KOMBIT

Version 1.3

Instruks til gennemførsel af og rapportering om penetrationstest

1. Formål **3**

2. Roller og Ansvar **3**

3. Omfang af penetrationstest **3**

3.1 Information om systemet 3

3.2 Håndtering af data in transit 3

3.3 Håndtering af data at rest 3

3.4 Håndtering af privatnøgler og certifikater 3

4. Udarbejdelse af penetrationstest **4**

4.1 Opstartsmøde 4

4.2 Detaljerede rapport 4

4.3 Handlingsplan 4

5. Versionshistorik **5**

1. Formål

Denne instruks er udarbejdet af KOMBIT til brug for KOMBITs kontrakter med leverandører om levering af drift, vedligeholdelse mm. af de enkelte it-systemer (i de enkelte kontrakter benævnt "Systemet").
Instruksen skal følges af leverandørerne ved gennemførsel af og rapportering om penetrationstest under den enkelte kontrakt med KOMBIT.

2. Roller og Ansvar

Det er forudsat, at data, der behandles i Systemet, i mange tilfælde vil være personoplysninger i henhold til persondatalovgivningen, eller på anden måde fortrolige oplysninger. For at sikre, at oplysningerne er tilstrækkeligt sikret mod uvedkommende adgang til data, skal det sikres, at systemet og driftsmiljøet ikke kan penetreres. Alle miljøer, som indeholder produktionsdata, herunder også pseudonymiseret data, skal have foretaget en fuld penetrationstest. Leverandøren er forpligtiget til at bruge et eksternt anerkendt sikkerhedsfirma, godkendt af KOMBIT, til gennemførsel af penetrationstest.
Til brug for KOMBITs og de(n) dataansvarliges tilsyn med leverandøren (underdatabehandler) og dennes underleverandører (under-underdatabehandlere) skal leverandøren i henhold til nedenstående levere en detaljeret rapport samt en selvstændig erklæring, begge udarbejdet af det eksterne sikkerhedsfirma.
De dataansvarlige har en forpligtigelse til at føre tilsyn og har derfor ret til at få den selvstændige erklæring udleveret. I særlige tilfælde vil den detaljerede rapport blive forevist for den dataansvarlige, men ikke udleveret.

3. Omfang af penetrationstest

Testen skal indeholde følgende områder:

3.1 Information om systemet

- Risikovurdering af systemet
- Typer af informationer, der behandles af systemet – fx GDPR-oplysninger, forretningsdata
- Anvendt drift og hosting model
- Løbende sårbarhedsscanninger
- Anvendte redundante løsninger (spejlede miljøer)
- Dedikeret sikkerhedslog, revisionslog og deres integritetsbeskyttelse

3.2 Håndtering af data in transit

- Udstillede brugergrænseflader
- Udstillede services til andre systemer

3.3 Håndtering af data at rest

3.4 Håndtering af privatnøgler og certifikater

4. Udarbejdelse af penetrationstest

4.1 Opstartsmøde

Leverandører skal forinden påbegyndelse af penetrationstest sammen med KOMBIT og sikkerhedsfirmaet, på 3-partsmøder indkaldt af leverandøren, foretage nedenstående:

- Indledningsvist gennemgå det tekniske set up for systemet og driftsmiljøet med særligt fokus på de forhold, som er relevante i forbindelse med leverandørens leverancer under kontrakten med KOMBIT.
- Identificere og gennemgå det tekniske set up leveret af underleverandører.
- Med udgangspunkt i best practice detaljeret gennemgå og aftale, hvilke typer af penetrationstests som skal gennemføres ud fra sikkerhedsfirmaets anbefalinger.
- Indarbejde KOMBITs skriftlige ønsker til specifikke penetrationstests.
- Tilrettelægge en proces, som sikrer involvering af KOMBIT inden underskrift af erklæring vedr. sikkerheden for systemet og driftsmiljøet med henblik på at afklare eventuelle anmærkninger fra sikkerhedsfirmaet.

4.2 Detaljerede rapport

Den detaljerede rapport skal indeholde følgende:

- Detaljeret beskrivelse af de test, som er gennemført, med udgangspunkt af det aftalte omfang, herunder dato for gennemført tests
- Er der afdækket risici og/eller svagheder, herunder i relation til overholdelse af persondatalovgivningen, driftsmiljøet og/eller sikkerhedsprocedurer, skal disse detaljeret fremgå af rapporten
- Beskrivelse af nødvendige tiltag for at fjerne sikkerhedsrisici
- Erklæring på, om sikkerhedsfirmaet kan stå inde for sikkerheden for systemet og driftsmiljøet.
- Erklæringen skal være baseret på de standarder, som betragtes som best practice på området – eksempelvis OWASP og/eller PTES, anbefalinger fra Center for Cybersikkerhed.

4.3 Handlingsplan

Såfremt den detaljerede rapport indeholder bemærkninger, kommentering mv. om forbedringsområder for sikkerheden af systemet og driftsmiljøet, skal leverandøren samtidig med fremsendelsen af rapporten fremsende en fyldestgørende handlingsplan.

Kritikalitet af findings	**Håndtering**
Kritiske	Håndteres som Incident A og/eller jf. kontraktens bestemmelser
Høj	Lukkes indenfor max 60 dage
Medium	Leverandøren redegør håndteringen; månedlig opfølgning på driftsmøder

Handlingsplanen adresserer leverandørens håndtering af findings og KOMBIT verificerer om:

- leverandøren har fundet en løsning
- leverandøren har testet løsningen
- leverandøren har implementeret løsningen
- evt. exceptions redegørelse af de findings, der ikke skal håndteres.

5. Versionshistorik

Versions-nummer	Dato	Initialer & Enhed	Udarbejdelse / Ændringer	Godkendt af:
1.2	01/09/2023	Drift	Gennemgang	FIG
1.3	11/08/2026	Drift	Opdatering	FIG