade fel och otydlig ansvarsfördelning. Den ger också stöd i att bedöma vilka skyddsåtgärder och begränsningar som krävs för att möjliggöra ett säkert införande i verksamheten.

1.1.1 Omfattning och avgränsning

Omfattningen och avgränsningen gäller teknisk och logisk informationssäkerhet. Detta innebär en översyn av de säkerhetsåtgärder som innefattas i hot mot stadens information som Copilot chatt skulle kunna medföra.

En avgränsning är att analysen inte hanterar verksamhetsspecifika dataskyddsrisker eller andra juridiska hot som inte kan hanteras genom tekniska åtgärder.

Denna riskanalys omfattar användningen av Copilot chatt, en fristående AI-chattjänst som görs tillgänglig inom stadens O365-miljö, men som inte är integrerad i 365-appar som Word, Outlook eller Teams.

Riskanalysen för Copilot chatt omfattar i nuläget två utföranden:

1. Copilot chatt i Edge, där assistenten använder information från den aktuella fliken i det öppna webbfönstret genom ett sidofönster

2. Copilot chatt för webb – ett webbläge där assistenten använder den information man väljer att skriva in eller dela samt Bing-sökningar för att ge svar baserade på allmän internetinformation.

Fokus ligger på att Copilot chatt erbjuder ett sätt att erbjuda AI på svenska servrar och den koppling som finns till O365 är att information hämtas från användaren har en licens inom organisationens Microsoft-miljö. Riskanalysen är avgränsad till frågor om informationssäkerhet och användaransvar.

Denna riskanalys omfattar inte andra Copilot-tjänster eller privat användning utan inloggning, ej heller användning genom en Copilot-app, externa AI-verktyg eller funktioner inom M365-program.

Exempel på vägledande frågeställningar i analysen är:

- Vilka risker finns det med att Copilot chatt får åtkomst till och genererar innehåll baserat på skyddsvärd information?
- Vilka organisatoriska eller tekniska hinder kan påverka en säker och effektiv återaktivering av tjänsten?

1.1.2 Grundläggande krav från intressenter

Det är i första hand hot och risker som kommer med en tänkt användning av tekniken, som identifierats.

Stadens dataskyddsombud, Dataskyddsenheten (DSE), lyfter att Copilot chatt innebär allvarliga dataskyddsrisker. De pekar på att tjänsten kan få åtkomst till mejl, filer och mappar via webben och skicka information vidare till externa tjänster som Bing, där Microsoft är personuppgiftsansvarig – utan att detta omfattas av stadens befintliga avtal. Riskanalysen behöver därför klargöra hur Copilot chatt fungerar tekniskt och hur data hanteras, så att denna riskbild adresseras.

1.1.3 Mål med riskhanteringen

Målet med riskhanteringen är att belysa de tekniska aspekterna, identifiera de hot som användningen kan innebära, samt utvärdera hur dessa hot kan hanteras direkt i verktyget eller genom åtgärder som verksamhet behöver initiera.

Riskanalysen ska ge ett konkret beslutsunderlag för om och hur Copilot chatt kan återaktiveras i stadens O365-miljö. Målet är att tydliggöra förutsättningarna för ett säkert och kontrollerat återinförande.

Analysen bygger på kriterier som informationssäkerhet, kontroll över informationsdelning, användarnas ansvar och ansvaret för efterlevnaden av GDPR.

Analysen ska användas för att bedöma riskerna med Copilot chatt, utan att inkludera andra Copilot-tjänster eller AI-funktioner inom Office365.

1.1.4 Metod för hantering av informationssäkerhetshot och risker

En risk inom informationssäkerhet och riskhantering kan definieras som en kombination av sannolikheten för att en händelse ska inträffa och konsekvenserna av händelsen om den skulle inträffa gentemot en identifierad informationstillgång.

Ett hot definieras som en potentiell orsak till en oönskad händelse som skulle kunna resultera i skada på system, organisationer, individer eller miljö. Ett hot är något som kan utnyttja en sårbarhet för att åstadkomma skada och har potentialen att orsaka skada, men det är inte säkert så kommer att ske. Tillgångar är i hothantering mer av allmän karaktär.

