17.1.2023

Risikonivå for 101 risikoer, etter tiltak.

USANNSYNLIG		R002, R008, R009, R017, R020, R031, R086, R048, R102, R111, R116, R117, R119, R120, R130, R134, R139, R145, R205, R226, R277, R291	R001, R006, R011, R012, R013, R015, R019, R021, R022, R023, R026, R027, R030, R033, R034, R040, R041, R042, R050, R052, R053, R054, R055, R056, R057, R074, R076, R097, R104, R105, R106, R109, R114, R124, R128, R132, R198, R202, R203, R204, R208, R209, R276, R278	R005, R080, R108, R122, R125, R201, R206
LITE SANNSYNLIG	R010	R003, R024, R029, R035, R078, R079, R091, R126, R129, R160, R275	R049, R051, R070, R075, R077, R084, R085, R086, R103, R107, R110, R112, R200, R238	
SANNSYNLIG		R115, R127		
SVÆRT SANNSYNLIG				
	UBETYDELIG	MODERAT	ALVORLIG	KRITISK

ID	Aktørgruppe	Aktør	Scenario (Som <aktør> er det en risiko for at [jeg]...)	Tiltak	S	K	Risiko
R001	Uvedkommende	Krøsus Kriminell	Som kriminell er det en risiko for at jeg bryter meg inn hos en av dine leverandører og kompromitterer deg for å stjele, manipulere eller sabotere dine verdier, som kundedata (value chain attack).	T038 - Sikkerhetsovervåking (SOC/CERT) T050 - Kontinuitets- og beredskapsplan T114 - Rutinemessig oppfølging av leverandører	1	3	3
R002	KS	Ulrik Utvikler	Som utvikler er det en risiko for at jeg gjør en feil som medfører en uønsket hendelse, uten at det er tilstrekkelig sporbarhet.	T021 - Audit-/revisjonslogg av vesentlige hendelser T027 - Kodegjennomgang T051 - Multifaktor autentisering	1	2	2
R003	KS	Dagny Driftsleverandør	Som driftsleverandør er det en risiko for at jeg ikke har sørget for god nok varsling ved driftsproblemer, noe som fører til at KS bruker unødvendig mye ressurser på å finne løsninger som jeg skulle ha løst.	T001 - Driftsovervåking med alarmering T026 - Rutine for daglig logg-gjennomgang	2	2	4
R005	Kommune	Siri Systemadministrator	Som systemadministrator er det en risiko for jeg harfor høy tillit til innholdet i forsendelser og tar ikke høyde for at kommunen kan motta vedlegg som inneholder ondsinnet programvare.	T010 - Scanning av mottatte meldinger	1	4	4
R006	KS	Ulrik Utvikler	Som utvikler er det en risiko for at jeg skriver kode som innholder en svakhet/et sikkerhetshull, som f.eks. en kjent, utnyttbar svakhet av typen OWASP TOP-10/API-TOP-10 el.l.	T027 - Kodegjennomgang T065 - Statisk kodeanalyse T067 - Dynamisk kodeanalyse (DAST)	1	3	3
R008	KS	Dagny Driftsleverandør	Som driftsleverandør er det en risiko for at jeg ikke har sørget for tilstrekkelig sikkerhetskopiering slik at det blir umulig eller tar uakseptabelt lang tid å gjenopprette løsningen hvis det oppstår et alvorlig problem, som f.eks. kryptovirus.	T030 - Offline sikkerhetskopi T054 - Tilpasset tjenestenivåavtale (SLA)	1	2	2
R009	KS	Dagny Driftsleverandør	Som driftsleverandør er det en risiko for at jeg ikke har sørget for å herde serverne jeg administrerer, noe som fører til kompromittering av dine løsninger.	T003 - Systematisk styring og kontinuerlig forbedring av informasjonssikkerhet (ISMS) T015 - Jevnlig sårbarhetsskanning	1	2	2
R010	KS	Ulrik Utvikler	Som utvikler er det en risiko for at jeg skriver kode som fører til uakseptabel responstid.	T027 - Kodegjennomgang T029 - Ytelsestesting	2	1	2
R011	KS	Ulrik Utvikler	Som utvikler er det en risiko for at jeg har for høy tillit til data fra utenfra, som kan føre til en utnyttbar svakhet via tredjepart.	T014 - Validering, filtrering og sanitering av innkommende data T138 - Policy for autentisering ved kryssing av alle tillitsgrenser	1	3	3
R012	KS	Frida Forvaltning	Som forvalter er det en risiko for at jeg misbruker mine tilganger til å snoke i kundedata, som fører til at data kommer på avveier.	T006 - Krav om begrunnelse for tilgang til data T021 - Audit-/revisjonslogg av vesentlige hendelser T053 - Rutine for tilgangskontroll og -revisjon	1	3	3
R013	Uvedkommende	Krøsus Kriminell	Som kriminell er det en risiko for at jeg gjennomfører et angrep mot din trafikk for å avlytte eller manipulere trafikken og kompromittere dine verdier (som f.eks. data om Inger Innbygger).	T078 - Innebygget personvern og informasjonssikkerhet	1	3	3
R015	KS	Dagny Driftsleverandør	Som driftsleverandør er det en risiko for at jeg ikke patcher viktig programvare raskt nok, noe som fører til at Fiks-plattformen blir kompromittert av uvedkommende.	T019 - Jevnlig møter med sikkerhetsfokus T031 - Automatisk oppdatering og oppgradering T038 - Sikkerhetsovervåking (SOC/CERT)	1	3	3
R017	KS	Ulrik Utvikler	Som utvikler er det en risiko for at jeg ikke saniterer feilmeldinger, som fører til at uvedkommende får informasjon om løsningene som gjør det lettere å kompromittere en eller flere tjenester på Fiks-plattformen.	T012 - Standard feil-side ved feilsituasjoner T027 - Kodegjennomgang T055 - Rutiner for testing av nye og endrete løsninger	1	2	2
R019	KS	Ulrik Utvikler	Som utvikler er det en risiko for at jeg gjør feil ved implementering av ID-porten, som fører til at uvedkommende kan forfalske ID-portens sikkerhetstoken og kompromittere Fiks-plattformen.	T002 - Standard autentisering m/ID-porten T027 - Kodegjennomgang	1	3	3
R020	KS	Ulrik Utvikler	Som utvikler er det en risiko for at jeg gjør en feil som legger til rette for at en angriper kan overta eller på annen måte misbruke DNS-tjenester.	T001 - Driftsovervåking med alarmering T053 - Rutine for endringshåndtering T056 - Rutiner for testing av nye og endrete løsninger T026 - Rutine for daglig logg-gjennomgang	1	2	2
R021	KS	Dagny Driftsleverandør	Som driftsleverandør er det en risiko for at jeg ikke beskytter trafikken til/fra de løsningene jeg administrerer for deg, som fører til at uvedkommende kan avlytte trafikken din.	T032 - Kryptering av trafikk (TLS) T033 - Meldingskryptering T008 - HTTP Strict-Transport-Security (HSTS header)	1	3	3
R022	KS	Ulrik Utvikler	Som utvikler er det en risiko for at jeg glemmer eller unnlater å kryptere en kobling, noe som øker sannsynligheten for avlytting og informasjon på avveier.	T009 - Test for TLS	1	3	3
R023	KS	Ulrik Utvikler	Som utvikler er det en risiko for at jeg ikke tar høyde for at fillageret kan inneholde filer med ondsinnet kode, noe som fører til en mulighet for at fillager kan benyttes til å spre ondsinnet programvare.	T024 - Beskyttelse mot OWASP Topp 10 T071 - Sikkerhetsopplæring og -trening	1	3	3
R024	KS	Ulrik Utvikler	Som utvikler er det en risiko for at jeg ikke oppdager ukjente feil i fiks-plattformen på et tidlig tidspunkt (dev/test), og som dermed fører til unødvendig nedetid på en eller flere tjenester i produksjon.	T001 - Driftsovervåking med alarmering T015 - Jevnlig sårbarhetsskanning T026 - Rutine for daglig logg-gjennomgang T049 - Rutine for avviksrapportering og -håndtering T050 - Kontinuitets- og beredskapsplan	2	2	4
