Enkäten om helhetsbilden av digital säkerhet

Tjänsten för helhetsbild av den digitala säkerheten är en tjänst som utvecklades och underhållas av Myndigheten för digitalisering och befolkningsdata med syftet att samla in uppgifter om läget av den digitala säkerheten hos organisationer i den offentliga förvaltningen.

Närmare information om tjänsten och hur man ansluter sig finns på https://dvv.fi/sv/publikationer-om-digital-sakerhet (se under rubriken Anvisningar).

Enkäten som kartlägger organisationens situation innehåller de följande påståenden om läget av den digitala säkerheten i administrativa sammanhang.

Svarmöjligheterna för alla påståenden är Ja – Dels – Nej – Kan inte tillämpas
Vissa påståenden har ytterligare information som hjälper med att svara.

Påstående nr	**1**
Delområde	**Ledning**
Beskrivning	Organisationens uppgifter och ansvar har identifierats och beskrivits tydligt.
Ytterligare information	

Påstående nr	**2**
Delområde	**Ledning**
Beskrivning	Organisationen har kartlagt den lagstiftning som styr dess digitala säkerhet och identifierat de skyldigheter den medför.
Ytterligare information	– Omfattar alla delområden inom digital säkerhet

---

Påstående nr	**3**
Delområde	**Ledning**
Beskrivning	Organisationen har kartlagt centrala intressent- och kundgrupper samt de krav på digital säkerhet som ställs på dem.
Ytterligare information	– lagstiftnings- och avtalsförpliktelser

---

Påstående nr	**4**
Delområde	**Ledning**
Beskrivning	Organisationen har tillräckligt med kompetent personal inom olika delområden inom den digitala säkerheten.
Ytterligare information	– Det finns tillräckligt med personer som ansvarar för digital säkerhet och de har tillräcklig kompetens

---

Påstående nr	**5**
Delområde	**Ledning**
Beskrivning	Organisationen har en tillräcklig budget för att upprätthålla och utveckla den digitala säkerheten.
Ytterligare information	

Påstående nr	**6**
Delområde	**Ledning**
Beskrivning	Organisationens ledning har förbundit sig att utveckla den digitala säkerheten.
Ytterligare information	– Organisationens ledning har kommunicerat och visat sig i tillräcklig utsträckning stödja förverkligandet och utvecklingen av digital säkerhet

Påstående nr	**7**
Delområde	**Ledning**
Beskrivning	Organisationens delområden inom digital säkerhet utvecklas systematiskt genom att utnyttja en eller flera tydliga processer eller hanteringsmodeller.
Ytterligare information	– t.ex. enligt ISO-standarder eller en annan allmän hanteringsmodell

Påstående nr	**8**
Delområde	**Ledning**
Beskrivning	Det finns tillräckliga anvisningar för personalen om digital säkerhet.
Ytterligare information	– bl.a. – principer för godtagbar användning och närmare anvisningar – anvisningar för behandling av informationsmaterial inklusive till exempel anvisningar om behandling av personuppgifter och sekretessbelagda uppgifter i olika tjänster – anvisningar om lokalernas informationssäkerhet – dataskyddsprinciper – Har anvisningarna och processerna förankrats och hur kan det påvisas?

Påstående nr	**9**
Delområde	**Ledning**
Beskrivning	Personalen ges regelbunden utbildning i digital säkerhet.
Ytterligare information	– Har den digitala säkerheten beaktats i personalens introduktion? – Har personalen regelbunden utbildning i digital säkerhet? – Har man beaktat särskilda behov i anslutning till olika roller och arbetsuppgifter – Upprätthåller man kompetensen regelbundet? – utbildningsplan – utbildnings- och introduktionsmaterial

Påstående nr	**10**
Delområde	**Ledning**
Beskrivning	Organisationen har en process för att reagera på missbruk.
Ytterligare information	– beskrivningar av process, ansvar och påföljder

Påstående nr	**11**
Delområde	**Ledning**
Beskrivning	Indikatorer för digital säkerhet har definierats.
Ytterligare information	– indikatorerna har definierats (utifrån målen) och data samlas in kontinuerligt

---

Påstående nr	**12**
Delområde	**Ledning**
Beskrivning	Den digitala säkerheten följs upp kontinuerligt.
Ytterligare information	– omfattar både administrativ och teknisk uppföljning

---

Påstående nr	**13**
Delområde	**Ledning**
Beskrivning	Organisationens ledning får regelbundna rapporter om helhetssituationen för den digitala säkerheten.
Ytterligare information	– minst en gång om året

Påstående nr	**14**
Delområde	**Riskhantering**
Beskrivning	Organisationen har riktlinjer, ansvar och processer för riskhantering som godkänts av ledningen och anpassats till verksamheten.
Ytterligare information	– riskhanteringspolicy eller motsvarande

---

Påstående nr	**15**
Delområde	**Riskhantering**
Beskrivning	Organisationen gör en regelbunden riskbedömning i anslutning till digital säkerhet där man beaktar nya fenomen, förändringar i verksamhetsmiljön och den egna verksamhetens inverkan på intressentgruppernas och kundernas situation.
Ytterligare information	– process och ansvar beskrivna och bevis på att processen fungerar

---

Påstående nr	**16**
Delområde	**Riskhantering**
Beskrivning	Organisationen informerar om den digitala säkerhetens risksituation och nya risker i hela organisationen.
Ytterligare information	– i samarbete mellan dem som ansvarar för digital säkerhet och kommunikation

---

Påstående nr	**17**
Delområde	**Riskhantering**
Beskrivning	Organisationen rapporterar regelbundet om risksituationer till ledningen.
Ytterligare information	– minst en gång om året

Påstående nr	**18**
Delområde	**Riskhantering**
Beskrivning	Ledningen får omedelbart rapporter om kritiska risker som hotar organisationens verksamhet.
Ytterligare information	– processen beskriven och bevis på att den fungerar

---

Påstående nr	**19**
Delområde	**Riskhantering**

Beskrivning	Organisationen följer regelbundet upp situationen beträffande riskerna och åtgärderna för att hantera dem.
Ytterligare information	– beskrivet förfarande och bevis på att det fungerar

---

Påstående nr	**20**
Delområde	**Riskhantering**
Beskrivning	Organisationen bedömer de resterande riskerna efter att riskhanteringsåtgärderna har genomförts och de resterande riskerna behandlas på relevant nivå.
Ytterligare information	– ledningen eller den som äger funktionen/risken fattar de beslut som behövs

---

Påstående nr	**21**
Delområde	**Riskhantering**
Beskrivning	Organisationen utvecklar riskhanteringsprocessen utifrån målen för riskhanteringen eller erfarenheter.
Ytterligare information	

Påstående nr	**22**
Delområde	**Verksamhetens kontinuitet och beredskap**
Beskrivning	Organisationens uppgifter och ansvar är tydliga även i undantagssituationer och undantagsförhållanden.
Ytterligare information	– beskrivs t.ex. i beredskapsplanen

Påstående nr	**23**
Delområde	**Verksamhetens kontinuitet och beredskap**
Beskrivning	Organisationen har en process och beredskap att snabbt och effektivt hantera störningar, hot och avvikelser i den digitala säkerheten.
Ytterligare information	– beskrivningar av process, ansvar och påföljder

---

Påstående nr	**24**
Delområde	**Verksamhetens kontinuitet och beredskap**
Beskrivning	Organisationen har beskrivit principerna, målen, organiseringen och ansvaret för kontinuitetshanteringen.
Ytterligare information	– principer för kontinuitetshantering eller motsvarande

---

Påstående nr	**25**
Delområde	**Verksamhetens kontinuitet och beredskap**
Beskrivning	Organisationen har identifierat och dokumenterat de objekt som ska skyddas.
Ytterligare information	– bl.a. personal, lokaler, datasystem, utrustning – De system, tjänster och anordningar (interna och externa) som organisationen använder samt frågor som påverkar deras säkerhet. – Organisationens datalager, beskrivningar av dem, databehandlingsprocesser, ansvar, risker och skyddsåtgärder.

Påstående nr	**26**

Delområde	**Verksamhetens kontinuitet och beredskap**
Beskrivning	Organisationen har identifierat funktioner, tjänster, uppgifter, datalager och datasystem som är kritiska för organisationens verksamhet.
Ytterligare information	– det finns en beskriven metod för att definiera hur kritiskt något är

---

Påstående nr	**27**
Delområde	**Verksamhetens kontinuitet och beredskap**
Beskrivning	Organisationen har fastställt hur långa driftsavbrott kritiska funktioner tål utan att störa organisationens verksamhet.
Ytterligare information	– Organisationen känner till kraven i lagstiftningen om tillgången till dess system, register och tjänster. – Organisationen känner till den egna verksamhetens och intressentgruppernas krav.

Påstående nr	**28**
Delområde	**Verksamhetens kontinuitet och beredskap**
Beskrivning	De krav på servicenivå som verksamhetens kontinuitet förutsätter är en del av upphandlingskraven och avtalen.
Ytterligare information	– bl.a. SLA, RPO, RTO

Påstående nr	**29**
Delområde	**Verksamhetens kontinuitet och beredskap**
Beskrivning	Risker med anknytning till kontinuitet och förändringar i risksituationen bedöms regelbundet.
Ytterligare information	– bl.a. SLA, RPO, RTO

Påstående nr	**30**
Delområde	**Verksamhetens kontinuitet och beredskap**
Beskrivning	Det har utarbetats kontinuitetsplaner för organisationen och dess kritiska funktioner/tjänster som grundar sig på identifierade risker.
Ytterligare information	– processen beskriven och bevis på att den fungerar

---

Påstående nr	**31**
Delområde	**Verksamhetens kontinuitet och beredskap**
Beskrivning	Man har uppgjort återhämtningsplaner för kritiska informationssystem.
Ytterligare information	– Inkluderar bl.a. förfaranden för ledning av störningssituationer och alternativa tillvägagångssätt

---

Påstående nr	**32**
Delområde	**Verksamhetens kontinuitet och beredskap**
Beskrivning	Organisationen har en kommunikationsplan för störnings- och krissituationer.
Ytterligare information	– Målgrupper, redskap, ansvar och huvudbudskap för kommunikationen – Även en plan för användningen av alternativa kommunikationssätt när telefon och kommunikationsnät inte är tillgängliga för organisationen eller dess intressentgrupper och kunder.

Påstående nr	**33**
Delområde	**Verksamhetens kontinuitet och beredskap**
Beskrivning	Personer som deltar i hanteringen av störningssituationer har utbildats om innehållet i planerna.
Ytterligare information	

Påstående nr	**34**
Delområde	**Verksamhetens kontinuitet och beredskap**
Beskrivning	Organisationen har skapat kontakter och nätverk för kommunikation mellan nödvändiga intressentgrupper vid avvikelser.
Ytterligare information	– kontaktpunkter och förfaranden har beskrivits

Påstående nr	**35**
Delområde	**Verksamhetens kontinuitet och beredskap**
Beskrivning	Organisationen har ett förfarande för att anmäla störningar, attacker och incidenter i samband med organisationens verksamhet till centrala myndigheter.
Ytterligare information	– bl.a. Polisen, Dataombudsmannens byrå, Cybersäkerhetscentret

Påstående nr	**36**
Delområde	**Verksamhetens kontinuitet och beredskap**
Beskrivning	Organisationen övar regelbundet på att observera, reagera och leda störningar, avvikelser och angrepp som riktas mot organisationens verksamhet.
Ytterligare information	– minst en gång per år (för det valda delområdet) – dokumentation av övningarnas genomförande och observationer

Påstående nr	**37**
Delområde	**Verksamhetens kontinuitet och beredskap**
Beskrivning	Kontinuitets-, återhämtnings- och kommunikationsplaner uppdateras utifrån övningar eller konstaterade störningar
Ytterligare information	– uppdateringsbevis

Påstående nr	**38**
Delområde	**Informationssäkerhet**
Beskrivning	Organisationen har en av ledningen godkänd datasäkerhetspolicy eller motsvarande handling som styr genomförandet av informationssäkerheten.
Ytterligare information	– bl.a. mål, principer, organisering, ansvar

Påstående nr	**39**
Delområde	**Informationssäkerhet**
Beskrivning	Organisationen har ett förfarande för kontroll av personernas bakgrund som omfattar den egna och tjänsteleverantörernas personal.
Ytterligare information	– beskrivet förfarande och bevis på att det fungerar

Påstående nr	**40**
Delområde	**Informationssäkerhet**
Beskrivning	Organisationen har en behörighetspolicy och en process för hantering av användarrättigheter.
Ytterligare information	– dokumenterad process

Påstående nr	**41**
Delområde	**Informationssäkerhet**
Beskrivning	Det säkerställs regelbundet att användarrättigheterna är uppdaterade.
Ytterligare information	– förfarandena har beskrivits, justering minst en gång per år

Påstående nr	**42**
Delområde	**Informationssäkerhet**
Beskrivning	Organisationen har fastställt fysiskt skyddade säkerhetsområden för att skydda dokumenthantering och datasystem.
Ytterligare information	– dokumentation och anvisningar

Påstående nr	**43**
Delområde	**Informationssäkerhet**
Beskrivning	Organisationens datasystem och enheter omfattas i stor utsträckning av systemhanteringen.
Ytterligare information	– bl.a. processer för automatiska uppdateringar

Påstående nr	**44**
Delområde	**Informationssäkerhet**
Beskrivning	Organisationen använder flerstegsautentisering vid fjärranvändning.
Ytterligare information	– MFA, Multi-Factor Authentication eller motsvarande

Påstående nr	**45**
Delområde	**Informationssäkerhet**
Beskrivning	Vid arbete utanför verksamhetslokalerna tillåts förbindelser till organisationens ICT-tjänster endast med VPN-förbindelse.
Ytterligare information	

Påstående nr	**46**
Delområde	**Informationssäkerhet**
Beskrivning	Organisationen har de tekniska lösningar och förfaranden som behövs för att identifiera och förhindra skadliga program.
Ytterligare information	– genomförande på gateway- och arbetsstationsnivå samt nödvändiga anvisningar till personalen

Påstående nr	**47**
Delområde	**Informationssäkerhet**

Beskrivning	Regelbundna säkerhetskopior tas av organisationens uppgifter och system.
Ytterligare information	– beskrivet förfarande och bevis på att det fungerar

---

Påstående nr	**48**
Delområde	**Informationssäkerhet**
Beskrivning	Återställandet av säkerhetskopior testas regelbundet
Ytterligare information	– åtminstone när det gäller kritiska tjänster

---

Påstående nr	**49**
Delområde	**Informationssäkerhet**
Beskrivning	Tillräckliga logguppgifter samlas in om användningen av datasystemen och utlämnandet av uppgifter.
Ytterligare information	– kraven i lagstiftningen och verksamheten har utretts och loggningen genomförts i enlighet med dem – Beaktande av 17 § i informationshanteringslagen och rekommendationen om den

---

Påstående nr	**50**
Delområde	**Informationssäkerhet**
Beskrivning	Meddelanden om tekniska sårbarheter i de datasystem som används följs upp och man reagerar på dem.
Ytterligare information	– beskrivet förfarande och bevis på att det fungerar

---

Påstående nr	**51**
Delområde	**Informationssäkerhet**
Beskrivning	Auditeringar av informationssäkerhet och datasystem görs regelbundet.
Ytterligare information	– innehåller administrativa och tekniska auditeringar – åtminstone i idrifttagningsskedet och regelbundet enligt kritiskhet