Riskhantering i denna analys innebär att identifiera, bedöma och prioritera hot samt genomföra åtgärder i form av att undvika, överföra, reducera eller acceptera hoten. Riskhanteringen är därmed inte färdig utan behöver fortsätta vad avser de informationstillgångar som hoten skulle kunna rikta sig mot.

Identifiering har skett genom omvärldsbevakning, riskworkshoppar och dokumentgranskning av Microsofts underlag. Även har tester utförts för att se vilken information som Copilot chatt faktiskt använder när ett webbläsarfönster är öppet

Riskprocessen, som beskrivs i “Processbeskrivning – Riskhantering informationssäkerhet”, ger en fullständig översikt över hur risker hanterades inom Intraservice och det praktiska genomförandet av en riskbedömning, ledd av en analysledare, och genomfördes i tre huvudsteg.

Steg 1: Identifiering och beskrivning av risker

Det första steget i riskanalysprocessen innebar att identifiera vilka risker som fanns genom brainstorming. Utöver själva identifieringen fokuserade detta steg på att arbeta fram en tydlig beskrivning av varje risk. Detta inkluderade att förstå orsakerna till riskerna samt vilka potentiella konsekvenser de kunde medföra. En grundlig beskrivning var avgörande för att kunna hantera riskerna effektivt i senare skeden av processen.

Steg 2: Analys och värdering av risker

I det andra steget genomfördes en diskussion vilket var analys och värdering av de identifierade riskerna. Under detta skede samlades teamet för att diskutera varje risk och värdera sannolikheten att den skulle inträffa samt hur allvarliga konsekvenserna skulle kunna bli. Detta steg innefattade också att räkna ut en risknivå för att sedan kunna prioritera de viktigaste riskerna.

Steg 3: Behandling och förvaltning av risker

Det tredje steget innebar att bestämma vem som skulle ta hand om varje risk vidare, det vill säga vem som blev riskägare. Riskerna skall förvaltas, vilket kan se olika ut i olika delar av organisationen.

Beslut togs om hur riskerna skulle hanteras, reduceras, övervakas eller accepteras beroende på deras natur och påverkan på organisationen.

2 Översiktsbeskrivning av riskområdet och funktionalitet

Microsoft Copilot chatt, även kallad Copilot i Edge, är en AI-assistent integrerad i webbläsaren Microsoft Edge. Den fungerar som ett verktyg för användaren att kommunicera med direkt i sidopanelen via text eller röst utan att lämna den aktuella webbsidan. Copilot kan analysera och sammanfatta innehållet på webbsidor eller dokument som visas i webbläsaren, vilket ger en snabb översikt och underlättar läsningen av långa texter. Den kan också hjälpa till med att formulera text, exempelvis genom att föreslå omformuleringar, förbättra tonfall eller ge förslag på nästa stycke i en skrivprocess. Copilot är integrerad med Microsoft 365-plattformen.

Microsoft betonar att säkerhet och integritet är högt prioriterade i Copilot chatt. När en användare är inloggad med ett organisationskonto aktiveras *Enterprise Data Protection* (EDP), vilket innebär att Copilot omfattas av samma dataskyddsåtgärder och avtalsmässiga garantier som övriga Microsoft 365-tjänster

All kommunikation med Copilot är krypterad, och Microsoft har ingen direkt insyn i användarens chattinnehåll. Den data som matas in används endast för att generera svar och används inte för att vidareutveckla de underliggande AI-modellerna – till skillnad från vissa offentliga AI-tjänster. Microsoft agerar som personuppgiftsbiträde enligt sitt dataskyddsavtal, och Copilot med EDP anses uppfylla kraven i GDPR (dataskyddsförordningen) inom ramen för Microsofts molntjänster. Enheten Digital arbetsplats kan styra Copilot chatt genom att hantera åtkomst, användning och livscykel för tjänsten inom organisationen. De kan till exempel ge tillgång till Copilot chatt separat för förvaltningar, bolag eller grupper.