R026	KS	Dagny Driftsleverandør	Som driftsleverandør er det en risiko for at jeg ikke vedlikeholder brannmurene slik at uvedkommende kan utnytte og kompromittere åpne porter.	T038 - Sikkerhetsovervåking (SOC/CERT) T055 - Rutiner for testing av nye og endrete løsninger T076 - Rutine for drift og vedlikehold av nettverkskonfigurasjon	1	3	3
R027	KS	Dagny Driftsleverandør	Som driftsleverandør er det en risiko for at jeg blir utsatt for distribuert tjenestenektangrep (DDOS), noe som fører til at dine digitale tjenester blir utilgjengelige.	T037 - Brannmur T022 - Retry og failover til sekundære kanaler T050 - Kontinuitets- og beredskapsplan	1	3	3

R029 Kommune	Skjalg Saksbehandler	Som saksbehandler er det en risiko for at jeg bruker feil fødselsnummer og får innsyn i eller gjør endringer i personopplysninger på feil person.	T021 - Audit-/revisjonslogg av vesentlige hendelser T045 - Rutiner for administrasjon og bruk av fagsystem T049 - Rutine for avviksrapportering og -håndtering	2	2	4
R030 Uvedkommende	Krøsus Kriminell	Som kriminell er det en risiko for at jeg bryter meg meg inn hos en avsender og misbruker dine tjenester til å stjele eller manipulere data, eller spre ondsinnet innhold via dine løsninger.	T038 - Sikkerhetsovervåking (SOC/CERT) T050 - Kontinuitets- og beredskapsplan T114 - Rutinemessig oppfølging av leverandører	1	3	3
R031 Innbygger	Inger Innbygger	Som innbygger er det en risiko for at jeg benekter å ha mottatt en forsendelse/melding, noe som fører til at kommunen får problemer med å oppfylle en lovpålagt plikt.	T002 - Standard autentisering m/ID-porten T020 - Sikkerhetslogging	1	2	2
R033 KS	Ulrik Utvikler	Som utvikler er det en risiko for at jeg ikke tar høyde for sikkerhetshull i tredjepartsbiblioteker, noe som fører til at svakheter i disse kan utnyttes til å kompromittere en eller flere tjenester på Fiks-plattformen.	T013 - Automatisert skanning og oppdatering av tredjepartsbiblioteker	1	3	3
R034 KS	Ulrik Utvikler	Som utvikler er det en risiko for at jeg planter skadelig kode i Fiks-plattformen, slik at jeg kan kompromittere en eller flere kunder.	T027 - Kodegjennomgang T021 - Audit-/revisjonslogg av vesentlige hendelser	1	3	3
R035 KS	Dagny Driftsleverandør	Som driftsleverandør er det en risiko for at jeg har manglende eller mangelfull varsling av problemer og/eller endringer, som fører til unødvendig lang nedetid og problemer for dine tjenester.	T001 - Driftsovervåking med alarmering T026 - Rutine for daglig logg-gjennomgang T049 - Rutine for avviksrapportering og -håndtering	2	2	4
R036 KS	Ulrik Utvikler	Som utvikler er det en risiko for at jeg ikke tar høyde for at det kan være bevisst/ubevisst feil i data som kommer fra kunde, noe som fører til mulighet kompromittering av en eller flere tjenester på Fiks-plattformen.	T103 - Sanitering av innkommende data T027 - Kodegjennomgang T020 - Sikkerhetslogging T026 - Rutine for daglig logg-gjennomgang	1	2	2
R040 KS	Dagny Driftsleverandør	Som driftsleverandør er det en risiko for at jeg gjør en driftsteknisk endring som fører til kortere eller lengre nedetid på en eller flere av dine digitale tjenester.	T053 - Rutine for endringshåndtering T056 - Rutiner for testing av nye og endrete løsninger	1	3	3
R041 KS	Dagny Driftsleverandør	Som driftsleverandør er det en risiko for at jeg misbruker tilgangen min til å stjele, manipulere eller til å gjøre informasjon utilgjengelig.	T020 - Sikkerhetslogging T030 - Offline sikkerhetskopi T049 - Rutine for avviksrapportering og -håndtering	1	3	3
R042 KS	Dagny Driftsleverandør	Som driftsleverandør er det en risiko for at jeg unnlater å følge god praksis for grunnleggende sikring av driftsmiljøet, som fører til problemer for en eller flere av dine digitale tjenester.	T003 - Systematisk styring og kontinuerlig forbedring av informasjonssikkerhet (ISMS)	1	3	3
R048 KS	Frida Forvaltning	Som forvalter er det en risiko for at jeg får innsyn i personopplysninger jeg ikke har tjenstlig behov for ved f.eks. å slå opp f.nr. i logger.	T006 - Krav om begrunnelse for tilgang til data T021 - Audit-/revisjonslogg av vesentlige hendelser T053 - Rutine for tilgangskontroll og -revisjon	1	2	2
R049 KS	Frida Forvaltning	Som forvalter er det en risiko for at jeg ved et uhell deler informasjon om Inger med feil kommune.	T049 - Rutine for avviksrapportering og -håndtering T050 - Kontinuitets- og beredskapsplan T071 - Sikkerhetsopplæring og -trening	2	3	6
R050 Kommune	Arne Administrator	Som administrator av Fiks-plattformen er det en risiko for at jeg skrur av eller glemmer å skru på en eller flere tjenester på Fiks-plattformen ved en feil, noe som fører til driftsforstyrrelser.	T045 - Rutiner for administrasjon og bruk av fagsystem T049 - Rutine for avviksrapportering og -håndtering	1	3	3
R051 Kommune	Arne Administrator	Som administrator av Fiks-plattformen er det en risiko for at jeg legger inn feil informasjon som er viktig for at en bestemt tjeneste skal fungere, som fører til utilgjengelighet.	T045 - Rutiner for administrasjon og bruk av fagsystem T049 - Rutine for avviksrapportering og -håndtering	2	3	6
R052 Kommune	Arne Administrator	Som administrator av Fiks-plattformen er det en risiko for at jeg gir meg selv tilganger jeg ikke trenger for dermed å få tilgang til informasjon jeg ikke har tjenstlig behov for, noe som fører til at informasjon kommer på avveier når jeg snoker.	T021 - Audit-/revisjonslogg av vesentlige hendelser T058 - Jevnlig kontroll av særlige oppslag/operasjoner	1	3	3
R053 Kommune	Arne Administrator	Som administrator av Fiks-plattformen er det en risiko for at jeg misbruker tilgangene mine og skrur av en eller flere tjenester på Fiks-plattformen, f.eks. fordi jeg ønsker at den ikke skal fungere. Det fører til utilgjengelighet for tjenesten.	T021 - Audit-/revisjonslogg av vesentlige hendelser T058 - Jevnlig kontroll av særlige oppslag/operasjoner	1	3	3
R054 Kommune	Arne Administrator	Som administrator av Fiks-plattformen er det en risiko for at jeg misbruker tilgangene mine og sletter en eller flere mottatte meldinger, f.eks. fordi jeg ønsker å «hjelpe» noen jeg kjenner eller ukjente som betaler godt. Dette fører til integritetsbrudd og utilgjengelighet.	T021 - Audit-/revisjonslogg av vesentlige hendelser T057 - Jevnlig kontroll av særlige oppslag/operasjoner T082 - Rollebasert tilgangskontroll	1	3	3
R055 Kommune	Arne Administrator	Som administrator av Fiks-plattformen er det en risiko for at jeg stjeler informasjon ved å gjøre et uautorisert innsyn i mottatte meldinger, som er et konfidensialitetsbrudd.	T021 - Audit-/revisjonslogg av vesentlige hendelser T057 - Jevnlig kontroll av særlige oppslag/operasjoner T082 - Rollebasert tilgangskontroll	1	3	3