---

Påstående nr	**52**
Delområde	**Informationssäkerhet**
Beskrivning	Informationssäkerhets- och dataskyddskraven är en del av upphandlingskraven och avtalen.
Ytterligare information	– är s.k. obligatoriska krav i upphandlingarna

---

Påstående nr	**53**
Delområde	**Informationssäkerhet**
Beskrivning	Informationssäkerhets- och dataskyddskraven beaktas också i utvecklingen och underhållet av systemen och tjänsterna.
Ytterligare information	– beskrivet förfarande och bevis på att det fungerar

---

Påstående nr	**54**
Delområde	**Dataskydd**
Beskrivning	Organisationen känner till vilka personuppgifter den behandlar (artikel 4.1 i dataskyddsförordningen)

Ytterligare information	– namn, adress, e-postadress, telefonnummer osv. – Personbeteckning (29 § i arbetsavtalslagen) – särskilda kategorier av personuppgifter (artikel 9 i dataskyddsförordningen, 6 § i arbetsavtalslagen) – personuppgifter om straffdomar och förseelser (artikel 10 i dataskyddsförordningen, 7 § i arbetsavtalslagen) – Personuppgifter som omfattas av spärrmarkering – Personuppgifter för personalen (integritetsskyddslagen), kunder, besökare, intressentgrupper

---

Påstående nr	**55**
Delområde	**Dataskydd**
Beskrivning	De rättsliga grunderna för behandling av personuppgifter har identifierats (artikel 6, 9 och 10 i dataskyddsförordningen, 6 och 29 § i arbetsavtalslagen och kapitel 2, 3, 5 och 6 i integritetsskyddslagen)
Ytterligare information	– samtycke – avtal – lagstadgad skyldighet (förutsätter att bestämmelsen specificeras) – livsviktiga intressen – allmänt intresse och offentlig makt (förutsätter att bestämmelserna specificeras, att det allmänna intresset specificeras och att den offentliga makten grundar sig på författningar) – berättigade intressen – Särskilda förutsättningar för behandling har beaktats bl.a. i följande fall – grunder för behandling av särskilda kategorier av personuppgifter – behandling av straffdomar och förseelser – behandling av personbeteckning – behandling av personuppgifter i samband med arbetsavtal

---

Påstående nr	**56**
Delområde	**Dataskydd**
Beskrivning	Organisationen har identifierat när den fungerar som personuppgiftsansvarig och när den fungerar som personuppgiftsbiträde (artikel 4 punkt 7–8 i dataskyddsförordningen)
Ytterligare information	– Det finns en process eller anvisningar för identifiering av den personuppgiftsansvarige och personuppgiftsbiträdet

---

Påstående nr	**57**
Delområde	**Dataskydd**
Beskrivning	Avtal om behandling av personuppgifter har ingåtts och avtalshanteringen är i skick (artikel 28 i dataskyddsförordningen)
Ytterligare information	– Är dataskyddet inbyggt i upphandlingsprocessen? – Har kraven och villkoren för behandlingen av personuppgifter beaktats i avtalen med personuppgiftsbiträdena? – Har en modell för avtalshantering utarbetats? – Har man tagit hänsyn till överföringar till tredje länder?

Påstående nr	**58**
Delområde	**Dataskydd**

Beskrivning	Situationer med gemensamt personuppgiftsansvariga har identifierats och man har kommit överens om ansvar för gemensamt personuppgiftsansvariga? (artikel 26 i dataskyddsförordningen; Obs! Även Europeiska dataskyddsstyrelsens anvisning)
Ytterligare information	– Identifieras situationer där det är fråga om gemensamt personuppgiftsansvariga? – Har man kommit överens om ansvarsfördelningen mellan de gemensamt personuppgiftsansvariga, från insamling av information till förstöring/arkivering? – Är rollerna och ansvaren tydliga och transparenta för de registrerade? – anvisning eller process som hjälper att identifiera gemensamt personuppgiftsansvariga och rollerna i anslutning till dem – avtal – kommunikation om roller och ansvarsfördelning till registrerade