Webbläsaren kräver att användaren ger sitt medgivande första gången för att Copilot ska få läsa av innehållet på en aktiv webbsida eller dokument. Användaren kan när som helst stänga av den funktionen, vilket ger kontroll över när lokal information delas till AI-tjänsten. När Copilot hämtar information från webben visas källhänvisningar och de sökfrågor som genererats mot Bing i chattsvaret. Detta gör att användaren kan se vilken extern information som använts och vilka webbfrågor Copilot ställt. Microsoft begränsar dessutom vilka data som skickas vid webbsökningar – endast relevanta nyckelord ur användarens fråga skickas till Bing, men inga hela dokument eller webbsidors textinnehåll. Inga användaridentifierande uppgifter följer med dessa sökningar.

2.1 Riskområden

Stadens förvaltningar och bolag bör vara medvetna om informationssäkerhetsriskerna med att använda Copilot chatt. Nedan listas de viktigaste riskområdena och deras påverkan på staden, baserat på Microsofts information.

2.1.1 Röjande av känslig information

Det finns en risk att användare av misstag eller på grund av bristande kunskap förser Copilot med känsliga eller sekretessbelagda uppgifter, såsom personuppgifter om anställda, medborgare eller intern information som inte bör spridas. Trots Microsofts kryptering av data och försäkran om att uppgifterna inte används utanför tjänsten, innebär varje inmatning att informationen lämnar stadens egna IT-miljö och skickas till Microsofts moln för bearbetning.

2.1.2 Begränsad kontroll över dataflödet

När användare i staden använder Copilot hanteras en del av data av Microsofts infrastruktur, vilket innebär att man förlitar sig på leverantörens säkerhetsåtgärder. Staden har begränsad insyn i och teknisk kontroll över vad som händer med data – de baserar sin tillit på de garantier och mekanismer som Microsoft har angett. Om något oväntat inträffar, såsom en säkerhetshändelse eller förändring i datalagring, har staden begränsade möjligheter att upptäcka eller påverka det direkt. Därför är det viktigt att följa Microsofts uppdateringar om Copilot och eventuella ändringar av avtalsvillkor.

2.1.3 Teknisk utveckling utanför stadens kontroll

Copilot och liknande AI-tjänster är nya och snabbt utvecklande teknologier. Microsoft uppdaterar kontinuerligt Copilots AI-modeller och funktioner för att förbättra tjänsten.

För staden innebär detta att verktygets funktioner kan förändras över tid utan att man själv initierar det – till exempel kan nya funktioner läggas till eller molntjänstens sätt att behandla data justeras av Microsoft. Sådana förändringar kan potentiellt introducera nya risker eller kräva att de egna regelverken behöver anpassas. Det kan också finnas en utmaning internt att hänga med i utvecklingen. För att hantera detta behöver staden ha en kontinuerlig bevakning av Copilot-tjänsten och en flexibel riskhanteringsprocess som snabbt kan adressera nya funktioner. Beroendet av en extern leverantörs teknikutveckling gör att egen kontroll minskar, vilket ställer krav på löpande dialog med leverantören och uppdatering av interna policys.

2.1.4 Osäkerheter kring dataöverföring och regelefterlevnad

Som offentlig aktör måste en kommun noga beakta var och hur data behandlas. Copilot drivs i Microsofts moln och även om Microsoft försäkrar att tjänsten är utformad för att följa GDPR och lagring och bearbetning sker på svenska servrar, finns det fortfarande frågor om skyddets praktiska tillräcklighet. Framförallt rör dessa frågor överföring av personuppgifter till tredje land (t.ex. USA). Eftersom Microsoft är ett amerikanskt bolag kvarstår viss osäkerhet om hur amerikanska myndigheter utanför EU kan få tillgång till data, trots adekvansbeslut, standardavtalsklausuler och andra juridiska skyddsmekanismer. Detta har blivit särskilt uppmärksammat efter Schrems II-domen. Denna fråga har redan behandlats i andra riskanalyser och är inte unik för Copilot chatt. Sammanfattningsvis behöver regelefterlevnad och dataskydd utvärderas löpande vid användning av Copilot, så att staden inte oavsiktligt bryter mot exempelvis offentlighets- och sekretesslag eller GDPR.