R056 Kommune	Arne Administrator	Som administrator av Fiks-plattformen er det en risiko for at jeg stjeler informasjon ved å kopiere data fra en forsendelse/digital melding jeg kan laste ned, som er et konfidensialitetsbrudd.	T021 - Audit-/revisjonslogg av vesentlige hendelser T057 - Jevnlig kontroll av særlige oppslag/operasjoner T082 - Rollebasert tilgangskontroll	1	3	3
R057 Kommune	Arne Administrator	Som administrator av Fiks-plattformen er det en risiko for at jeg endrer informasjon i data mottatt gjennom en eller flere Fiks-tjenester, ved f.eks. å slette vedlegg eller lignende, som fører til brudd på krav til integritet og tilgjengelighet.	T021 - Audit-/revisjonslogg av vesentlige hendelser T057 - Jevnlig kontroll av særlige oppslag/operasjoner T082 - Rollebasert tilgangskontroll	1	3	3
R070 Innbygger	Inger Innbygger	Som innbygger er det en risiko for at jeg sender feil informasjon til en tjeneste, pga. misforståelser, slik at formålet med tjenesten ikke blir oppfylt.	T080 - Brukermedvirket språkvask og -tilpasning	2	3	6
R074 Uvedkommende	Sutekh Statsaktør	Som statsaktør er det en risiko for at jeg sender en spesielt godt utformet melding (f.eks. e-post) til flere av dine ansatte som klikker på en lenke, kjører min kode og bidrar til at jeg får tilgang til dine data (spearphishing, watering hole, m.m.).	T038 - Sikkerhetsovervåking (SOC/CERT) T050 - Kontinuitets- og beredskapsplan T071 - Sikkerhetsopplæring og -trening	1	3	3

R075 Uvedkommende	Sutekh Statsaktør	Som statsaktør er det en risiko for at jeg samler inn informasjon om dine ansatte slik at jeg lettere kan gjette meg til brukernavn, passord, sikkerhetsspørsmål og lignende, og dermed gjøre det lettere for meg å bryte meg inn i dine løsninger (datainnbrudd).	T051 - Multifaktor autentisering T038 - Sikkerhetsovervåking (SOC/CERT)	2	3	6
R076 Uvedkommende	Sutekh Statsaktør	Som statsaktør er det en risiko for at jeg skanner nettverket ditt, finner noe utdatert utstyr og/eller programvare som inneholder tekniske sårbarheter, og bryter meg inn i løsningene dine (datainnbrudd).	T003 - Systematisk styring og kontinuerlig forbedring av informasjonssikkerhet (ISMS) T015 - Jevnlig sårbarhetsskanning	1	3	3
R077 Uvedkommende	Krøsus Kriminell	Som kriminell er det en risiko for at jeg gjetter meg til et eller flere av dine dårlige passord og skaffer meg tilgang til en konto for å få tilgang til løsningene dine.	T015 - Jevnlig sårbarhetsskanning T038 - Sikkerhetsovervåking (SOC/CERT) T071 - Sikkerhetsopplæring og -trening	2	3	6
R078 Uvedkommende	Krøsus Kriminell	Som kriminell er det en risiko for at jeg sender en spesielt utformet e-post rettet mot akkurat deg, slik at du klikker på en lenke eller åpner et vedlegg, og dermed får kjørt ondsinnet kode inne i dine løsninger (phishing, kryptovirus, bakdør, el.l.).	T015 - Jevnlig sårbarhetsskanning T038 - Sikkerhetsovervåking (SOC/CERT) T071 - Sikkerhetsopplæring og -trening	2	2	4
R079 Uvedkommende	Krøsus Kriminell	Som kriminell er det en risiko for at jeg sender en lite troverdig e-post til deg og alle dine kolleger, samt noen millioner andre, i et håp om at én promille eller to skal bli lurt (spam).	T113 - Automatisk filtrering av meldinger/trafikk med ondsinnet innhold (f.eks. spam) T071 - Sikkerhetsopplæring og -trening T038 - Sikkerhetsovervåking (SOC/CERT)	2	2	4
R080 Uvedkommende	Hanne Hacktivist	Som hacktivist er det en risiko for at jeg saboterer en eller flere av de digitale tjenestene dine for å få oppmerksomhet rundt min egen sak (DOS, DDOS, Defacement, el.l.).	T001 - Driftsovervåking med alarmering T050 - Kontinuitets- og beredskapsplan	1	4	4
R081 Uvedkommende	Krøsus Kriminell	Som kriminell er det en risiko for at jeg bruker din løsning til å angripe brukerne dine ved å putte inn ondsinnet kode alle steder det er mulig (Cross-Site Scripting - XSS).	T071 - Sikkerhetsopplæring og -trening T078 - Innebygget personvern og informasjonssikkerhet T038 - Sikkerhetsovervåking (SOC/CERT)	2	2	4
R084 Innbygger	Inger Innbygger	Som innbygger er det en risiko for at jeg får personopplysningene mine behandlet uten dokumentert, rettslig grunnlag.	T042 - Personvernkonsekvensvurdering (DPIA)	2	3	6
R085 Innbygger	Inger Innbygger	Som innbygger er det en risiko for at jeg får personopplysningene mine behandlet til et formål som ikke er forenelig med det formålet som er oppgitt i DPIA.	T040 - Veiledningsmateriell og opplæring T045 - Rutiner for administrasjon og bruk av fagsystem	2	3	6
R086 Innbygger	Inger Innbygger	Som innbygger er det en risiko for at jeg får overført mine personopplysninger til en tredjestat (et land utenfor EU/EØS).	T044 - Standardisert databehandleravtale for å bruke tjenesten	2	3	6
R097 Uvedkommende	Krøsus Kriminell	Som kriminell er det en risiko for at jeg finner en eller flere svakheter i løsningene dine, bryter meg inn, sprer ondsinnet kode i din infrastruktur og forlanger løsepenger (kryptovirus via sårbarheter).	T078 - Innebygget personvern og informasjonssikkerhet T015 - Jevnlig sårbarhetsskanning T038 - Sikkerhetsovervåking (SOC/CERT) T050 - Kontinuitets- og beredskapsplan	1	3	3
R102 Innbygger	Inger Innbygger	Som innbygger er det en risiko for at jeg ikke finner en personvernerklæring som forteller meg hvem som er ansvarlig for behandlingen og hvordan mine friheter og rettigheter er ivaretatt i løsningen osv.	T041 - Tjenesten dekkes av organisasjonens personvernerklæring	1	2	2
R103 Innbygger	Inger Innbygger	Som innbygger er det en risiko for at jeg ikke får innsyn i mine egne opplysninger, noe som er et brudd mot mine rettigheter etter personopplysningsloven.	T043 - Rutine for innsyn i egne data	2	3	6
R104 Innbygger	Inger Innbygger	Som innbygger er det en risiko for at jeg ikke får mulighet til å reservere meg mot automatisert behandling, noe som er et brudd mot mine rettigheter etter personopplysningsloven.	T042 - Personvernkonsekvensvurdering (DPIA)	1	3	3
R105 Innbygger	Inger Innbygger	Som innbygger er det en risiko for at behandlingen av mine opplysninger mangler et legitimt og klart definert formål, noe som er et brudd mot mine rettigheter etter personopplysningsloven.	T042 - Personvernkonsekvensvurdering (DPIA)	1	3	3
R106 Innbygger	Inger Innbygger	Som innbygger er det en risiko for at behandlingen av mine opplysninger ikke er å anse som nødvendig og/eller proporsjonal ift. det oppgitte formålet, noe som er et brudd mot mine rettigheter etter personopplysningsloven.	T042 - Personvernkonsekvensvurdering (DPIA)	1	3	3
R107 Innbygger	Inger Innbygger	Som innbygger er det en risiko for at opplysningene om meg ikke er korrekt.	T043 - Rutine for å ivareta innbyggers rett til innsyn, retting og sletting egne opplysninger T042 - Personvernkonsekvensvurdering (DPIA)	2	3	6
