Anlage ./1 – Technisch-Organisatorische Maßnahmen

VERTRAULICHKEIT

- **Zutrittskontrolle:**
  Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen
  Gewährleistet durch Schlüssel, Alarmanlage und Videoüberwachung
- **Zugangskontrolle**:
  Schutz vor unbefugter Systembenutzung
  Kennwörter (einschließlich entsprechender Policy für automatische Sperrung bei Brute Force Attacken o.ä.), Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern bzw. Passwortdateien
- **Zugriffskontrolle**:
  Ein unbefugter Zugriff ist durch Policy für automatische Sperrung und Zwei-Faktor Authentifizierung sämtlicher Administrativer Accounts gewährleistet
- **Pseudonymisierung**:
  Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.
- **Klassifikationsschema für Daten:**
  Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

INTEGRITÄT

- **Weitergabekontrolle**:
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport:
  Verschlüsselung von übertragenen Dateien, Virtual Private Networks (VPN) für Zugriffe von extern, elektronische Signatur für Rechnungen
- **Eingabekontrolle**:
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:
  Diese Daten werden ausschließlich vom Eigentümer bearbeitet

VERFÜGBARKEIT UND BELASTBARKEIT

- **Verfügbarkeitskontrolle**:
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:
  Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Mehrstufiges Sicherungskonzept mit Auslagerung der Sicherungen an zweiten Bürostandort (die Datenübertragung erfolgt verschlüsselt)
- Rasche **Wiederherstellbarkeit**
  im Deseasterfall innerhalb von 24 Stunden
- **Löschungsfristen**:
  Sowohl für Daten selbst als auch Metadaten wie Logfiles
  Daten werden nach Ablauf der gesetzlichen Aufbewahrungsfristen gelöscht.

VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen