



Västerås stad

Granskning IT- och informationssäkerhet
December 2022

Sammanfattning

På uppdrag av Västerås stads förtroendevalda revisorer har EY genomfört en granskning av kommunens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att identifiera om det finns brister i kommunens interna kontroll avseende IT- och informationssäkerheten.

Följande revisionskriterier användes:

- ▶ Myndigheten för samhällsskydd och beredskaps (MSBs) ramverk ledningssystem för informationssäkerhet (LIS), som är ett etablerat ramverk i ett stort antal kommuner och inom offentlig förvaltning. Ramverket bygger på den svenska och internationella standarden för informationssäkerhet, ISO/IEC 27000.
- ▶ Kommunallagen
- ▶ Stadens gällande och relevanta styrdokument inom IT- och informationssäkerhet

Granskningen genomfördes från augusti till december 2022 och baserades på intervjuer med identifierade nyckelpersoner i kommunens informationssäkerhetsarbete och genomgång av insamlad dokumentation. Granskningen bygger på EY:s ramverk för granskning av IT- och informationssäkerhet, "Granskningsprogram Cyber- och Informationssäkerhet" (GCI), särskilt framtagen för svensk kommunal sektor. Enligt metoden bedöms kommunens mognadsgrad enligt 57 punkter på en ordinarie skala från 1 (*begynnande*) till 5 (*optimerad*) inom de respektive områdena. Representanter för kommunens informationssäkerhetsarbete har beretts tillfälle att faktagranska rapporten som även kvalitetssäkrats internt av EY:s utsedda kvalitetsgranskare.

Baserat på den analys och granskning som genomförts bedöms Västerås stad ha en genomsnittlig mognadsgrad på 2,50 vilket är något lägre än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Givet den stora mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras inom Västerås stads är mognadsgraden, trots att den är nära genomsnittet, lägre än vad EY rekommenderar för en kommun likt Västerås stad. Granskningsresultatet indikerar att kommunens mognadsgrad är högst inom området personal och behörigheter. Kommunens lägsta mognadsgrad är inom området programförändringar.

I granskningen har ett antal förbättringsområden identifierats och rekommendationer lämnats. Främst rekommenderar EY att kommunstyrelsen i Västerås stad tillser att:

- ▶ En plan upprättas för kontinuerlig uppdatering och kommunikation av styrande dokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.
- ▶ En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.
- ▶ En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Innehållsförteckning

Sammanfattning	2
Innehållsförteckning	3
1 Bakgrund	1
1.1 Syfte och revisionsfrågor	1
1.2 Avgränsning	1
1.3 Revisionskriterier	2
1.4 Metod och genomförande	2
2 Analys	5
2.1 Styrning	7
2.2 Personal och behörigheter	9
2.3 Drift	10
2.4 Programförändringar	12
2.5 Personuppgifter	13
3 Övergripande rekommendationer	16
4 Revisionsfrågor	17
5 Slutsatser	19
Bilaga 1: Källförteckning	20
Bilaga 2: Definitioner	22

1 Bakgrund

Västerås stad och dess nämnder hanterar stora mängder digital information. Detta ger många nya möjligheter i form av effektivare förvaltning, uppföljning och utökad service till medborgare, samtidigt som risker uppstår när informationen inte hanteras ändamålsenligt. För att uppnå god informationssäkerhet krävs att styrning och arbete bedrivs på ett sådant sätt att informationen är tillgänglig, riktig samt har tillräckligt starkt skydd.

Under 2020 genomfördes en granskning av följsamheten till dataskyddsförordningen GDPR inom staden, där ett antal väsentliga noteringar gjordes. Sedan dess har den generella hotbilden både inom IT i allmänhet och mot offentliga institutioner i synnerhet ökat. Med utgångspunkt i sin årliga riskanalys 2022 har stadens förtroendevalda revisorer identifierat risker relaterat till kommunens övergripande arbete med informationssäkerhet samt IT-risker.

1.1 Syfte och revisionsfrågor

Granskningens syfte är att bedöma om kommunens interna kontroll avseende IT- och informationssäkerhet är tillräcklig. Vidare är syftet också att bedöma i vilken omfattning styrelse och nämnder styr och följer upp arbetet på området. För att uppnå granskningens syfte besvaras följande frågor:

- ▶ Bedriver Västerås stad ett tillräckligt och ändamålsenligt IT- och informationssäkerhetsarbete?
 - ▶ Kan *styrningen* av arbetet med IT- och informationssäkerhet, för de behov kommunens verksamhet har, bedömas som ändamålsenligt?
 - ▶ Är arbetet med att *följa upp* att beslut och styrdokument relaterat till informationssäkerhet efterlevs ändamålsenligt?
 - ▶ Är Västerås stads *incidenthanteringsprocess* ändamålsenlig?
 - ▶ Har tillräckliga åtgärder vidtagits av staden med anledning av de rekommendationer som revisionen lämnade vid sin granskning av stadens arbete med GDPR?

1.2 Avgränsning

Granskningen är avgränsad till att ge en övergripande bild av stadens arbete när det gäller IT- och informationssäkerhetsarbetet. Härutöver inkluderar granskningen en uppföljning av den GDPR-granskning som genomfördes av revisorerna 2020. Granskningen omfattar kommunens samtliga nämnder, med kommunstyrelsen som ansvarig nämnd. De kommunala bolagen ingår inte i granskningen.

Granskningen innebär inte att några stickprov, penetrationstester eller dylikt av IT-system genomförs.

1.3 Revisionskriterier

- ▶ Myndigheten för samhällsskydd och beredskaps (MSBs) ramverk ledningssystem för informationssäkerhet (LIS), som är ett etablerat ramverk i ett stort antal kommuner och inom offentlig förvaltning. Ramverket bygger på den svenska och internationella standarden för informationssäkerhet, ISO/IEC 27000.
- ▶ Kommunallagen
- ▶ Stadens gällande och relevanta styrdokument inom IT- och informationssäkerhet

1.4 Metod och genomförande

Granskningen har byggts på EY:s ramverk för granskning av IT- och informationssäkerhet, särskilt framtagen för svensk kommunal sektor. Ramverket omfattar flera områden vilka täcker in de domäner som är väsentliga utifrån ett internkontrollperspektiv för att bedöma eventuella avvikelser och risker kopplat till brister i IT- och informationssäkerhet.

Inledningsvis har relevant dokumentation kring kommunens rutiner och processer granskats av EY. Därefter har granskningsmöten hållits med kommunens representanter för att gå igenom de områden som är inkluderade i EY:s ramverk för granskning av IT- och informationssäkerhet i kommuner. Under granskningen har dock inga stickprovstester utförts, vilket innebär att själva efterlevnaden av kommunens rutiner och kontroller inte har testats. Slutligen har den samlade bilden av dokumentation samt information inhämtad via granskningsmöten analyserats och bedömts.