R108 Innbygger	Inger Innbygger	Som innbygger er det en risiko for at opplysningene om meg ikke er tilstrekkelig sikret med basis i risikovurderinger for å ivareta både konfidensialitet, integritet og tilgjengelighet.	T075 - Rutine for risikovurdering og -håndtering T079 - Forhåndsutfylt ROS og DPIA for tjenesten	1	4	4
R109 Innbygger	Inger Innbygger	Som innbygger er det en risiko for at opplysningene om meg behandles av andre uten at det foreligger en databehandleravtale som ivaretar mine rettigheter og friheter.	T044 - Standardisert databehandleravtale for å bruke tjenesten T064 - Internkontroll	1	3	3
R110 Innbygger	Inger Innbygger	Som innbygger er det en risiko for at jeg glemmer å oppdatere opplysninger i Skatteetatens folkeregister (adresse, navn, kjønn, m.m.) slik at opplysningene mine blir feil i fagsystemene til Skjalg.	T043 - Rutine for å ivareta innbyggers rett til innsyn, retting og sletting egne opplysninger T058 - Rutine for kvalitetssikring av opplysninger	2	3	6
R111 Innbygger	Inger Innbygger	Som innbygger, og kanskje ansatt i kommunen, er det en risiko for at navnet mitt vises i kommunens fagsystem eller andre tjenester på en måte jeg ikke ønsker, f.eks. et mellomnavn jeg aldri bruker el.l.	T092 - Fleksibel navnevisning i fagsystem T028 - Spesifiser og verifiser kompetansekrav hos leverandør	1	2	2
R112 Innbygger	Inger Innbygger	Som innbygger er det en risiko for at jeg plutselig får behov for å skjule min adresse pga. en vanskelig situasjon og er avhengig av at ingen opplyser om min nye situasjon kommer uvedkommende i hende, noe som kan medføre en fare for mitt/min families liv og helse.	T093 - Integrasjon mot sentrale innbygger-registre, som kontakt- og folkeregisteret T028 - Spesifiser og verifiser kompetansekrav hos leverandør	2	3	6
R114 Kommune	Skjalg Saksbehandler	Som saksbehandler er det en risiko for at jeg fyller inn feil, manglende eller mangelfull informasjon når jeg oppdaterer opplysninger om Inger Innbygger.	T040 - Veiledningsmateriell og opplæring T045 - Rutiner for administrasjon og bruk av fagsystem	1	3	3

R115 Kommune	Skjalg Saksbehandler	Som saksbehandler er det en risiko for at jeg glemmer å låse eller logge av PC/fagsystem når jeg forlater arbeidsplassen min.	T072 - Sikkerhetsopplæring og -trening T050 - Rutine for avviksrapportering og -håndtering T048 - Taushetserklæring T049 - Sikkerhetsintruks	3	2	6
R116 Kommune	Skjalg Saksbehandler	Som saksbehandler er det en risiko for at jeg snakker om Inger Innbygger til uvedkommende.	T072 - Sikkerhetsopplæring og -trening T050 - Rutine for avviksrapportering og -håndtering T048 - Taushetserklæring T049 - Sikkerhetsintruks	1	2	2
R117 Kommune	Skjalg Saksbehandler	Som saksbehandler er det en risiko for at jeg gir en kollega tilgang til et fagsystem med mine opplysninger.	T072 - Sikkerhetsopplæring og -trening T050 - Rutine for avviksrapportering og -håndtering T048 - Taushetserklæring T049 - Sikkerhetsintruks	1	2	2
R119 Kommune	Skjalg Saksbehandler	Som saksbehandler er det en risiko for at jeg passer for dårlig på opplysninger om Inger Innbygger slik at de kommer på avveier: -tar opplysninger med meg ut av arbeidslokalene -lar opplysninger ligge åpent tilgjengelig på arbeidsstasjonen min	T072 - Sikkerhetsopplæring og -trening T050 - Rutine for avviksrapportering og -håndtering T048 - Taushetserklæring T049 - Sikkerhetsintruks	1	2	2
R120 Kommune	Skjalg Saksbehandler	Som saksbehandler er det en risiko for at jeg blir lurt per e-post/telefon eller i en samtale til å oppgi taushetsbelagte opplysninger om Inger Innbygger.	T072 - Sikkerhetsopplæring og -trening T050 - Rutine for avviksrapportering og -håndtering T048 - Taushetserklæring T049 - Sikkerhetsintruks	1	2	2
R122 Kommune	Skjalg Saksbehandler	Som saksbehandler er det en risiko for at jeg glemmer eller er sen med å oppdatere informasjon om f.eks. familierelasjonene til Inger Innbygger.	T040 - Veiledningsmateriell og opplæring T045 - Rutiner for administrasjon og bruk av fagsystem	1	4	4
R124 Kommune	Skjalg Saksbehandler	Som saksbehandler er det en risiko for at jeg misbruker mine tilganger til å slå opp, endre eller slette informasjon om Inger.	T021 - Audit-/revisjonslogg av vesentlige hendelser T040 - Veiledningsmateriell og opplæring T049 - Rutine for avviksrapportering og -håndtering T064 - Internkontroll	1	3	3
R125 Kommune	Skjalg Saksbehandler	legger til grunn at folkeregisteret har korrekt informasjon, også når kommunen innehar mer opplysninger om den/de personene det gjelder. (F.eks. fosterbarn.)	T058 - Rutine for kvalitetssikring av opplysninger om daglig omsorg	1	4	4
R126 Kommune	Skjalg Saksbehandler	Som saksbehandler er det en risiko for at jeg får mer informasjon enn jeg har bedt om.	T047 - Taushetserklæring T049 - Rutine for avviksrapportering og -håndtering T127 - Rutine for sletting av overflødighetsinformasjon	2	2	4
R127 Kommune	Siri Systemadministrator	Som systemadministrator er det en risiko for jeg ikke sørger for at fagsystemet til Skjalg blir integrert med Fiks folkeregister.	T093 - Integrasjon mot sentrale innbygger-registre, som kontakt- og folkeregisteret	3	2	6
R128 Kommune	Siri Systemadministrator	Som systemadministrator er det en risiko for jeg misbruker min tilgang som administrator av fagsystemet til å slå opp, endre eller slette informasjon og skape problemer for Inger, Skjalg eller andre.	T053 - Rutine for tilgangskontroll og -revisjon T064 - Internkontroll	1	3	3
R129 Kommune	Siri Systemadministrator	Som systemadministrator er det en risiko for jeg får tilgang til informasjon jeg ikke har tjenstlig behov for.	T047 - Taushetserklæring T049 - Rutine for avviksrapportering og -håndtering	2	2	4
R130 Kommune	Siri Systemadministrator	Som systemadministrator er det en risiko for jeg gjør en feil som fører til at fagsystemet ikke blir oppdatert med de siste opplysningene fra sentrale registre.	T053 - Rutine for tilgangskontroll og -revisjon T056 - Rutine for administrasjon av tjenesten	1	2	2
R131 Kommune	Siri Systemadministrator	Som systemadministrator er det en risiko for jeg gjør feil i forsøk på å filtrere vekk hemmelig adresse (kode 6 eller 7) i forbindelse med ulike typer uttrekk i fagsystemet.	T040 - Veiledningsmateriell og opplæring T045 - Rutiner for administrasjon og bruk av fagsystem	1	2	2
R132 Kommune	Siri Systemadministrator	Som systemadministrator er det en risiko for jeg får ikke varsel om at filtrering av hemmelig adresse (kode 6 eller 7) ikke har fungert som det skal	T047 - Taushetserklæring T049 - Rutine for avviksrapportering og -håndtering	1	3	3
R139 Kommune	Turid Tjenesteadministrator	Som Tjenesteadministrator er det en risiko for at jeg oppretter en rolle med tilgang til mer eller mindre informasjon enn det er tjenstlig behov for.	T040 - Veiledningsmateriell og opplæring T056 - Rutine for administrasjon av tjenesten T021 - Audit-/revisjonslogg av vesentlige hendelser	1	2	2