---

Påstående nr	**59**
Delområde	**Dataskydd**
Beskrivning	Den egna organisationens interna roller och ansvar i anslutning till behandlingen av personuppgifter har identifierats och fastställts (§ 4.2 i informationshanteringslagen, artikel 37 i dataskyddsförordningen)
Ytterligare information	– registerägare / ansvarspersoner – ledningens ansvar – chefer – personal – kontroll – dataskyddsansvarig – övriga roller (informationshantering, dataskydd, informationssäkerhet, riskhantering, lokalsäkerhet)

Påstående nr	**60**
Delområde	**Dataskydd**
Beskrivning	Dataskyddsombudets ställning och roll har definierats (artikel 37–39 i dataskyddsförordningen)
Ytterligare information	– behovet av att utse ett dataskyddsombud har utretts – Dataskyddsombudets vikariearrangemang i skick, kontakt under frånvaron – dataskyddsombudets uppgifter och ställning följer lagen – beslutet om att utse ett dataskyddsombud – t.ex. ställning definieras i förvaltningsstadgan, arbetsordningen – uppgiftsbeskrivning

---

Påstående nr	**61**
Delområde	**Dataskydd**
Beskrivning	Ett register över behandling har upprättats (artikel 30 i dataskyddsförordningen)
Ytterligare information	– Ingår den information som krävs? – Förverkligas dataskyddsprinciperna i din organisations verksamhet? (artikel 5 i dataskyddsförordningen) – lagenlighet, rimlighet, transparens – ändamålsbegränsning – uppgiftsminimering – korrekthet – begränsning av förvaring – integritet och konfidentialitet

Påstående nr	**62**
Delområde	**Dataskydd**
Beskrivning	Organisationen känner till i vilka datasystem personuppgifter behandlas
Ytterligare information	– datasystemportfölj/datasystemregister – dataflödesbeskrivningar – hjälpfiler/listor

Påstående nr	**63**
Delområde	**Dataskydd**
Beskrivning	Uppgifter utan struktur är identifierade och hanteringen av dem har beskrivits
Ytterligare information	– Identifiering och hantering av sporadiska, icke-strukturerade elektroniska uppgifter – Informationen behandlas i miljöer där informationens livscykel inte kan kontrolleras med hjälp av metadata. – t.ex. e-postmeddelanden, filer på nätdiskar, filer för team på Teams, diskussionshistorik på Skype/Teams

Påstående nr	**64**
Delområde	**Dataskydd**
Beskrivning	Informationspraxis har definierats och följs (artikel 12–14 i dataskyddsförordningen, lag om tillhandahållande av digitala tjänster (306/2019))
Ytterligare information	– Informationens målgrupp samt behandlingens omfattning och karaktär beaktas vid valet av informationspraxis. – Kunna visa att den registrerade har fått information – är informationen begriplig och tillgänglig

Påstående nr	**65**
Delområde	**Dataskydd**
Beskrivning	Organisationen har en process för att identifiera behovet av en konsekvensbedömning (artikel 35 (1) i dataskyddsförordningen)
Ytterligare information	– Har det identifierats när konsekvensbedömning eller förhandssamråd ska genomföras? – Finns det en standardiserad process för att identifiera kriterierna?