Under granskningen har följande roller intervjuats:

- ▶ Verksamhetschef
- ▶ Tillförordnad projektledare inom digitalisering
- ▶ Informationssäkerhetsstrateg
- ▶ Säkerhetschef
- ▶ Dataskyddsombud

De intervjuade personerna har givits möjlighet att sakgranska rapporten i syfte att säkerställa att slutsatser grundar sig i korrekt fakta.

Fullständig källförteckning framgår av bilaga 1.

Under uppdraget har EY granskat 5 huvudområden som brutits ner på 18 underområden enligt nedan.

Styrning

- Ledningssystem
- Policy
- Strategi och rutiner
- Organisation

Personal och behörigheter

- Personal
- Behörighetshantering

Drift

- Incidenthantering
- Informationsklassning
- Nätverk
- Brandväggar
- Kontinuitetsplanering

Programförändringar

- Förändringshantering

Personuppgifter

- Personuppgiftsstyrning
- Personuppgiftsbehandling
- Personuppgiftsrutiner
- Dataskydd
- Utbildning inom dataskyddsförordningen
- Molntjänster

Under granskningen har EY gjort en sammanfattande betygsättning på samtliga 18 underområden på en skala 1-5. Skalans definition presenteras nedan:

Tabell 1: Skala för bedömning av Västerås stadsmognadsgrad inom informationssäkerhetsområden

1	Det finns ingen dokumentation eller uppföljning, händelser hanteras ad hoc
2	Viss grundläggande dokumentation finns, men denna kan variera mellan olika enheter och vara bristfällig i sin omfattning och tillämpning
3	Det finns dokumenterade processer och dessa tillämpas i stor mån genom hela organisationen
4	Förutom väldokumenterade processer som tillämpas i hela organisationen, finns det dessutom ett system för uppföljning
5	Baserat på uppföljningen finns också rutiner för kontinuerlig förbättring och uppdatering av processer och ramverk

Ett områdes färgkod visar en genomsnittlig mognadsgrad som beräknas över alla krav som ingår i området. Mognadsgraden per område indikerar vilka områden som har störst förbättringsbehov, men på grund av genomsnittsberäkningen kan till exempel ett område med grön färgkod ändå sakna viktiga delar. Granskningens huvudsakliga värde ligger i dess observationer och rekommendationer som beskrivs i en bredare kontext i själva granskningsrapporten.

Tidsplanen för arbetet såg ut enligt följande:

Tabell 2: Tidsplan för IT- och informationssäkerhetsgranskningen

Förberedelser och planering	September 2022
Insamling och analys av dokumentation	Oktober 2022
Arbetsmöte	Oktober 2022
Rapportskrivning samt intern kvalitetssäkring	Oktober 2022
Faktagranskning av kommunen	November 2022
Justering samt färdigställande av rapport	November 2022
Avrapportering och slutpresentation	Januari 2023

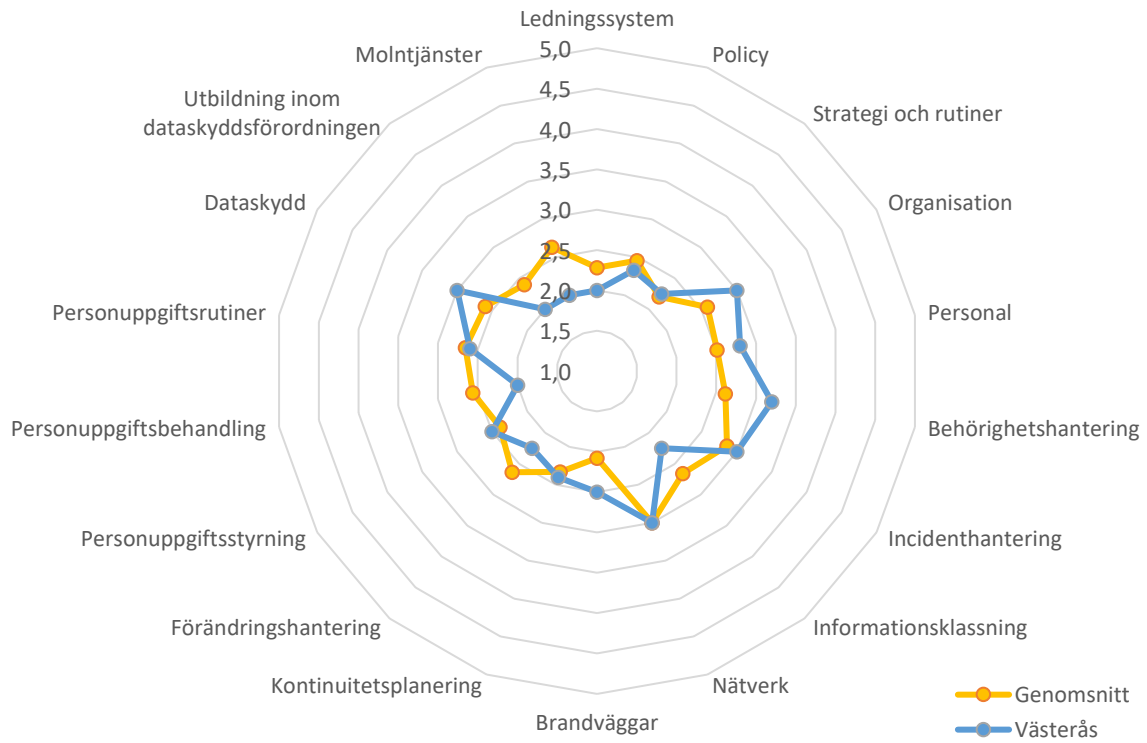
2 Analys

Baserat på den analys och granskning som genomförts bedöms Västerås stad ha en genomsnittlig mognadsgrad på 2,50 vilket är något lägre än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Givet den stora mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras inom Västerås stad är mognadsgraden, trots att den är nära genomsnittet, lägre än vad EY rekommenderar för en kommun likt Västerås stad. Granskningsresultatet indikerar att kommunens mognadsgrad är högst inom området personal och behörigheter. Kommunens lägsta mognadsgrad är inom området programförändringar.

