1) Zugangskontrolle (Zutritt zum Raum)

Organisatorische Maßnahmen

- Raumbuchungspflicht (Kalendersystem), Räume nur für berechtigte Teams
- Teilnehmerlisten / Registrierung bei Schulungen und Veranstaltungen
- Regel „kein Zutritt ohne Einladung“ + sichtbare Hinweise am Eingang

Technische/Physische Maßnahmen

- Raumzugang über Schließsystem / Transponder / Code
- Besucher nur mit Begleitung, ggf. Besucherbadge
- Fenster/Türen schließen, gerade bei vertraulichen Meetings

2) Benutzer- und Zugriffskontrolle (IT & Präsentationstechnik)

Maßnahmen

- Präsentations-PC / Konferenzsystem mit Benutzerkonten und Rollen
- Anmeldung nur via:
    - Firmenkonto (SSO / Azure AD / AD)
    - oder separater Gastmodus (ohne Zugriff auf interne Daten)
- Automatische Bildschirmsperre nach X Minuten
- Keine „shared“ Accounts ohne Nachvollziehbarkeit

3) Übertragungskontrolle

Maßnahmen

- Trennung in:
    - internes Netz
    - Gast-WLAN
- Gast-WLAN:
    - eigenes VLAN
    - Captive Portal / Voucher
    - keine Sichtbarkeit interner Systeme (Client Isolation)
- LAN-Ports deaktiviert
- Videokonferenzen nur über verschlüsselte Protokolle (TLS/SRTP)

4) Eingabekontrolle & Nachvollziehbarkeit

Maßnahmen

- Konferenz-PC protokolliert:
    - Login/Logout
    - Geräteverbindungen (USB/HDMI)
- Dokumente und Präsentationen in Systemen mit:
    - Versionierung
    - Zugriffsprotokoll
- Videokonferenz:
    - Meeting-Links nicht öffentlich
    - Warteraum / Lobby aktivieren
    - Host kontrolliert Teilnehmer

5) Verfügbarkeitskontrolle & Wiederherstellbarkeit

Maßnahmen

- Präsentationstechnik standardisiert:
    - Ersatzkabel, Adapter, Presenter
- Geräte regelmäßig gewartet:
    - Updates
    - Funktionscheck