

Verzeichnis der IKT-Hardwareausstattung der Arbeitsplätze (IKT-HW-AusVz)

1. HW-Standardausstattung

In diesem Verzeichnis sind diejenigen IKT-Hardware-Komponenten aufgelistet, die zu der IKT-Standardausstattung der Arbeitsplätze gehören.

- Arbeitsplatz-Desktop-PC
- 22“-Bildschirm
- Tastatur und Maus
- DVD- bzw. CD-ROM-Laufwerk

Alternativ hierzu in dienstlich begründeten Fällen oder Telearbeit:

- Notebook (mit mindestens 14“ Display)
- Hard- und Software zur Ver- und Entschlüsselung und Einwahl in das BMBF-Netz
- 22“-Bildschirm
- Tastatur und Maus
- Transportmittel

2. Optionale HW-Ausstattung

In diesem Verzeichnis sind diejenigen IKT-Hardware-Komponenten aufgelistet, die zu der IKT-Standardausstattung einzelner Arbeitsplätze von der Dienststelle hinzugefügt werden können, ohne dass hierfür eine Beteiligung des Personalrates gemäß § 3ff DV-IKT erforderlich ist. Voraussetzung für die Bereitstellung dieser IT-Komponenten ist die dienstliche Notwendigkeit.

- CD/ DVD/Blu-ray-Brenner
- 23“-Bildschirm oder größer
- Netzwerkdrucker
- Scanner
- Fußschalter für Diktiersoftware
- Digitales Diktiergerät
- USB-Stick, externe Festplatte
- Smartphone, Tablet-PC
- Headset
- Braillezeile
- Funk-Maus/-Tastatur
- OWA-Token
- Smartcard Lesegeräte

3. Mobile HW-Ausstattung

In diesem Verzeichnis sind diejenigen IKT-Komponenten (Hardware) aufgelistet, die mobile Kommunikationsdienste per SIM-Karte (aktuell: UMTS-Technologie) nutzen.

Diese können zu der IKT-Ausstattung einzelner Arbeitsplätze von der Dienststelle hinzugefügt werden, ohne dass hierfür eine Beteiligung des Personalrates gemäß § 3ff DV-IKT erforderlich ist. Voraussetzung für die Bereitstellung dieser IKT-Komponenten ist die dienstliche Notwendigkeit.

- Notebook/Ultrabook
- Tablet-PC
- Smartphone

Alle Geräte werden nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie dem BMBF IT-Sicherheitskonzept gegen unbefugten Zugriff gesichert.

Die mobilen Endgeräte greifen verschlüsselt auf interne Ressourcen (z. B. Kontakte, E-Mail, Intranet) zu. Dabei wird sowohl die Sicherheit interner Ressourcen als auch die Kommunikationssicherheit und die Sicherheit der mobilen Endgeräte selbst gewährleistet.