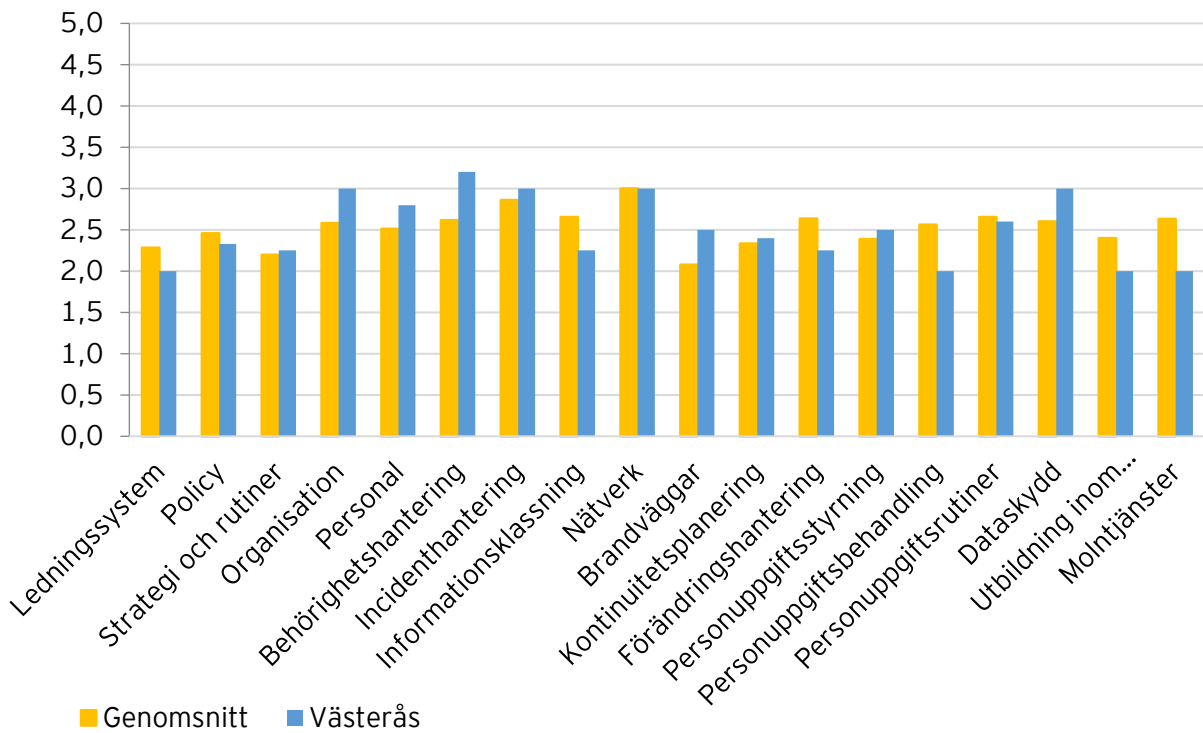
Västerås stad arbetar aktivt för att utveckla arbetet med informationssäkerhet. Bland annat bedrivs arbete för att uppdatera informationssäkerhetspolicyn. Mål om att expandera interna IT-säkerhetsutbildningar till medarbetare och nyanställa, samt att tydligare definiera dataskyddsombudens arbetsuppgifter utåt.

Kommunens främsta förbättringsbehov gäller upprättandet av en heltäckande internkontroll för IT- och informationssäkerhetsområdet. Behov för förbättring har även identifierats gällande kommunikation av policy och riktlinjer avseende IT- och informationssäkerhet, samt att upprätta en process för utbildning av informationssäkerhet för kommunens verksamhet.

Figur 1 nedan redovisar kommunens mognadsgrad för de 5 huvudområden som granskats samt en jämförelse med andra kommuner av motsvarande storlek och karaktär. Figur 2 visar detsamma fast nedbrutet på 18 underområden. Genomsnittet för andra offentliga organisationer av motsvarande storlek och karaktär är framtaget genom att bedöma mognadsgrad för samma områden och enligt samma metod som för Västerås stad.



Figur 1: Överblick över kommunens mognadsgrad för de 5 huvudområden som granskats i relation till vad EY generellt observerar i offentlig verksamhet av motsvarande storlek och karaktär.



Figur 2: Överblick över kommunens mognadsgrad för de 18 underområden i relation till vad EY generellt observerar i offentlig verksamhet av motsvarande storlek och karaktär.

2.1 Styrning

I sektionen nedan beskrivs nulägesbilden för huvudområdet *styrning* samt de iakttagelser som noterats under granskningens utförande (se Tabell 3).

Tabell 3: Nuläge och iakttagelser inom huvudområdet Styrning

Område	Nuläge	Iakttagelser	Mognad
Lednings-system	<p>Västerås stad har enligt styrande dokument inte etablerat ett Ledningssystem för informationssäkerhet (LIS) baserat på ISO/IEC 27001, Ledningssystem för informationssäkerhet.</p> <p>Kommunen har arbetat fram <i>riktlinjer för informationssäkerhet</i> baserat på ISO/IEC 27000 etablerat 2019 och arbetar med en <i>Handlingsplan för Ledningssystem för informationssäkerhet i Västerås stad</i> enligt given standard.</p>	Kommunen har inte ett uppdaterat och helt fungerande Ledningssystem för informationssäkerhet (LIS).	2,00
Policy	<p>Västerås stads arbete med informationssäkerhet beskrivs på en övergripande nivå i den nuvarande <i>informationssäkerhetspolicyn</i> upprättad 2011. I policyn fastställs Västerås stads syn på informationssäkerhet samt övergripande mål och roller. Informationssäkerhetspolicyn fungerar således som det överordnade och styrande dokumentet.</p> <p>Policyn beskriver kortfattat ansvarskrav avseende informationssäkerhet på olika roller inom kommunen, däribland <i>objektansvariga</i>, <i>stadsledningskontoret</i> och <i>informationsägarna</i>. Policyns övergripande mål är bland annat att leva upp till krav från användare av kommunens tjänster, förhålla sig till lagar och säkerställa godkända interna rutiner.</p> <p>Enligt policyn ska chefer på alla nivåer aktivt verka för kännedom hos medarbetare. Anställda hänvisas till policy och riktlinjer på intranätet. Vid upplärningsprocessen är det den nyanställdas ansvar att ta del av informationen i policy och riktlinjer. Att nyanställda ska ta del av policy och riktlinjer avseende IT- och informationssäkerhet finns dokumenterat i en särskild utbildningsprocess. Dock har processen ännu inte blivit implementerad då den vid tid för granskning planeras att lanseras inom kort.</p> <p>Vid tid för granskning bedrivs ett arbete inom kommunen att revidera <i>informationssäkerhetspolicyn</i>, med ett nuvarande utkast från 2022. Den reviderade policyn beslutas av kommunfullmäktige och utkastet innehåller i nuläget påbörjade tillägg såsom uppföljning.</p>	<p>Den gällande informationssäkerhetspolicyn är mer än 10 år gammal.</p> <p>Det saknas en dokumenterad process för hur det säkerställs att medarbetare kontinuerligt tar del av policy och riktlinjer avseende IT- och informationssäkerhet.</p> <p>En dokumenterad process för hur det säkerställs att nyanställda har tagit del av policy och riktlinjer avseende IT- och informationssäkerhet har ännu inte blivit implementerad.</p>	2,33

