

IB-ICT Input tav aanbesteding Werkplekken

1. Doel en uitgangspunt

Dit document beschrijft de kaderstellende input vanuit IB-ICT (Informatiebeveiliging ICT) ten behoeve van de aanbesteding van werkplekhardware.

Doel is te borgen dat de aan te besteden werkplekhardware:

- Aansluit op het geldende informatiebeveiligingsbeleid en de architectuurkaders;
- Gedurende de volledige lifecycle beheersbaar en veilig inzetbaar is;
- Geen onnodige security-, compliance- of continuïteitsrisico's introduceert.

IB-ICT levert met dit document kaders en minimale eisen, bedoeld voor opname in aansluitvoorwaarden en Programma van Eisen (PvE).

Dit document bevat geen detailontwerp, configuratie-instructies of leverancierskeuze.

2. Aansluitvoorwaarden (randvoorwaarden)

De aan te besteden werkplekhardware moet aantoonbaar kunnen aansluiten op de bestaande ICT- en security-inrichting van de organisatie.

2.1 Architectuur en security-baselines

- De hardware sluit aan op de vastgestelde doelarchitectuur voor de Moderne Werkplek.
- De hardware is compatibel met geldende security- en hardening-baselines.
- Afwijkingen van standaarden zijn niet toegestaan zonder expliciete goedkeuring.

2.2 Beheer en integratie

- De hardware is geschikt voor integratie met centrale device management-oplossingen.
- Ondersteuning voor integratie binnen de bestaande identity & access management (IAM)-inrichting.
- De hardware ondersteunt beveiligde configuratie en centraal beleid voor beveiligingsinstellingen.

2.3 Lifecycle management

- Er zijn duidelijke en afdwingbare afspraken over:
 - Firmware- en BIOS-updates;
 - Securitypatches;
 - End-of-life (EOL) en end-of-support (EOS).
- Gedurende de beoogde gebruiksduur wordt volledige security-ondersteuning geleverd.
- Er ontstaat geen afhankelijkheid van verouderde of niet-ondersteunde componenten.

2.4 Leveranciersketen en verantwoordelijkheid

- Transparantie over herkomst van hardware en kritische componenten.
- Tijdige levering van security-updates en kwetsbaarheidsinformatie.
- Duidelijke verantwoordelijkheden bij kwetsbaarheden, incidenten en noodzakelijke mitigerende maatregelen.

3. Security-eisen voor opname in het Programma van Eisen (PvE)

In het PvE worden minimaal de volgende security-eisen opgenomen. Deze eisen zijn toetsbaar, verifieerbaar en contractueel afdwingbaar.

3.1 Secure by design / secure by default

- De hardware ondersteunt een beveiligde configuratie vanaf ingebruikname.
- Onnodige of risicovolle functionaliteit kan standaard worden uitgeschakeld.
- De hardware kan zonder uitzonderingen worden opgenomen in de standaard werkplekinrichting.

3.2 Beveiligingsfunctionaliteit

Toelichting (niet normatief)

Ter illustratie kan bij de nadere uitwerking in het PvE gedacht worden aan het toepassen van business-grade werkplekapparatuur met gangbare beveiligingsvoorzieningen, zoals aanvullende BIOS-beveiliging, fysieke camerabescherming en ondersteuning van actuele beveiligingsstandaarden voor draadloze netwerken (bijv. WPA3). Dit betreft voorbeelden en geen uitputtende of productspecifieke eisen.

- Ondersteuning voor minimaal:
 - Device-encryptie;
 - Secure boot of gelijkwaardige beveiligingsmechanismen;
 - Beveiligde opslag van sleutels en credentials.

- Ondersteuning voor centrale logging en monitoring, waar van toepassing binnen de werkplekarchitectuur.

3.3 Beheerbaarheid en support

- De hardware is geschikt voor grootschalige en uniforme uitrol en beheer.
- De leverancier ondersteunt afhandeling van security-incidenten die de hardware raken.
- Heldere SLA's ten aanzien van:
 - Security-updates;
 - Beschikbaarheid van patches;
 - Reactietijden bij kwetsbaarheden.

3.4 Compliance en audit

- Security-eisen zijn concreet, meetbaar en toetsbaar geformuleerd.
- Open normen zonder verificatiecriteria worden vermeden.
- De leverancier faciliteert aantoonbaarheid richting audits en compliance-verantwoording.

4. Afbakening

Niet binnen de scope van deze aanbesteding en dit document vallen:

- De operationele beheerinstelling;
- Detailconfiguraties van werkplekken;
- Dagelijkse securityprocessen en monitoring.

Deze onderwerpen worden ingericht binnen bestaande beheer- en securityprocessen na gunning.

5. Resumerend

Door deze IB-ICT securitykaders vooraf expliciet mee te nemen in aansluitvoorwaarden en het PvE:

- Wordt herstelwerk en heronderhandeling na gunning voorkomen;
- Blijven security- en compliance-risico's beheersbaar;
- Ontstaat een toekomstbestendige en contractueel houdbare werkplekoplossing.