R145 Innbygger	Inger Innbygger	Som innbygger er det en risiko for at opplysninger om meg lagres lenger enn nødvendig, noe som er et brudd på mine friheter og rettigheter etter personopplysningsloven.	T042 - Personvernkonsekvensvurdering (DPIA) T044 - Standardisert databehandleravtale for å bruke tjenesten T087 - Rutine for arkivering/sletting av data som ikke lenger er saksrelevant.	1	2	2
R160 Kommune	Siri Systemadministrator	Som systemadministrator er det en risiko for jeg ikke sørger for at fagsystemet til saksbehandler blir integrert med relevante registre i Fiks-plattformen.	T093 - Integrasjon mot sentrale innbygger-registre, som kontakt- og folkeregisteret	2	2	4
R198 Kommune	Turid Tjenesteadministrator	Som Tjenesteadministrator er det en risiko for at jeg oppretter en bruker i løsningen til meg selv, og benytter denne brukeren til å gjøre oppslag i informasjon jeg ikke har tjenestlig behov for.	T021 - Audit-/revisjonslogg av vesentlige hendelser	1	3	3
R200 Kommune	Turid Tjenesteadministrator	Som Tjenesteadministrator er det en risiko for at jeg glemmer, eller ikke tar meg tid til, å fjerne brukere som ikke lenger skal ha tilgang til løsningen.	T054 - Rutine for tilgangskontroll og -revisjon	2	3	6
R201 Kommune	Turid Tjenesteadministrator	Som Tjenesteadministrator er det en risiko for at jeg gjør en feil og sletter bruker, rolle eller annen informasjon fra løsningen.	T040 - Veiledningsmateriell og opplæring T056 - Rutine for administrasjon av tjenesten	1	4	4
R202 Kommune	Turid Tjenesteadministrator	Som Tjenesteadministrator er det en risiko for at jeg endrer, eller legger inn feil informasjon som er viktig for at løsningen skal fungere.	T040 - Veiledningsmateriell og opplæring T056 - Rutine for administrasjon av tjenesten	1	3	3

R203	Kommune	Turid Tjenesteadministrator	Som Tjenesteadministrator er det en risiko for at jeg stjeler informasjon ved å gjøre et uautorisert innsyn i mottatt informasjon.	T021 - Audit-/revisjonslogg av vesentlige hendelser T048 - Sikkerhetsintruks T064 - Internkontroll T071 - Sikkerhetsopplæring og -trening	1	3	3
R204	Kommune	Turid Tjenesteadministrator	Som Tjenesteadministrator er det en risiko for at jeg kopierer informasjon fra systemet og videreformidler den til en tredjepart.	T047 - Taushetserklæring T048 - Sikkerhetsintruks T049 - Rutine for avviksrapportering og -håndtering T071 - Sikkerhetsopplæring og -trening	1	3	3
R205	Kommune	Turid Tjenesteadministrator	Som Tjenesteadministrator er det en risiko for at jeg ikke videreformidler informasjon om f.eks. planlagt nedetid i løsningen, slik at brukere ikke får planlagt og tatt høyde for driftsforstyrrelser.	T040 - Veiledningsmateriell og opplæring T056 - Rutine for administrasjon av tjenesten	1	2	2
R206	Kommune	Siri Systemadministrator	Som systemadministrator er det en risiko for at brukerkontoen min blir kompromittert av Krøsus, Hanne eller Sutekh, og de benytter mine tilganger til ondsinnede handlinger	T015 - Jevnlig sårbarhetsskanning T038 - Sikkerhetsovervåking (SOC/CERT) T071 - Sikkerhetsopplæring og -trening	1	4	4
R208	Uvedkommende	Sutekh Statsaktør	Som statsaktør er det en risiko for at jeg manipulerer informasjon for å undergrave tillitten innbyggerne har til offentlig sektor. For å dekke over mine handlinger, får jeg det til å se ut som om det var Krøsus eller Hanne som stod bak angrepet (datainnbrudd).	T031 - Automatisk oppdatering og oppgradering T038 - Sikkerhetsovervåking (SOC/CERT) T050 - Kontinuitets- og beredskapsplan	1	3	3
R209	Uvedkommende	Sutekh Statsaktør	Som stasaktør er det en risiko for at jeg benytter løsningene dine til å samle informasjon om interessante personer i Norge og bygger opp en profil av dem, slik at jeg lettere kan finne måter å manipulere/skade dem på.	T020 - Sikkerhetslogging T038 - Sikkerhetsovervåking (SOC/CERT) T063 - Rutine for gjennomgang av innebygget personvern	1	3	3
R226	KS	Ulrik Utvikler	Som utvikler er det en risiko for at jeg integrerer interne løsninger med sentrale registre uten å følge gjeldende rutiner og retningslinjer for den aktuelle tjenesten.	T107 - Rutine for integrasjon av fellesregistre	1	2	2
R238	Innbygger	Inger Innbygger	Som innbygger er det en risiko for at noen snoker i opplysningene mine uten tjenstlig behov, noe som er et brudd på mine rettigheter og friheter.	T020 - Sikkerhetslogging T049 - Rutine for avviksrapportering og -håndtering T064 - Internkontroll	2	3	6
R275	Kommune	Siri Systemadministrator	Som systemadmin er det en risiko for at jeg ikke følger opp endringer i avtalen, noe som kan føre til at personvern og informasjonssikkerhet blir for dårlig ivaretatt i forhold til krav.	T136 - Organisasjon og rutiner for arbeid med avtaleforvaltning	2	2	4
R276	Kommune	Olve Oppvekst	Som saksbehandler innen oppvekst gjør jeg feil i forbindelse med oppdatering av familierelasjoner, noe som kan få store konsekvenser for de registrerte.	T021 - Audit-/revisjonslogg av vesentlige hendelser T050 - Kontinuitets- og beredskapsplan T058 - Rutine for kvalitetssikring av opplysninger T064 - Internkontroll	1	3	3
R277	Kommune	Olve Oppvekst	Som saksbehandler innen oppvekstområdet misbruker jeg mine tilganger til å snoke i taushetsbelagte opplysninger jeg ikke har tjenstlig behov for, noe som er et alvorlig brudd på taushetsplikten min og de registrertes personvern.	T021 - Audit-/revisjonslogg av vesentlige hendelser T064 - Internkontroll T050 - Kontinuitets- og beredskapsplan	1	2	2
R278	Kommune	Olve Oppvekst	Som saksbehandler innen oppvekstområdet misbruker jeg mine tilganger til å manipulere eller slette opplysninger om familierelasjoner, noe som kan få store konsekvenser for de registrerte.	T021 - Audit-/revisjonslogg av vesentlige hendelser T064 - Internkontroll T050 - Kontinuitets- og beredskapsplan	1	3	3
R291	Kommune	Siri Systemadministrator	Som systemadministrator av kommunens identitetsadministrasjonssysteme (IDM) gjør jeg en feil i oppsett av integrasjon mot Fiks-plattformen som fører til at Skjalg ikke får nødvendig tilganger til å løse sine oppgaver.	T040 - Veiledningsmateriell og opplæring T045 - Rutiner for administrasjon og bruk av fagsystem T049 - Rutine for avviksrapportering og -håndtering	1	2	2

ID	Tiltak	Ansvarlig	Frist	Status	Kommentar
T136	Organisasjon og rutiner for arbeid med avtaleforvaltning	Kommune		Kommune	
T138	Policy for autentisering ved kryssing av alle tillitsgrenser	KS		Innført	
T001	Driftsovervåking med alarmering	KS		Innført	Alle tjenester på Fiks-plattformen overvåkes mht. oppetid, feil og problemer. Det går automatisk en alarm dersom det oppstår uønskede situasjoner.