<p>Strategi och rutiner</p>	<p>Kommunens strategi avseende informationssäkerhet beskrivs i riktlinjerna. Riktlinjerna ska ses som ett minimumkrav för hantering av information, och de riktar sig till samtliga medarbetare inom kommunen.</p> <p>Det finns även dokumenterade riktlinjer för inköp och hantering av IT-relaterade produkter och tjänster inom kommunen. Riktlinjerna innefattar bland annat IT-säkerhet, styrning av IT samt målsättning med IT-arbetet. De nuvarande riktlinjerna avseende IT fastställdes under 2018 och är giltig tills 2021.</p> <p>Det saknas konkreta riktlinjer som beskriver vilka rutiner och säkerhetslösningar som behövs för att uppfylla de mål som beskrivs i informationssäkerhetspolicyn. Flertalet riktlinjer är äldre än 7 år.</p>	<p>Det saknas en definierad frekvens för hur ofta riktlinjer avseende informations-säkerhet ska granskas.</p>	<p>2,25</p>
<p>Organisation</p>	<p>Organisationen samt roll- och ansvarsfördelning för Västerås stad informationssäkerhetsarbete beskrivs i kommunens <i>informationssäkerhetspolicy</i> samt <i>riktlinjer för informationssäkerhet</i>.</p> <p>Informationssäkerhetspolicyn upprättas av kommunfullmäktige 2011. Det är denna policy som reglerar det övergripande arbetet med informationssäkerhet. I policyn beskrivs även de olika ansvarsområden inom detta arbete. I nuläget pågår även arbete om att uppdatera <i>informationssäkerhetspolicyn</i> och upprätta en mer detaljerad dokumentation över roller och ansvar inom informationssäkerhet hos kommunen.</p> <p>I den existerande policyn framgår det att årliga mål och ramar för informationssäkerhetsarbetet sätts upp i verksamhetsplaneringen.</p> <p>Ansvar för informationen är decentraliserad och ligger hos respektive verksamhet. Det finns rådgivning tillgängligt i stadsledningskontoret i form av informationssäkerhetsstrateg. Varje dataskyddsombud agerar också som stöd till verksamheten. Det finns i nuläget inte några formaliserade kontroller eller rutiner för Stadsledningskontoret att följa upp på arbetet med informationssäkerhet hos verksamheterna.</p> <p>Arbete på strategisk nivå inom informationssäkerhet ska ledas från stadsledningskontoret centralt. Informationssäkerhetsstrategen vid stadsledningskontoret har ansvaret för att samordna stadens arbete av informationssäkerhet. Beskrivning av informationssäkerhetsstrategens ansvar finns i <i>riktlinjer för informationssäkerhet</i>.</p>	<p>Styrdokumentet är till viss del utdaterade.</p> <p>Det saknas formaliserade kontroller och rutiner för Stadsledningskontoret att följa upp på arbetet med informationssäkerhet hos verksamheterna.</p>	<p>3,00</p>

	<p>Informationssäkerhetsstrateg arbetar som stöd för verksamheten i informationssäkerhetsfrågor. Mer operativa arbeten ska skötas av objektägaren/objektledaren samt dataskyddssamordnare. Vid verksamhetsviktig information utses en eller fler informationsägare. Beskrivning av informationsägarens ansvar finns i <i>riktlinjer för informationssäkerhet</i>.</p>		
--	---	--	--

2.2 Personal och behörigheter

I sektionen nedan beskrivs nulägesbilden för respektive område inom huvudområdet *personal och behörigheter* samt de iakttagelser som noterats under granskningens utförande (se Tabell 4).

Tabell 4: Nuläge och iakttagelser inom huvudområdet *Personal och behörigheter*

Område	Nuläge	Iakttagelser	Mognad
Personal	<p>Grundläggande informationssäkerhetsutbildning, kallat Nano-Learning, erbjuds för alla terminsvis - en på våren och en under hösten. De digitala utbildningarna är inte obligatoriska. För objektledare delas även information under nätverksträffar.</p> <p>Det finns en Nano-Learning för nyanställda, den är i nuläget inte obligatorisk men är planerad att bli det i framtiden. Vid nyanställning ansvar anställande chef för att den nyanställde tar del av utbildningen kring informationssäkerhet. Det är även varje användares ansvar att ta del av utbildningar och regelverk kring informationssäkerhet under anställningen. För objektägare sker nätverksträffar för utbyte av information och uppdateringar kring säkerhet.</p> <p>Samtliga av kommunens IT-system en utsedd systemägare.</p> <p>Kommunen har en dokumenterad rutin avseende säkerhet vid rekrytering för personal i vanlig såväl säkerhetsklassade befattningar. I <i>riktlinjen för informationssäkerhet</i> och <i>Instruktion Basnivå Informationssäkerhet</i> framgår det att säkerhetsprövningen ska innehålla kontroll av identitet. Säkerhetsprövning kan även inkludera bakgrundskontroll för medarbetare. Enligt riktlinjen ska det vid inhyrning av extern personal för utförande av tjänster åt staden upprättas sekretessavtal.</p> <p>Kommunens informationssäkerhetsfunktion är något underbemannad med resurser. Det dels på grund av nuvarande vakanta poster på stadsledningskontoret.</p>	<p>Utbildning i informationssäkerhet är inte obligatoriskt.</p> <p>Det saknas obligatorisk utbildning i informationssäkerhet till nyanställda.</p>	2,80
Behörighets-hantering	Kommunen har en definierad process för behörighetshantering som är beskriven i kommunens		3,20

	<p><i>basnivå informationssäkerhet och riktlinje för informationssäkerhet.</i> Dokumenten är fastställda 2015 respektive 2019.</p> <p>Höga behörigheter ska inte tilldelas fler individer än nödvändigt, och samtliga höga behörigheter ska vara individuella behörigheter. Behörigheter med åtkomst till infrastruktur förekommer inte eftersom kommunen inte äger någon infrastruktur då detta hanteras av extern driftleverantör. Kommunen har i avtal ställt krav på leverantören att endast säkerhetsprövad personal får ha tillgång till infrastrukturen.</p> <p>Instruktioner för behörighetskontroll finns i <i>Instruktion åtkomst till system och nätverk</i>. Där finns även styrning av systemadministrativa behörigheter. Dokumentet är fastställt 2015.</p> <p>Genomgång av användarbehörigheter ska genomföras minst årligen, och det är objektledarens ansvar att göra detta. Genomgången ska inkludera en verifiering av att personerna i fråga har ett oförändrat åtkomstbehov. Behörigheter ska tas bort vid avslutad tjänst. Genomgång av behörigheter hanteras i samband med klassning av system, det finns i handlingsplanen en uppföljningsplan om att ta fram den typen av rutiner i objektsledningen.</p> <p>I de allra flesta system så skickas beställningar på roller/systembehörigheter i ett beställningsflöde till ansvarig chef, enligt anvisning på Insidan. Vid tid för granskning finns det ingen dokumenterad process för att säkerställa en lämplig segregering av roller och behörigheter inom både organisationen och informationssystemen.</p> <p>Kommunen har en lösenordspolicy. Det finns tre nivåer av lösenordsregler baserat på karaktären av kontot med ökande krav av svårighetsgrad. Enligt de intervjuade nyckelpersonerna lever dessa lösenordsinställningar upp till kraven i lösenordspolicyn för samtliga system. Det är tjänsteansvarig för IT-infrastrukturen som ansvarar för lösenordspolicyn och hanteringen av den.</p>	<p>Det saknas en dokumenterad process avseende att systemägare ska dokumentera genomförandet av periodisk genomgång av behörigheter.</p> <p>Kommunen saknar en dokumenterad process för att säkerställa segregering av roller och behörigheter inom organisation och system.</p> <p>Det finns ingen dokumenterad uppföljning på att lösenordspolicyn följs.</p>	
--	---	---	--

2.3 Drift

I sektionen nedan beskrivs nulägesbilden för respektive område inom huvudområdet *drift* samt de iakttagelser som noterats under granskningens utförande (se Tabell 5).