2.1.5 Risk för felaktigt eller vilseledande svar

Copilot använder Open AI:s GPT-4o för att generera svar, vilket kan ge övertygande men felaktiga eller inaktuella svar. Microsoft varnar för att systemet trots kvalitetskontroller kan producera felaktig information. I kommunal verksamhet kan detta leda till risker såsom felaktiga beslut eller spridning av missvisande information. Användare bör granska och verifiera Copilots output och inte se den som garanterad sanning. Staden bör uppmuntra en kritisk användning av AI-assistenten genom att dubbelkolla fakta och använda mänskligt omdöme.

3 Sammanfattning av risker

Risker i denna rapport översiktligt och utan detaljer av de hot som identifierats, samt utan med en direkt koppling till informationstillgångar. En fullständig beskrivning av som omfattar olika aspekter såsom tillgång, hot, oönskade

händelser, existerande skydd, sårbarheter och konsekvenser finns i excelfilen *Riskhantering - Copilot chatt - 2025-04-11.xlsx*

21 risker identifierades, varav de prioriterats i risknivåer som mycket höga, höga, medel och låga.

3.1.1 Riskkategorier

Riskerna är grupperade i kategorierna:

- Tekniska risker
- Användningsrisker
- Organisatoriska risker
- dataskyddsrisker

Kategorierna gör det enklare att överblicka risker. Målet är att visualisera risker för att underlätta förvaltningars och bolags förståelse av relevanta risktyper, deras koppling till verksamheten och identifiering av nödvändiga åtgärder.

Varje verksamhet behöver granska lokala risker, speciellt vad gäller användning och dataskydd. Användarnas arbete med AI-verktyg, informationshantering och efterlevnad av interna styrdokument direkt påverkar dessa risker.

3.1.2 Mycket höga risker

Inga risker

3.1.3 Höga risker

Två risker:
#5 Utbildning saknas som leder till röjande oavsiktligt
#6 Användare lägger medvetet in information av känslig karaktär för bearbetning av data

3.1.4 Medelrisker

Elva risker:
#1 Begränsad faktakontroll
#2 Risk för bias i modellen
#3 Bristande förståelse för kontext (chat-app)
#8 Bristande förståelse för kontext (Edge)
#10 Copilot Chat kan ge inaktuell information
#12 Microsoft ändrar betalningsmodell

#15 Microsoft får tillgång till känslig information i aktuellt webbfönster
#16 Olämplig lagring av skyddsvärda data i molnet när filer laddas upp
#17 Informationen kan behandlas i länder utanför EU
#19 Kontinuerlig snabb vidareutveckling av AI-tjänsten
#20 Använder Copilot utan att vara inloggad

3.1.5 Låga risker

Inga risker

3.1.6 Strukna eller flyttade risker

Risk flyttas:
#7 Skugg Generativ-AI (vilket är en indirekt risk och inte gäller Copilot)
#4 Stresspåslag för de som hamnar efter
#11 Edge uppdateras var 8:e vecka utan att nyheter bedöms
#18 EU-domstolen eller EU-kommissionen anser att USA är opålitligt.
#21 Göteborgs Stad ses som en oattraktiv arbetsgivare

Strukna risker
#9 Målmedveten påverkan (ligger i AI-modellen, kan inte hanteras av Digital arbetsplats)

Strukna risker som är dubbletter av #5:
#13 Användare skickar omedvetet känslig information till Microsoft
#14 Känslig information hamnar hos Microsoft

3.2 Tabell över risker

Risker presenteras i en gruppering av olika kategorier av risker och därefter i den ordning de prioriteras (ej strukna eller flyttade risker).