T002	Standard autentisering m/ID-porten	KS		Innført	ID-porten benyttes som standard autentiseringsmekanisme i Fiks-plattformen. Dette sørger for en standardisert og sentralisert autentiseringsløsning på tvers av tjenester på plattformen. Det medfører også at tjenestene på plattformen automatisk kommer med såkalt sterk autentisering. Jf. OWASP API Top-10 --> API2
T003	Systematisk styring og kontinuerlig forbedring av informasjonssikkerhet (ISMS)	KS		Innført	Intilitys datasentre og Grafisk Digital er ISO27k-sertifisert
T006	Krav om begrunnelse for tilgang til data	KS		Innført	Alle oppslag i kundedata blir begrunnet med knytning til, eller etablering av, kundeforespørsel i Freshdesk.
T008	HTTP Strict-Transport-Security (HSTS header)	KS		Innført	Benytter HTTP Strict Transport Security (HSTS) with long duration som standard for å unngå MitM, protocol downgrade og cookie hijacking.
T009	Test for TLS	KS		Innført	Sporadisk testing av alle endepunkter med SSL-Labs. 15.3.21, får fortsatt: This server supports TLS 1.0 and TLS 1.1 jf. T076 Deprekering av uakseptabel funksjonalitet.
T010	Scanning av mottatte meldinger	Kommune		Kommune	Dette må evt. gjøres i mottakssystemet. Dette lar seg ikke gjøre uten å endre dataflyt og vil skape grunnlag for flere uønskede sårbarheter.
T012	Standard feil-side ved feilsituasjoner	KS		Innført	For å unngå at man eksponerer teknisk informasjon til uvedkommende, benyttes en standard feilside som standard i Fiks-plattformen. Dette fører til mindre sannsynlighet for at feilsituasjoner kan benyttes til å utføre onde hensikter.
T013	Automatisert skanning og oppdatering av tredjepartsbiblioteker	KS		Innført	P.t. er overvåking og varsling automatisert gjennom github (via Dependabot security og version updates, som automatisk lager en PR for å holde både kode og manifester oppdatert).
T014	Validering, filtrering og sanitering av innkommende data	KS		Innført	Data fra en hvilken som helst leverandør/integrasjon bør kontrolleres for ondsinnet kode SQL/NoSQL/LDAP/OS/XML/ORM. Jf. OWASP API Top-10 --> API8
T015	Jevnlig sårbarhetsskanning	KS		Innført	Ukentlig skanning av alt innenfor brannmuren.
T019	Jevnlig møter med sikkerhetsfokus	KS		Innført	Månedlige møter, samt ad-hoc møter ved behov.
T020	Sikkerhetslogging	KS		Innført	Alle sikkerhetsrelaterte hendelser blir logget både i system- og eventlogg. Data for når en forsendelse blir lest logges. Fnr, dato og tidspunkt logges.
T021	Audit-/revisjonslogg av vesentlige hendelser	KS		Innført	Audit-logg følger WORM-prinsippet (write once, read many) og krever begrunnelse for oppslag. Må backes av T068 Internkontroll
T022	Retry og failover til sekundære kanaler	KS		Innført	Retry 4 ganger, deretter forsøke andre aktuelle kanaler.
T024	Beskyttelse mot OWASP Topp 10	KS		Innført	Sjekkes både gjennom Spotbugs i IDE og av SonarCloud.
T026	Rutine for daglig logg-gjennomgang	KS		Innført	Utfyller T001 - Driftsovervåkning og -alarmering, for å sjekke mot en grunnleggende normaltilstand for enhver tjeneste og oppdage eventuelle unormale og uønskede hendelser ifm. med tjenestene.
T027	Kodegjennomgang	KS		Innført	Alle kodeendringer skal gjennomgås av en annen utvikler enn den som har skrevet koden (peer-reviewes via pull requests i github).
T028	Spesifiser og verifiser kompetansekrav hos leverandør	Alle		Innført	I den grad det kreves særlig kompetanse hos leverandør er det viktig at dette blir godt beskrevet, stilt krav om i avtaleverk og fulgt opp ved behov. Behov for oppfølging kan typisk oppstå ved evaluering av feilsituasjoner og uønskede hendelser.
T029	Ytelsestesting	KS		Pågår	Ytelsestesting har vist seg å være nødvendig. I tilfeller hvor vi har opplevd ytelsesutfordringer er det skrevet enhets- og/eller integrasjonstester for å teste ytelse, men vi planlegger å jobbe med å oppnå bedre dekning for hele plattformen.
T030	Offline sikkerhetskopi	KS		Innført	Komplett restore gjennomført ved migrering til ny driftsleverandør.
T031	Automatisk oppdatering og oppgradering	KS		Innført	
T032	Kryptering av trafikk (TLS)	KS		Innført	All trafikk til og fra API-ene krypteres i dag med TLS 1.3 som minimum.
T033	Meldingskryptering	KS		Innført	
T037	Brannmur	KS		Innført	
T038	Sikkerhetsovervåking (SOC/CERT)	KS		Innført	Intility SOC driver SIEM og ThreatIntel 24/7, ringer hvis alvorlig og ellers rapport via sikkerhetsmøter. Jobber med å få ut info i portal.intility.no
T040	Veiledningsmateriell og opplæring	Kommune		Kommune	Veiledning, opplæring og trening er viktig om man skal oppnå ønsket resultat. Derfor er det viktig å se på veilednings- og opplæringsmateriell som en vesentlig del av en tjeneste. Avviksoppfølging, ROS og DPIA kan være et godt grunnlag for å utvikle og vedlikeholde denne typen materiell.