Tabell 5: Nuläge och iakttagelser inom huvudområdet Drift

Område	Nuläge	Iakttagelser	Mognad
--------	--------	--------------	--------

<p>Incidenthantering</p>	<p>Enligt <i>riktlinjer för informationssäkerhet</i> ska säkerhetsincidenter som misstänks kunna påverka informationssäkerheten rapporteras till närmsta chef utan dröjsmål. Gäller det fel och/eller brister i systemet ska dessa även rapporteras till objektägaren. IT- och informationssäkerhetsincidenter rapporteras genom att fylla i en standardiserad mall.</p> <p>Hantering av säkerhetsincidenter beskrivs i <i>Instruktion för säkerhetsincidenthantering</i>. Dokumentet beskriver ansvar och roller mellan staden och IT-leverantören, principer för prioritering, med mera. Instruktionen saknar dock en beskrivning för hur säkerhetsincidenter ska följas upp på aggregerad nivå, vilket kan försvåra för staden att kontinuerligt förbättra såväl processen, som den faktiska hanteringen. Enligt intervjuade personer följs incidenter upp i <i>säkerhetsforum</i> tillsammans med leverantören.</p> <p>Säkerhetsincidenter loggas alltid. Mindre ärenden, som inte ses som incidenter, loggas som ärenden.</p>	<p>Incidenthanteringsprocessen beskriver inte hur uppföljning av incidenter på aggregerad nivå ska ske.</p>	<p>3,00</p>
<p>Informationsklassning</p>	<p>Västerås stad använder en modell för klassificering som bygger på Myndigheten för Samhällsskydd och beredskaps (MSB) och SKL:s rekommendationer som i sin tur utgår ifrån ISO/IEC 27000-standard för informationssäkerhet.</p> <p>Västerås informationshantering styrs till stor del av bestämmelser i Tryckfrihetsförordning (1949:105) och Offentlighets- och sekretesslag (OSL) 2009:400. Vidare hanteras en stor del information som lyder under Personuppgiftslagen (PuL) 1998:204.</p>	<p>Västerås stad hänvisar fortfarande till stor del till PuL.</p>	<p>2,25</p>
<p>Nätverk</p>	<p>Kommunen har ett dokument som beskriver nätverksdesign. Dokumentet innefattar bland annat nätverks säkerhet, brandväggsadministration och nätverkssegmentering. Det beskrivs även hur nätverkstrafik ska styras. Dokumentet är upprättat av IT-direktör 2014.</p> <p>Kommunen har implementerat Intrusion Prevention System (IPS) och Intrusion Detection System (IDS) för att analysera nätverksaktivitet.</p>	<p>Nätverksdokumentationen är gammal och bör revideras.</p>	<p>3,00</p>
<p>Brandväggar</p>	<p>Västerås stad har ett brandväggsråd som ska sammanträda varje vecka. Brandväggsrådet hanterar externa och interna brandväggar och brandvägsregler på servrar och klienter.</p> <p>Det finns upprättade rutiner och instruktioner för hur ändringar i brandväggar ska göras och varje ändring granskas och godkänns innan förändringen genomförs. Ingen dokumenterad brandväggspolicy för att styra underhåll och dokumentation av brandväggsrelaterade aktiviteter finns.</p>	<p>Det finns ingen upprättad brandväggspolicy, -instruktion eller liknande.</p>	<p>2,50</p>

	<p>Enligt rutin för ansökan om portöppning ska ansökan beställas av objektledare och följa en förutbestämd mall med information. En godkänd portöppningsansökan signeras av ordförande för brandväggsrådet.</p> <p>Ingen dokumenterad granskning av brandväggsskyddet finns.</p>	Brandväggarnas funktion och konfiguration granskas inte.	
Kontinuitetsplanering	<p>Kontinuitetsplanering beskrivs övergripande i <i>riktlinje för informationssäkerhet</i> och inkluderar vad en kontinuitetsplan i verksamheten ska omfatta. Verksamhetsansvarig chef ansvarar för att det finns en kontinuitetsplan dokumenterad. Det kan förekomma små, eller nyligen produktionssatta, system utan kontinuitetsplan.</p> <p>Det finns en kundkontinuitetsplan där det finns definierat vad en katastrof och kris innebär för Västerås stad. Den är en bilaga i avtal, och det regleras där. Det finns rutiner för att testa stadens känsligare system i driftpartnerns årshjul, där bl.a. återläsningstest genomförs. Kontinuitetsplanerna följs inte upp och testas inte på regelbunden basis.</p>	Det saknas en rutin för att följa upp och testa kontinuitetsplaner.	2,40

2.4 Programförändringar

I sektionen nedan beskrivs nulägesbilden för respektive område inom huvudområdet *programförändringar* samt de iakttagelser som noterats under granskningens utförande (se Tabell 6).

Tabell 6: Nuläge och iakttagelser inom huvudområdet Programförändringar

Område	Nuläge	Iakttagelser	Mognad
Förändringshantering	<p>Rutiner för förändringshantering ska finnas etablerade inom systemets förvaltningsorganisation, och vara framtagen i samråd med IT-driftleverantör.</p> <p>Respektive systemägare ansvarar för att hålla systemet uppdaterat. Därtill ligger ansvaret hos systemförvaltaren att det ska finnas en förvaltningsplan för systemet.</p> <p>Enligt instruktion ska alla ändringar av programvara vara formellt godkända innan den installeras i utbildnings-, acceptanstest- eller produktionsmiljö. Det ska även finnas ett testprotokoll som är undertecknat av styrgrupp eller motsvarande. Alla program har inte testmiljöer.</p> <p>Samtliga ändringar ska vara spårbara och de ska kunna härledas till en ansvarig beställare. Övervakningsrutiner för driftmiljöer som säkerställer att inga programförändringar införs som inte är godkända ska vara implementerade.</p>	För vissa system testas förändringar direkt i produktionsmiljön.	2,25

	<p>Ändringar i driftmiljön i system som utbyter information med andra system (integrationer) ska följa stadens riktlinjer för systemintegration.</p> <p>Avtalet mellan kommunen och den externa driftleverantören ska beskriva en tydlig process för förändringshantering som inkluderar att samtliga förändringar protokollförs.</p> <p>En 'Patch Tuesday' äger rum en gång i månaden för att få in mindre uppdateringar enligt ett regelbundet schema.</p>		
--	--	--	--

2.5 Personuppgifter

I sektionen nedan beskrivs nulägesbilden för respektive område inom huvudområdet *personuppgifter* samt de iakttagelser som noterats under granskningens utförande (se Tabell 7).