Riskidentifiering			**Riskbehandling**	
Nr	**Riskrubrik**	**Oönskad händelse**	**Alternativ**	**Tänkt åtgärd**
Användningsrisker 👥				
5	Utbildning saknas som leder till röjande oavsiktligt	Användaren sprider information som är känslig. Röjande.	Reducera risk ↙	A2: Utbildning i hur generativ AI används.
6	Användare lägger medvetet in information av	Känslig information hamnar utanför vår kontroll	Reducera risk ↙	A3: Uppdatera regler för användning av IT så att de även omfattar användning

	känslig karaktär för bearbetning av data			av generativ AI, och att dessa regler gäller för hela staden. A2: Utbildning i hur generativ AI används.
1	Begränsad faktakontroll	Användaren kan fatta beslut baserade på osanna eller missvisande uppgifter	Reducera risk ↙	A2: Utbildning i hur generativ AI används.
20	Använder Copilot utan att vara inloggad	Införande av ny funktionalitet som vi inte känner till	Reducera risk ↙	A2: Utbildning i hur generativ AI används.
3	Bristande förståelse för kontext (chat-app)	Kan leda till ineffektiva svar	Reducera risk ↙	A2: Utbildning i hur generativ AI används.
Dataskyddsrisker				
15	Microsoft får tillgång till känslig information i aktuellt webbfönster	Användare ber Copilot om att sammanfatta innehållet av fliken i Edge, och Copilot läser öppen flik som innehåller känslig info	Reducera risk ↙	A2: Utbildning i hur generativ AI används. A6: Om en förvaltning eller ett bolag väljer att återaktivera sidofönstret för Copilot chatt i Edge rekommenderas att tydliga instruktioner ges.
16	Olämplig lagring av skyddsvärda data i molnet när filer laddas upp	Användare delar med sig av skyddsvärd information via chattar, uppladdning av filer eller på annat sätt.	Reducera risk ↙	A2: Utbildning i hur generativ AI används.
17	Informationen kan behandlas i länder utanför EU	Information som skickas till Bing kan innehålla olämpliga data	Reducera risk ↙	A2: Utbildning i hur generativ AI används.
Tekniska risker				
2	Risk för bias i modellen	Risk att diskriminerande mönster reproduceras	Reducera risk ↙	A2: Utbildning i hur generativ AI används
8	Bristande förståelse för kontext (Edge)	Kan leda till ineffektiva svar	Reducera risk ↙	A2: Utbildning i hur generativ AI används.
10	Copilot Chat kan ge inaktuell information	Inaktuell information	Reducera risk ↙	T1: Bibehåll aktiveringen mot Bing för att säkerställa

				tillgång till aktuell och uppdaterad information A2: Utbildning i hur generativ AI används.
19	Kontinuerlig snabb vidareutveckling av AI-tjänsten	Införande av ny funktionalitet som vi inte känner till	Reducera risk ↙	A4: Stärk bemanningen inom tjänsten Office 365 för att säkerställa en kontinuerlig bevakning av ny funktionalitet, där även systematisk riskhantering integreras i arbetet.
Organisatorisk risk				
12	Microsoft ändrar betalningsmodell	Microsoft börjat ta betalt för tjänsten	Acceptera risk ▶	A5: Bevaka risken

4 Sammanfattning och rekommendationer

Hot- och riskanalysen för Copilot chatt fokuserar på identifiering och hantering av potentiella risker associerade vid en eventuell implementering och användning inom stadens digitala infrastruktur.

4.1 Åtgärder

Nedan följer en mer utförlig beskrivning av de åtgärder som riskanalysen rekommenderar:

Åtgärd	**Risk(er) om reduceras**
A2: Utbildning i hur generativ AI används på ett effektivt och ansvarsfullt sätt bör ges hög prioritet. För att säkerställa att utbildningsinsatserna når ut i hela organisationen behöver en kommunikationsplan tas fram. Utbildningen kan inkludera: - onlinekurser via utbildningsportalen	1 Begränsad faktakontroll #2 Risk för bias i modellen #3 Bristande förståelse för kontext (chat-app) #5 Utbildning saknas som leder till röjande oavsiktligt