T041	Tjenesten dekkes av organisasjonens personvernerklæring	Kommune		Kommune	Kommunen, som behandlingsansvarlig, har en plikt til å sørge for at enhver behandling er dekket av en personvernerklæring som skal være lettlest og forståelig for alle og enhver. Erklæringen bør inneholde en beskrivelse av hvilke data som behandles, til hvilke formål og hvem hvilken lovhjemmel. I tillegg skal erklæringen inneholde informasjon til den registrerte om hvor og hvordan henvende seg ved spørsmål om ivaretakelse etter personvernlovgivningen (GDPR).
T042	Personvernkonsekvensvurdering (DPIA)	Kommune		Kommune	Kommunen, som behandlingsansvarlig, har en plikt til å sørge for å gjøre en vurdering av ivaretakelsen av personvernet til den registrerte (vanligvis Inger Innbygger) knyttet til enhver behandling kommunen foretar seg.

T043 Rutine for å ivareta innbyggers rett til innsyn, retting og sletting egne opplysninger	Kommune	Kommune	Kommunen må sørge for å ha en rutine som beskriver hvordan forespørsel fra den registrerte om innsyn i, retting eller sletting av egne opplysninger etter personvernforordningen skal håndteres.
T044 Standardisert databehandleravtale for å bruke tjenesten	Kommune	Kommune	KS har utarbeidet en standard databehandleravtale. Den er et bilag til tjenesteavtalen kommunen skal ha tegnet med KS for bruk av Fiks-plattformen. I tillegg skal det undertegnes et eget vedlegg til denne databehandleravtalen for hver enkelt tjeneste kommunen tar i bruk. Disse vedleggene finner man på portal.fiks.ks.no.
T045 Rutiner for administrasjon og bruk av fagsystem	Kommune	Kommune	Det bør foreligge en rutine for hvordan et fagsystem skal administreres, hvilke roller som har hvilket ansvar, hva som er prosedyren for tildeling av tilganger, hvem som kan bestille tilganger osv.
T047 Taushetserklæring	Kommune	Kommune	KS har egne taushetserklæringer for den enkelte ansatte, så vel som med underleverandører. Kommunens ansatte har i utgangspunktet en generell taushetsplikt om "noens personlige forhold" via forvaltningsloven, men bør vurdere behovet for en mer eksplisitt erklæring i tilknytning til tjenester med særlig sensitiv behandling av persondata.
T048 Sikkerhetsintruks	Kommune	Kommune	KS har en egen erklæring om akseptabel bruk av IKT, som alle ansatte i avdeling for digitale fellestjenester må undertegne. Dette for å gjøre behovet for å ta opplæring, trening og ansvar på alvor og sørge for at alle får samme, gode utgangspunkt for å sette seg inn i hvor grensene går innen personvern og informasjonssikkerhet. Det er ansett som god praksis å ha en slik erklæring. Den kan gjerne kombineres med taushetserklæring (jf. T047). Kommunen bør ha en tilsvarende erklæring i tilknytning til tjenester som behandler særlig sensitive personopplysninger, som f.eks. tjenestene smittesporing, digisos og bekymringsmelding.
T049 Rutine for avviksrapportering og -håndtering	Kommune	Kommune	For å fange opp at noe går galt er man nødt til å ha en lav terskel for hva man anser som avvik. Uansett alvorlighet vil ethvert avvik representere en berikelse av risikobildet i egen organisasjon. Hvis det f.eks. forekommer 20 mindre hendelser knyttet til feilregistrering i ett bestemt system, kan det tyde på at det vil være en god investering å innføre bedre opplæring, be om en endring fra systemleverandør eller innføre kontrolltiltak før noe lagres endelig osv.
T050 Kontinuitets- og beredskapsplan	Kommune	Kommune	KS har en egen kontinuitets- og beredskapsplan til bruk om noe ikke går som det skal. Dette for å være sikrest mulig på at man reagerer raskt og effektivt, hvis en tjeneste f.eks. opplever ustabilitet, eller vi skulle få beskjed om at noen forsøker å gjøre ugagn mot de digitale fellestjenestene. Kommunen skal også ha en slik kontinuitets- og beredskapsplan som dekker den enkelte tjeneste. Hva gjør man om tjenesten slutter å virke?
T051 Multifaktor autentisering	Kommune	Kommune	For behandling av særlige kategorier personopplysninger, også kalt sensitive personopplysninger, krever Datatilsynet at man benytter "sterk autentisering", dvs. en pålogging som krever en tilleggskode utover passord, slik man f.eks. har i forbindelse med pålogging til banken vha. BankID. Alle tjenester i Fiks krever en form for sterk eller flerfaktor autentisering, men kommunen bør også skru dette på i sine egne fagsystemer for at hele kjeden av systemer skal være like godt sikret.
T053 Rutine for tilgangskontroll og -revisjon	Alle	Kommune	Ofte er det enklere å få tilgang enn å bli kvitt den. Enhver organisasjon må selv sørge for rutinemessig og jevnlig gjennomgang av hvem som får tilgang til hva og om tilgangene de har passer til jobben de er satt til å gjøre. Ethvert fagsystem og en hver tjeneste bør ha en egen rutine for hvordan dette skal foregå, med mindre man har en sentral, standardisert rutine som skal følges av alle.
T054 Tilpasset tjenestenivåavtale (SLA)	Kommune	Kommune	Kommunen har trolig inngått en tjenesteavtale med KS' avdeling for digitale fellestjenester, men om ikke det er gjort skal dette gjøres. Det samme må gjøres med andre leverandører av tjenester i tilknytning til tjenesten, for at tjenestens totalleveranse skal henge sammen, bør disse avstemmes med hensyn til leveransekrav.
T055 Rutiner for testing av nye og endrete løsninger	Alle	Kommune	Som nevnt i tiltak T053 - Rutine for endringshåndtering og -oppfølging øker sannsynligheten for feil og mangler ved endringer, dermed er det også god praksis å sørge for god testing før, under og etter produksjonssetting av nye og endrete løsninger.
T056 Rutine for administrasjon av tjenesten	KS & Kommune	Kommune	Kommunen må sørge for å ha en tydelig rutine for administrasjon av tjenesten. Rutinen må presisere evt. krav til hvem som skal og kan ha det formelle ansvaret for tjenesten, f.eks. skal Fiks smittesporing "eies" av Kåra Kommunelege, da det er kommunelegen som har det formelle ansvaret for å drive smittesporing. Den tjenesteansvarlige delegerer tilgang til bruk av tjenesten, til f.eks. Stig Smittesporer.
T057 Jevnlig kontroll av særlige oppslag/operasjoner	Kommune	Kommune	Som en del av internkontrollvirksomheten innen personvern og informasjonssikkerhet, bør det foreligge en rutine for jevnlig kontroll av særlige oppslag og/eller operasjoner mot alle systemer som behandler personopplysninger. Spesielt bør det være fokus på systemer og løsninger som behandler særlige kategorier personopplysninger, som helse- og sosial-systemer.
T058 Rutine for kvalitetssikring av opplysninger	Kommune	Kommune	Innen alle områder hvor familierelasjoner er en viktig del av saksbehandlingen, er det nødvendig å ha en rutine for å ta en ekstra sjekk knyttet til nåværende situasjon da familierelasjoner endrer seg.
T063 Rutine for gjennomgang av innebygget personvern	KS	Innført	Innebygget personvern er et sentralt krav i personopplysningsloven og betyr at det tas hensyn til personvern i alle utviklingsfaser av en løsning. Rutine for gjennomgang av innebygget personvern skal sørge for at KS' tjenester oppfyller personvernprinsippene, så langt det lar seg gjøre, og at de ivaretar de registrertes rettigheter (jf. datatilsynet.no/rettigheter-og-plikter/virksomhetens-plikter/innebygget-personvern)
T064 Internkontroll	Alle	Kommune	Rutine for sporadisk kontroll av logger for å avdekke anomalier som misbruk o.l.