Tabell 7: Nuläge och iakttagelser inom huvudområdet Personuppgifter

Område	Nuläge	Iakttagelser	Mognad
Personuppgifts-styrning	<p>Västerås stads riktlinjer innefattar bland annat att personuppgifter endast får samlas in för berättigade ändamål samt att personuppgifter inte får sparas längre än nödvändigt.</p> <p>Det finns ett dokument för konsekvensbedömning (DIPA), för personuppgiftsbehandling.</p> <p>Det finns en dokumenterad process för registerutdrag där det framgår hur kommunen ska hantera en begäran.</p> <p>Granskning av dataskyddsarbetet sker framför allt på verksamhetsnivå där de besvarar ett antal kontrollfrågor utformat av dataskyddsorganisationen som sedan DSO sammanställer, analyserar och använder för att ge råd för det fortsatta arbetet med GDPR. Dataskyddsombuden sätter ihop en granskningsrapport som återrapporteras till nämnderna.</p> <p>Ingen efterlevnadsutvärdering görs på förvaltningarna.</p> <p>I riktlinje för dataskyddsarbetet finns mycket information för verksamheterna kring dataskyddsombuden, mindre information kring arbetet som utförs. En ny version håller på att tas fram, med ett delsyfte att förbättra detta.</p>	<p>Västerås stad har ett flertal dokument upprättade före 2018 som refererar till PuL i samband med personuppgifter.</p> <p>Kommunen har ej säkerställt att styrande dokument avseende GDPR förblir riktiga och aktuella över tid.</p> <p>Uppföljning förlitar till stor del på självutvärdering i verksamheterna.</p> <p>Riktlinje för dataskyddsarbete fokuserar lite på hur personuppgifter faktiskt ska hanteras.</p>	2,50

<p>Personuppgifts- behandling</p>	<p>Kommunstyrelsen och varje nämnd har eget ansvar för att de personuppgifter som behandlas i deras verksamhet sker lagligt och korrekt enligt centrala riktlinjer.</p> <p>Kommunens registerförteckning innefattar cirka 65 personuppgiftsbehandlingar. Vissa ändamål i kommunstyrelsens registerförteckning saknar uttalad rättslig grund.</p> <p>Det saknas även fullständiga registerförteckningar hos vissa nämnder.</p> <p>Kommunen upprättar PuB-avtal med leverantörer som hanterar kommunens personuppgifter enligt SKR-avtalsmall. Avtalen innefattar bl.a. ansvar, säkerhetsåtgärder och sekretess.</p>	<p>Registerförteckningen är inte fullständig och korrekt för alla delar i Västerås stad.</p>	<p>2,00</p>
<p>Personuppgifts- rutiner</p>	<p>Kommunen har dokumenterade instruktioner för personuppgiftsincidenter. Medarbetare ska vid osäkerhet kontakta och samråda med dataskyddsombud på stadsledningskontoret. Personuppgiftsincidenter loggförs för att hålla koll på antalet incidenter som uppstår.</p> <p>Dataskyddssamordnare inom verksamheterna ansvarar för samordning och agerar kontaktperson mot dataskyddsombuden på stadsledningskontoret.</p> <p>Gallringsplaner ligger hos respektive verksamhet.</p> <p>Västerås stad har ett fastställt dokument för hantering av skyddade personuppgifter.</p>	<p>Krav på gallring saknas centralt.</p>	<p>2,60</p>
<p>Dataskydd</p>	<p>För att etablera ett allmänt dataskydd inom kommunen har åtgärder vidtagits i form av riktlinjer för IT-stöd. I <i>Instruktion Basnivå IT-säkerhet</i> finns specifika instruktioner gällande planering och godkännande av IT-stöd, åtgärder mot skadlig kod och säkerhetsuppdateringar. Instruktionen är fastställd 2015.</p> <p>Kommunstyrelsen och varje nämnd besitter eget ansvar över de personuppgifter de hanterar. Dataskyddsombuden hjälper till med stöd till verksamheterna samt leder och samordnar dataskyddarbetet i Västerås stad.</p>	<p>Instruktioner för IT-säkerhet revideras ej med fastställda intervaller.</p> <p>Genom att både implementera och granska dataskydd riskerar DSO att granska sitt eget arbete.</p>	<p>3,00</p>
<p>Utbildning inom dataskydds-förordningen</p>	<p>GDPR-utbildningar utförs genom Nano-Learning, vilket innebär regelbundna korta internetutbildningar. Utbildning ges till samtliga medarbetare terminsvis. Utbildningarna följs ej upp med avseende på deltagande. Det är verksamhetschefernas ansvar att se till att samtliga anställda inom verksamheten har genomfört utbildningarna.</p>	<p>Västerås stad följer inte upp vilka medarbetare som deltar i Nano-Learnings.</p>	<p>2,00</p>

	Underlag finns från dataskyddsutbildning på stadsledningskontoret där ansvar och krav går igenom. Dessa utbildningar ansvaras för, och leds av dataskyddsombudet.		
Molntjänster	<p>Kommunen hanterar personuppgifter i molntjänster. En särskild säkerhetsanalys ska göras för anslutningar via molntjänster.</p> <p>Enligt <i>Instruktion anskaffning av IT stöd</i> ska anskaffning av molntjänster följa samma procedur som vid outsourcing till extern leverantör. Det finns ett kravbibliotek för staden där krav kan väljas i de fall som ett införande ska ligga i molnet. Dokumentationen hänvisar till lathund av Myndigheten för Samhällsberedskap (MSB) för stöd vid anskaffning.</p> <p>Tekniska krav på molntjänstleverantörer framgår inte.</p>	<p>Västerås stad har ingen sammanställd riktlinje specifikt för molntjänster</p> <p>Det finns ingen teknisk kravspecifikation på molntjänster.</p>	2,00

3 Övergripande rekommendationer

Granskningen har identifierat iakttagelser inom flera delar av ramverket. EY har valt att presentera de mest relevanta rekommendationerna för Västerås stad och förslag på åtgärder för de främsta riskerna inom IT- och informationssäkerhetsarbetet.

Revision av styrdokument och riktlinjer

Riktlinjer och styrdokument avseende informationssäkerhet saknar vid tid för granskning en definierad frekvens för hur ofta de ska revideras. Kommunstyrelsen rekommenderas tillse att riktlinjer avseende IT- och informationssäkerhet revideras kontinuerligt utefter ett förutbestämt tidsintervall för att säkerställa att riktlinjer förbli riktiga och aktuella över tid. Kommunstyrelsen rekommenderas även tillse att granskning av riktlinjer dokumenteras även i de fall ingen förändring av dokumenten utförs.

Kommunikationsplan

Kommunikation av policy och riktlinjer sker i praktiken enligt flertalet metoder som inte är dokumenterade. Kommunstyrelsen rekommenderas tillse att en dokumenterad kommunikationsplan för policy och riktlinjer avseende IT- och informationssäkerhet upprättas. Kommunikationsplanen bör indikera vem som ansvarar för att kommunicera policy och riktlinjer till medarbetare inom kommunen samt på vilket sätt detta ska göras.