- nano-learning genom korta centrala informationsutskick - möjlighet att avropa externa data- och AI-utbildningar. Som stöd för ett enhetligt och säkert användande bör även en funktionsbeskrivning av Copilot chatt tas fram för förvaltningar och bolag, samt en användarguide som stödjer korrekt användning av generativ AI.	#6 Användare lägger medvetet in information av känslig karaktär för bearbetning av data #8 Bristande förståelse för kontext (Edge) #10 Copilot Chat kan ge inaktuell information #15 Microsoft får tillgång till känslig information i aktuellt webbfönster #16 Olämplig lagring av skyddsvärda data i molnet när filer laddas upp #17 Informationen kan behandlas i länder utanför EU #20 Använder Copilot utan att vara inloggad
A3: Uppdatera regler för användning av IT så att de även omfattar användning av generativ AI, och att dessa regler gäller för hela staden. Varje förvaltning och bolag rekommenderas att ta fram egna anvisningar som tydliggör hur generativ AI ska användas inom den egna verksamheten, i linje med de övergripande reglerna.	#6 Användare lägger medvetet in information av känslig karaktär för bearbetning av data
A5: Det rekommenderas att området bevakas kontinuerligt om Microsoft börjat ta betalt för tjänsten.	#12 Microsoft ändrar betalningsmodell
A6: Om en förvaltning eller ett bolag väljer att återaktivera sidofönstret för Copilot chatt i Edge rekommenderas att tydliga instruktioner ges om att inte använda sidofönstret för att sammanfatta information som är känslig på den webbflik som är aktiv.	#15 Microsoft får tillgång till känslig information i aktuellt webbfönster
T1: Bibehåll aktiveringen mot Bing för att säkerställa tillgång till aktuell och uppdaterad information	#10 Copilot Chat kan ge inaktuell information
T2: Enheten Klientplattform har tagit fram en lösning som gör det möjligt för en förvaltning eller ett bolag att stänga av sidofönstret för Copilot chatt i Edge vid behov. Nuvarande status är att Copilot chatt i Edge är avslagen för hela staden.	#15 Microsoft får tillgång till känslig information i aktuellt webbfönster

4.1.1 Åtgärder för risker som flyttas

Nr	Riskrubrik	Åtgärd
#4	Stresspåslag för de som hamnar efter	Flyttas till HR med motiveringen: Arbetsmiljörisk som bör hanteras genom utbildning för att minska stress via ökad förståelse och trygghet i användning

#7	Skugg Gen-AI	Risken är indirekt, vid avsaknad av rekommenderad lösning i staden. Risk flyttas då det inte gäller Copilot chatt.
#11	Edge uppdateras var 8:e vecka utan att nyheter bedöms	Flyttas till Klientplattform med motiveringen: Klientplattform behöver bevaka och bedöma förändringar i Edge.
#18	EU-domstolen eller EU-kommissionen anser att USA är opålitligt	Risken kan inte hanteras av Digital Arbetsplats, eftersom lagändringar eller domslut påverkar användning oavsett strategi och behöver hanteras på annan nivå.
#21	Göteborgs Stad ses som en oattraktiv arbetsgivare	Ej en informationssäkerhetsfråga och bör hanteras som varumärkesrisk

4.2 Slutsatser

Slutsatsen är att denna strukturerade ansats inte bara underlättar förståelsen av utmaningar med hot och risker för informationssäkerhet. Analysen ger också förslag för att behandla identifierade risker vidare.

Verksamheter behöver göra egna bedömningar av risker och eventuella samt anpassa sin användning av Copilot chatt därefter.

Vidare behöver genomförbarhet bedömmas av de åtgärder som föreslås för att reducera risker. Detta innefattas aspekter av kostnad, tidsåtgång, mognad, mottaglighet, kompetens, komplexitet, teknik, styrdokument, leverantörsavtal, lagar och förordningar samt politisk viljeinriktning.

Med föreslagna åtgärder kan staden återaktivera Copilot chatt för de förvaltningar och bolag som önskar det, med varje enhet ansvarig för sin egen informationshantering.

Inga risken bedömdes som höga efter att föreslagna åtgärder är införda.

5 Bilagor

1. Ett exceldokument *Riskhantering - Copilot chatt - 2025-04-11.xlsx* som är en detaljerad riskbehandlingsplan med en mer fullständig identifiering av hoten.