T065 Statisk kodeanalyse	KS	Innført	Kjører SonarCloud på alle repos. Anbefaler utv. å bruke SpotBugs i IDE for å unngå de fleste problemene som fanges opp av Sonar.
T067 Dynamisk kodeanalyse (DAST)	KS	Pågår	Vurderer OWASP ZAP automatisert inn i pipen, i stedet for hostedscan og sporadisk
T071 Sikkerhetsopplæring og -trening	Alle	Kommune	Årlige 2-trinns opplæring; grunnleggende og ISMS.

T072 Deprekering av uakseptabel/utdatert funksjonalitet	KS	Pågår	På tross av at vi har noen fagsystemer som integrerer mot gamle versjoner av f.eks. SvarUt-API, så er det planlagt å deprekere gamle API-versjoner som f.eks. benytter SAML i stedet for OIDC.
T075 Rutine for risikovurdering og -håndtering	Kommune	Kommune	En risikovurdering er et verktøy for å identifisere uønskede hendelser og risikoen for at disse skal inntreffe. Risikovurdering er en viktig del av virksomhetens internkontroll og rutinen for risikovurdering og -håndtering i KS sørger for at risiko til enhver tid blir hensyntatt i forbindelse med forvaltning, drift og vedlikehold av Fiks-plattformen.
T076 Rutine for drift og vedlikehold av nettverkskonfigurasjon	KS	Innført	Driftsleverandør må ha en driftsrutine som beskriver hvordan de skal håndtere endringer i nettverkskonfigurasjonen, fra brannmurendringer, oppdatering/oppgradering av nettverksutstyr som medfører eller kan medføre konsekvenser for en av våre tjenester.
T078 Innebygget personvern og informasjonssikkerhet	Kommune	Kommune	Personvern og informasjonssikkerhet har fokus gjennom hele prosessen i alt fra utvikling av brukerhistorier (krav), opplæring via fokus på sikker koding og fokus på arkitektur- og risikoanalyse samt sikkerhetstesting på flere nivåer med både enhetstesting, statisk- og dynamisk kodetesting, brukertesting og penetrasjonstesting.
T079 Forhåndsutfylt ROS og DPIA for tjenesten	KS	Innført	KS bidrar til å gjøre jobben med å utføre ROS og DPIA enklere ved å publisere forhåndsutfylte ROS og DPIA. KS har foreslått en vurdering av risiko, men det er opp til kommunen selv å vurdere sannsynlighet og konsekvens, for å oppnå en reell risikovurdering. Både risikohistoriene og tiltakene er å anse som forslag fra KS sin side. Dermed må kommunene gjerne legge til å trekke fra basert på egne behov og vurderinger.
T080 Brukermedvirket språkvask og -tilpasning	KS	Innført	KS har kontinuerlig dialog med brukerrepresentanter for å oppnå best mulig kommunikasjon og brukeropplevelse i tjenestene sine.
T082 Rollebasert tilgangskontroll	KS & Kommune	Kommune	Fiks-plattformen baserer seg på en fingranulert ansvarsfordeling basert på rollebasert tilgangskontroll, som gir sentral støtte for prinsippet om "separation of concerns". Dette medfører blant annet at hovedadministrator ikke kan tildele andre brukere enn rollen som tjenesteansvarlig, og at tjenesteansvarlig er ansvarlig for tildeling av ordinære brukere av tjenesten osv. Det er viktig at kommunene følger opp med gode rutiner for tildeling av roller, samt internkontroll internt i egen organisasjon.
T087 Rutine for arkivering/sletting av data som ikke lenger er saksrelevant.	Kommune	Kommune	Det er viktig å sørge for å ha en overordnet beslutning om hvor lenge man har behov for tilgang til data i den enkelte tjeneste, og lage en rutine for arkivering/sletting av data som ikke lenger er nødvendig.
T092 Fleksibel navnevisning i fagsystem	Fagsystem	Planlagt	Den enkelte fagsystemleverandør må støtte bruk av Fiks folkeregister og implementere mulighet for alternative visninger av navn, f.eks. med eller uten mellomnavn osv.
T093 Integrasjon mot sentrale innbygger-registre, som kontakt- og folkeregisteret	Kommune	Kommune	Kommunen er avhengig av at opplysningnene om Inger Innbygger er oppdatert for å kunne følge opp sine plikter overfor innbygger på en forsvarlig måte, derfor er det viktig at alle fagsystemer er koblet opp mot innbyggerregistere som DigDirs kontaktregister og Skatteetatens folkeregister slik at opplysningene om Inger Innbygger er så oppdatert som mulig. Begge deler får man gjennom en integrasjon mot Fiks folkeregister.
T103 Sanitering av innkommende data	Kommune	Kommune	Det er god praksis å "sanitere" innkommende data, uansett hvor de kommer fra. På teknisk nivå er det viktig å sjekke innkommende eller mottatte data er av ønsket karakter og ikke innholder uønskede elementer, for å forsikre seg om at de ikke kan skade eller skape problemer. Dette gjelder så vel i kommunens egne systemer som i Fiks-plattformen.
T107 Rutine for integrasjon av fellesregistre	KS	Innført	For å hindre at utvikling integrerer sentrale registre, som Fiks folkeregister, skal utvikling følge denne rutinen for å sikre at integrasjoner blir planmessig utført.
T113 Automatisk filtrering av meldinger/trafikk med ondsinnet innhold (f.eks. spam)	Kommune	Kommune	All innkommende nettverkstrafikk bør filtreres for potensielt ondsinnet innhold. De fleste har f.eks. filtrering av e-post for å unngå for mye "spam".
T114 Rutinemessig oppfølging av leverandører	Kommune	Kommune	Alle leverandører bør følges opp i forhold til de krav man stiller, også til informasjonssikkerhet og personvern. KS' avdeling for digitale fellestjenester tar f.eks. sporadiske kontroller av sine leverandører og ber f.eks. om å få se risikovurderinger eller avvikssystem. Kommunen bør sørge for å gjøre det samme med sine leverandører, eks. fagsystemleverandører og andre som tar del i tjenesteleveransen.
T127 Rutine for sletting av overflødighetsinformasjon	Kommune	Kommune	Det er viktig at mottaker av informasjon gjør en vurdering av hvor nødvendig det faktisk er å ta vare på den, og hvor vidt den belyser den faktiske saken eller ikke. Mottar man opplysninger som ikke er nødvendig, bør disse slettes.

Hanne Hacktivist	Bror Brukerstøtte	Arne Administrator	Bjarne Barnet
Krøsus Kriminell	Dagny Driftsleverandør	Berit Barnevern	Erna Elev
Sara Snoker	Fenrik Fellestjeneste	Inga Internkontroll	Inger Innbygger
Snurre Scriptkiddie	Frida Forvaltning	Kåra Kommunelege	Vera Verdensborger
Sutekh Statsaktør	Pelle Printleverandør	Olve Oppvekst	Ulla Ungdom
Mathias Misfornøyd	Sjur Sikkerhet	Pernille Personvern	Frode Forsørger
	Ulrik Utvikler	Siri Systemadministrator	Frigg Forelder
	Arn Arkitekt	Fredrik Fastlege	Frøya Fosterforelder
		Ina Innreiseoppfølger	Vilde Verge
		Larry Leverandør	
		Rune Revisor	
		Skjalg Saksbehandler	
		Stig Smittesporer	
		Telle Teknolog	
		Tore Tjenestemann	
		Turid Tjenesteadministrator	