Påstående nr	**66**
Delområde	**Dataskydd**
Beskrivning	Organisationen har en process för hantering av personuppgiftsincidenter (artikel 33–34 i dataskyddsförordningen)
Ytterligare information	– Finns det en standardiserad process för att hantera och dokumentera incidenter? – fastställande av kanal för anmälan och ansvarspersoner för behandlingen av anmälningar – myndighetsanmälningar, beslutsansvar för anmälningar – anmälan till registrerade – Hur säkerställs personalens förmåga att identifiera säkerhetsincidenter? – beskrivning av processen

Påstående nr	**67**
Delområde	**Dataskydd**
Beskrivning	Om personuppgifter överförs till tredjeländer, har organisationen utrett förutsättningarna för överföringen? (kapitel 5 i dataskyddsförordningen)
Ytterligare information	– Har man förstått vad som avses med överföring till tredjeländer (t.ex. tillgång till information från tredje land)? – Har man identifierat situationer där överföringar till tredje land sker? – Har man i kravdefinitionen beaktat de situationer där överföringar till tredjeländer inte är möjliga? – Har man beaktat överföringar till tredjeländer i hela underleverantörskedjan? – Villkor för överföring till tredje land

Påstående nr	**68**
Delområde	**Dataskydd**
Beskrivning	I organisationen har omsorgen om dataskyddet förändrats till verksamhet, kultur och attityd (artikel 5 i dataskyddsförordningen)
Ytterligare information	– Fundera på hur du kan bedöma hur verksamheten, kulturen och attityden förändras i din organisation. – t.ex. enkätundersökningar riktade till ledningen och personalen – servicelöfte om beaktande av dataskyddet i organisationens verksamhet – dataskyddspolitik – årsklocka – kompetensmätning

Påstående nr	**69**
Delområde	**Cybersäkerhet**
Beskrivning	Organisationen har beaktat digital säkerhet som en del av helhetsarkitekturen.
Ytterligare information	– åtminstone informationssäkerhet

Påstående nr	**70**
Delområde	**Cybersäkerhet**
Beskrivning	Organisationen har tillräckliga resurser och kompetens för att utveckla den digitala säkerheten som en del av helhetsarkitekturen.
Ytterligare information	– en utsedd ansvarsperson och tid för uppgifterna

Påstående nr	**71**
Delområde	**Cybersäkerhet**
Beskrivning	Organisationen har identifierat sin egen roll i uppgifter enligt Säkerhetsstrategin för samhället samt i ett globalt perspektiv
Ytterligare information	– Hur beroende är samhället av de tjänster som organisationen producerar? – Risk för hybrid-/informationspåverkan samt beredskap för detta

Påstående nr	**72**
Delområde	**Cybersäkerhet**
Beskrivning	Organisationen har identifierat de kritiska tjänster som har en betydande inverkan på verksamheten i andra organisationer eller i samhället.

Ytterligare information – tjänster som andra organisationers operativa verksamhet är beroende av

---

Påstående nr **73**
Delområde **Cybersäkerhet**
Beskrivning Organisationen har på ett heltäckande sätt identifierat kritiska tjänsters beroende av externa tjänsteleverantörer.
Ytterligare information – leverantörer av kritiska tjänster och hur störningar i dessa påverkar organisationens verksamhet

---

Påstående nr **74**
Delområde **Cybersäkerhet**
Beskrivning Risker i anslutning till organisationens kritiska tjänster bedöms och hanteras regelbundet och heltäckande i samarbete med tjänsteleverantörerna.
Ytterligare information – beskrivet förfarande och bevis på att det fungerar

---

Påstående nr **75**
Delområde **Cybersäkerhet**
Beskrivning Tillsammans med kritiska leverantörer och underleverantörer behandlas digital säkerhet regelbundet på leverantörs-/servicehanteringsmöten.
Ytterligare information – beskrivet förfarande och bevis på att det fungerar

---

Påstående nr **76**
Delområde **Cybersäkerhet**
Beskrivning Organisationen har förberett sig och utarbetat en plan för svartmålnings- eller påverkanskampanjer som riktar sig mot organisationen.
Ytterligare information – förfaranden har beskrivits

Påstående nr **77**
Delområde **Cybersäkerhet**
Beskrivning Organisationen har ett förfarande genom vilket den följer upp fenomen i verksamhetsmiljön och bedömer deras inverkan på organisationens verksamhet.
Ytterligare information – förfaranden har beskrivits