TL;DR – Too Long; Didn't Read

Veilederen gir retningslinjer for sikker programvareutvikling i Oslo kommune, med mål om å integrere sikkerhet i alle deler av utviklingsprosessen. Den bygger på anbefalte sikkerhetstiltak i ISO 27002 og NSMs grunnprinsipper, samt GDPR-kravene om innebygd personvern (art. 25) og informasjonssikkerhet (art. 32). Veilederen følger DevOps-metodikken, hvor sikkerhet inngår i hver fase av utviklings- og driftsprosessen. Ansvarsfordelingen *mellom systemeier, teamleder, techlead og utviklere* sikrer at sikkerhet håndteres systematisk, effektivt og i tråd med kommunens sikkerhetskrav.

Prinsipper for sikker utvikling

Sikkerhet må være en naturlig og kontinuerlig del av programvareutviklingen. Dette oppnås ved:

- **Tydelig ansvarsfordeling** mellom systemeiere, teamleads, techleads og utviklere for å sikre helhetlig risikostyring. HUKI-matrisen brukes for å tydeliggjøre hvem som gjør hva:
  - **Hovedansvarlig (H)** – Ansvarlig for initiativ, gjennomføring og oppfølging av oppgaver.
  - **Utførende (U)** – Utfører det praktiske arbeidet med oppgaven.
  - **Konsulteres (K)** – Må involveres i gjennomføring og kan påvirke utfallet.
  - **Informeres (I)** – Skal holdes løpende informert om status og resultater.
- **Sikkerhetsopplæring** for å holde teamet oppdatert på trusler, regelverk og beste praksis innen sikker programvareutvikling.
- **Automatisering** av sikkerhetstiltak gjennom sikkerhetsskanning, kodeanalyse og kontinuerlig overvåking av applikasjoner og infrastruktur.
- **Risikostyring** for å prioritere tiltak og ressurser basert på sårbarhetsvurderinger, trusselanalyser og sikkerhetsetterlevelse av relevante forskrifter.

Faser i sikker programvareutvikling

Planlegge: Fastsette sikkerhetskrav, gjennomføre risikovurderinger og allokere nødvendige ressurser.

Programmere: Utvikle sikker kode med oppdaterte rammeverk, begrensede rettigheter og systematisk kodekontroll.

Bygge: Automatisere sikkerhetstester, sårbarhetsanalyser og sikre at kodegjennomganger gjennomføres regelmessig.

Teste: Validere sikkerhetsfunksjoner og bruke trygg testdata med kontinuerlig testing og vurdering av penetrasjonstester.

Utrulling: Sørge for sikker og kontrollert distribusjon med autentisering, tilgangsstyring, overvåking og testet rollback i produksjonsmiljøet.

Drift: Sikre stabil og trygg drift gjennom oppdateringer, tilgangsstyring, sikkerhetskopiering og sårbarhetsanalyser.

Systemovervåking og hendelseshåndtering: Oppdage, varsle og håndtere hendelser raskt med definerte rutiner, øvelser og eskalering.

Avvikling: Avslutte systemer trygt gjennom risikovurdert avvikling, sikker sletting og fjerning av tilganger.

Veilederen understreker at sikker programvareutvikling ikke er et engangstiltak, men en kontinuerlig prosess. Ved å integrere sikkerhet i alle faser reduseres risikoen for sårbarheter, og robuste digitale tjenester bygges for å beskytte brukere, data, systemer og samfunnskritiske tjenester mot cybertrusler.

Veileder: informasjons- og personopplysningssikkerhet i programvareutvikling

Fase	Oppgave	Systemeier	Teamleder	Techlead	Utvikler
Planlegge	Akseptnivå for risiko	K	H	I	I
	Risikoanalyse	K	H	U	U
	Restrisiko	K	H		
	Planlegg og iverksett tiltak etter risikoanalyse		I	H	U
	Etablere rutiner for utviklingsfaser		H	U	U
	Etablere plan for kompetanseheving		H		
	Sikre finansiering for alle utviklingsfaser	H	I		
	Sikre tilstrekkelige ressurser (bemanning)		H	I	I
Programmere	Kompetanseheving i programmeringsfasen		H	KU	U
	Tredjepartsbiblioteker og rammeverk holdes oppdatert			H	U
	Begrensede rettigheter i utviklingsmiljøer		H	K	I
	Benytte kontinuerlig kildekodekontroll			H	U
	Manuell kildekodegjennomgang (QA)			H	U
	Kjøre automatiserte enhetstester			H	U
Bygge	Kompetanseheving i byggefasen		H	KU	U
	Teknisk konfigurasjon av sikkerhetsverktøy			H	U
	Kjøre automatiserte sikkerhetstester			H	U
	Oppfølging av avvik		H	KU	U
Teste	Kompetanseheving på sikkerhetstesting		H	KU	U
	Sikre trygg bruk av testdata		H	U	U
	Kontinuerlig sikkerhetstesting		K	H	U
	Vurdere ytterligere sikkerhetstester som penetrasjonstest	I	H		
	Oppfølging av testresultatene	I	H	KU	U
Utrulling	Følge etablerte utrullingsrutiner			H	U
	Automatisering og overvåkning av utrulling		I	H	U
	Verifikasjon funksjonalitet og sikkerhet			H	U
	Tilrettelegge for og teste tilbakerulling (rollback)			H	U
	Oppdatere og vedlike utrullingsdokumentasjon		H	U	U
Drift	Tjenestetilgjengelighet og ytelse (SLA) i tråd med avtaler	K	H	U	U
	Bruker- og systemtilganger revideres og justeres		H	KU	U
	Håndtere endringer i produksjonsmiljø		I	H	U
	Automatisert sikkerhetskopiering og gjenoppretting			H	U
	Håndtere sikkerhetsoppdateringer			H	U
	Sårbarhetsanalyse og validering av tiltak		K	H	U
Systemover-våking og hendelses-håndtering	Opplæring og øvelser i sikkerhetshendelser		H	KU	U
	Planverk for håndtering av sikkerhetshendelser	I	H	U	I
	Drift av verktøy for systemovervåkning		I	H	U
	Eskalering og tiltak ved kritiske hendelser	K	H	I	
	Informasjon til eksterne ved alvorlige hendelser	H	U	I	
	Verifisere loggfunksjonalitet			H	U
	Evaluere og lære av hendelser (postmortem)	I	H	U	I
Avvikle	Beslutning og risikovurdering av avvikling	K	H	I	I
	Arkivering og dataoverføring	K	H	U	U
	Teknisk sanering og datasletting	I	K	H	U
	Håndtering og fjerning av fysiske og digitale tilganger	I	K	H	U