Utbildningsplan

Utbildning för informationssäkerhet på generell nivå saknar dokumenterad utbildningsplan och systematisk uppföljning av utbildningarnas genomförande. Kommunstyrelsen rekommenderas att ta fram en dokumenterad utbildningsplan för såväl långvariga medarbetare som nyanställda och säkerställa att genomförandet av utbildningar bland medarbetare kontinuerligt följs upp. Dessutom rekommenderas en undersökning av kunskapsbehoven hos medarbetare och därefter anpassade utbildningsinsatser.

Internkontrollplan, samt uppföljning och efterlevnad

Dataskyddsombud sammanställer vartannat år självutvärderingar hos förvaltningar gällande dataskyddsförordningen. Det saknas dock formaliserade kontroller och rutiner för Stadsledningskontoret att följa upp på arbetet med informationssäkerhet som helhet i Västerås stads nämnder och förvaltningar. Kommunstyrelsen rekommenderas tillse att en internkontrollplan avseende IT- och informationssäkerhet upprättas som är heltäckande för de olika områdena inom kommunens IT- och informationssäkerhetsarbete. Genom en heltäckande internkontrollplan kan kommunstyrelsen kontrollera efterlevnad av policy och riktlinjer avseende IT- och informationssäkerhet samt upptäcka eventuella gap.

4 Revisionsfrågor

Granskningen har utgått från revisionsfrågan: bedriver Västerås stad ett tillräckligt och ändamålsenligt IT- och informationssäkerhetsarbete? Revisionsfrågan har brutits ner och besvarats enligt nedan.

Tabell 8: Förklaring av färgkod

Färgkod	Förklaring
	Revisionsfråga besvaras ej tillfredsställande
	Revisionsfråga besvaras delvis tillfredsställande
	Revisionsfråga besvaras tillfredsställande

Tabell 9: Svar på revisionsfrågor

Revisionsfråga	Svar
<p>► Kan styrningen av arbetet med IT- och informationssäkerhet, för de behov kommunens verksamheter har, bedömas som ändamålsenligt?</p>	<p>Styrningen av kommunens arbete med IT- och informationssäkerhet bedöms vara delvis ändamålsenlig.</p> <p>Svaret grundar sig i att kommunen har flertalet upprättade styrdokument för att styra och organisera IT- och informationssäkerhetsarbetet. Det finns en informationssäkerhetspolicy samt riktlinjer som beskriver flera områden inom IT- och informationssäkerhet. Dock saknas det en definierad frekvens för hur ofta riktlinjer ska uppdateras - vilket kan leda till att riktlinjer inte förbli riktiga och aktuella över tid. Vidare saknas en dokumenterad process för att kontinuerligt säkerställa att anställda har tagit del av och har kännedom om policy och riktlinjer avseende IT- och informationssäkerhet.</p> <p>Kommunen har dokumenterade riktlinjer avseende personuppgiftshantering. Riktlinjer avseende hantering av personuppgifter och registrerades rättigheter enligt GDPR har däremot inte blivit uppdaterade sedan 2019. En del dokumentation refererar till PuL som upphörde att gälla 2018. Vidare saknas lokalt anpassade riktlinjer avseende GDPR för nämnder/verksamheter inom kommunen.</p>

<p>▶ Är arbetet med att <i>följa upp</i> att beslut och styrdokument relaterat till informationssäkerhet efterlevs ändamålsenligt?</p>	<p>Uppföljningen av efterlevnad av kommunens arbete med IT- och informationssäkerhet bedöms vara delvis ändamålsenlig.</p> <p>Svaret grundar sig i att det genomförs riskanalys årligen av system som hanterar personuppgifter eller verksamhetsinformation. Det genomförs även en årsvis utvärdering av GDPR-arbetet för att kontrollera hur kommunen efterlever GDPR.</p> <p>Uppföljningsarbetet bedöms inte vara fullständigt ändamålsenligt då det saknas en dokumenterad process för att säkerställa att det sker kontroll eller uppföljning av samtliga områden inom kommunens IT- och informationssäkerhetsarbete samt att deltagande på utbildningar inom informationssäkerhet inte följs upp.</p>	
<p>▶ Är Västerås stads <i>incidenthanteringsprocess</i> ändamålsenlig?</p>	<p>Kommunens incidenthanteringsprocess bedöms vara delvis ändamålsenlig.</p> <p>Svaret grundar sig i att kommunen har en dokumenterad process för IT- och informationssäkerhetsincidenter, samt ett formulär för att anmäla dessa incidenter. Kommunen har även en separat process samt formulär för anmälan av personuppgiftsincidenter.</p> <p>Incidenthanteringsprocessen beskriver dock inte hur staden systematiskt ska följa upp incidenter för att kunna förbättra såväl incidenthanteringen sig samt själva processen.</p>	
<p>▶ Har tillräckliga åtgärder vidtagits av staden med anledning av de rekommendationer som revisionen lämnade vid sin granskning av stadens arbete med GDPR?</p>	<p>Åtgärderna av stadens arbete med GDPR bedöms vara delvis ändamålsenlig.</p> <p>Svaret grundar sig i att kommunen har tillfört viss dokumentation för hantering av personuppgifter utifrån GDPR. Dock så finns gamla dokument utan hänvisning till GDPR som inte har reviderats sedan innan dataskyddsförordningen trädde i kraft 2018.</p>	

5 Slutsatser

Granskningens syfte har varit att bedöma om det finns brister i kommunens interna kontroll avseende informationssäkerheten. Vidare har syftet också varit att bedöma i vilken omfattning kommunstyrelse och nämnder styr och följer upp detta arbete.


Baserat på den analys och granskning som genomförts bedöms Västerås stad ha en genomsnittlig mognadsgrad på 2,50 vilket är något lägre än andra offentliga organisationer av liknande storlek och karaktär där genomsnittet ligger på 2,52. Givet den stora mängd personuppgifter och andel personuppgifter av känslig karaktär som hanteras inom Västerås stad är mognadsgraden, trots att den är nära genomsnittet, lägre än vad EY rekommenderar för en kommun likt Västerås stad.

EY:s övergripande bedömning är att Västerås stad arbete med IT- och informationssäkerhet är delvis ändamålsenligt. Bedömningen grundar sig i att kommunen har en väldefinierad organisation och ändamålsenliga styrdokument avseende IT- och informationssäkerhet på plats. Däremot saknas vissa formaliserade processer avseende kontinuerlig kommunikation och revision av styrande dokument. Bedömningen grundar sig även i att det saknas en formaliserad process för att säkerställa att samtliga medarbetare genomför relevant utbildning inom informationssäkerhet.

Med grund i ovan är EY:s främsta rekommendationer att kommunstyrelsen i Västerås stad tillser att:

- ▶ En plan upprättas för kontinuerlig uppdatering och kommunikation av styrdokument till anställda inom kommunen, i syfte att säkerställa en god kännedom om kommunens IT- och informationssäkerhetsarbete.
- ▶ En dokumenterad utbildningsplan inom informationssäkerhet upprättas för samtliga medarbetare.
- ▶ En internkontrollplan avseende IT- och informationssäkerhet upprättas som täcker samtliga områden inom kommunens IT- och informationssäkerhetsarbete.

Stockholm 2022-12-13



Helena Törnqvist, Partner

Bilaga 1: Källförteckning

Intervjuade roller:

- ▶ Verksamhetschef
- ▶ Tillförordnad projektledare inom digitalisering
- ▶ Informationssäkerhetsstrateg
- ▶ Säkerhetschef
- ▶ Dataskyddsombud

Dokumentförteckning:

- ▶ 150129_Instruktion logghantering och spårbarhet v 1_0
- ▶ 150319_Instruktion Basnivå Informationssäkerhet v 1_0
- ▶ 150417_Instruktion Anskaffning utv och under av is v 1_0
- ▶ 150417_Instruktion Åtkomst till system och nätverk v 1_0
- ▶ 150518 Instruktion Basnivå IT-säkerhet v 1_0
- ▶ 160309 Instruktion Skyddade personuppgifter v 1_0 Dnr 2016_169_KS_009
- ▶ Begäran om registerutdrag - ifyllnadsbar PDF
- ▶ Bilaga 1, bekräftelsebrev registerutdrag (1)
- ▶ Bilaga 1, Checklista vid utredning av personuppgiftsincident
- ▶ Bilaga 2, Rapport - Dataskyddsombudets omedelbar bedömning
- ▶ Bilaga 2, registerutdrag
- ▶ Bilaga 3, Ordförandebeslut - Beslut om anmälan till integritetsskyddsmyndigheten
- ▶ Bilaga 4, Beskrivning av personuppgiftsincident
- ▶ Dataskydd - Västerås stad Intranät
- ▶ Digitaliseringsenhetens styrande dokument
- ▶ DPIA - Konsekvensbedömning - mall (1)
- ▶ Handlingsplan för digital förnyelse-2019
- ▶ Handlingsplan Ledningssystem för informationssäkerhet_2022
- ▶ Instruktion anskaffning av IT-stöd
- ▶ Instruktion för arbete med registerutdrag
- ▶ Instruktion för hantering utav personuppgifter i Västerås stad
- ▶ Instruktion för radering och rättelse (1)
- ▶ Kompletterande instruktion till PUB, version 3
- ▶ Lösenordsbyten - Västerås stad Intranät
- ▶ Målbild i avtalet om Säkerhetstjänster
- ▶ PUB-avtal, KS eller enskild nämnd som PUA, leverantör som PUB, version 2.0, slutversion mall
- ▶ Rapportmall
- ▶ Registerförteckning KS
- ▶ Riktlinje för dataskyddsarbetet i Västerås stad, version 2, 2020-09-08
- ▶ Riktlinje_för_digitala_verktyg_och_telefonitjänster_V2_fastställd
- ▶ Riktlinje för informationssäkerhet
- ▶ Riktlinje för utskriftstjänster 2021
- ▶ Riktlinjer för nätverksdesign
- ▶ Riktlinjer för systemintegration
- ▶ Rutin för ansökan om portöppning för Västerås stad till TietoEVERY 2022
- ▶ Rutiner för konsekvensbedömning (1)
- ▶ Roller i Västerås stads organisation för informationssäkerhet_utkast_220315
- ▶ Roller i Västerås stads organisation för informationssäkerhet_utkast_220325
- ▶ Samverkansavtal mellan leverantörer

- ▶ Stadsgemensam informationshanteringsplan version 2020 1.2
- ▶ Styrning och samverkan
- ▶ Styrning och samverkan 1.0
- ▶ Säkerhetskrav
- ▶ Tjänsteavtal - IT drift
- ▶ Tjänstebilaga Säkerhetstjänster
- ▶ Utbildning SK
- ▶ Utskick sökning registerutdrag
- ▶ Vägledning grundläggande kryptering för kommentarer
- ▶ Vägledning för fysisk säkerhet i IT-utrymmen

Bilaga 2: Definitioner

Change Advisory Board: En konstellation av IT- och verksamhetsrepresentanter som stödjer processen avseende förändringar genom att ge råd och fatta beslut.

Dataskyddsbud (DSO): Särskilt utsedd person vilken tillser att personuppgifter behandlas på korrekt och lagenligt sätt inom organisationen, genom att till exempel utföra kontroller och utbildningsinsatser.

Data Protection Impact Assessment (DIPA): En konsekvensbedömning som beskriver syftet med personuppgiftsbehandlingen och de risker som kan uppstå för personen vars uppgifter behandlas.

Informationsklassning: Klassning av informationstillgångar enligt i riktlinjer dokumenterade regler med avseende på informationens sekretess, riktighet, tillgänglighet och konfidentialitet.

Informationssäkerhet: Säkerhetsfrågor som berör information, oberoende av system och plattformar.

Informationssäkerhetssamordnare: Särskilt utsedd person som innehar det övergripande ansvaret att leda och samordna utvecklingen av kommunens informationssäkerhet.

Intrusion detection system (IDS): Ett verktyg som används för att upptäcka intrång eller intrångsförsök i ett datasystem.

Intrusion prevention system (IPS): Ett verktyg som används för att upptäcka och reagera intrång eller intrångsförsök i ett datasystem.

IT-säkerhet: Säkerhet som huvudsakligen relaterar till IT-infrastruktur, systemfrågor och konfigurerings.

ITIL V3: ITIL (Information Technology Infrastructure Library) är ett ramverk för att standardisera IT-relaterade aktiviteter. ITIL V3 är en version som även inkluderar strategiska element i syfte att IT bättre ska sammanvävas med verksamheten.

Kontinuitetsplanering: Planering och åtgärder med syfte att motverka avbrott i verksamheten och skydda kritiska verksamhetsprocesser mot konsekvenser av allvarliga fel i system eller katastrofer.

Ledningssystem: Definierat verktyg eller system för att leda, planera, kontrollera, följa upp och utvärdera den egna verksamhetens arbete med informationssäkerhet.

Molntjänster: Tjänster och system som inte drivs lokalt av kommunen och som nås via en internetuppkoppling och inte direkt via det lokala nätverket.

Nätverk: Ett nätverk administrerar koppling mellan olika resurser såsom olika program.

Patchning: Tillägg till ett program eller system avsett att rätta till sårbarheter.

Riskanalys: Redovisning av de samlade kraven på ett informationssystem avseende tillgänglighet, riktighet och sekretess. Systemsäkerhetsanalysen ska redogöra för vidtagna samt ytterligare nödvändiga säkerhetsåtgärder vilka är nödvändiga för att kraven på informationssystemet ska uppfyllas.

Server: En server är ett datorprogram som bidrar med funktionalitet till ett annat program via en nätverksuppkoppling.

Systemleverantör: Leverantör av IT-system som agerar supporterande vid incidenter med systemet och i vissa fall tillhandahåller drift av systemet. Leverantören tillhandahåller uppdateringar av systemversioner samt löpande rättningar av identifierade systemfel.



Objektägare: Verksamhetens chef eller särskilt utsedd person med ansvar för administration och drift av ett eller flera informationssystem inom ramen för antagna mål, vilken agerar ledningsfunktion över systemets förvaltning.