## EINSATZ VON FAX-, DRUCK- UND KOPIERGERÄTEN

**1.** Fax-, Druck- und Kopiergeräte sollten so platziert sein, dass Unbefugte keine Möglichkeit erhalten Einsicht bzw. Zugriff durch das Lesen oder Senden von Informationen zu nehmen.

**2.** Im Rahmen des Datenschutzgeheimnisses (§ 53 DSAnpUG-EU/BDSG n.F.; § 5 BDSG a.F.) und Fernmeldegeheimnisses (§ 88 TGK) sind Faxe, Drucke oder Kopien, dazu zählen auch die Sende- und Empfangsprotokolle, sorgsam zu verwahren (z.B. in Abwesenheit - keine personenbezogenen Daten sichtbar auf dem Schreibtisch).

**3.** Beim Versenden eines Faxes oder eines eingescannten Druckes per E-Mail-Anhang ist die eingegebene Nummer bzw. die E-Mail-Adresse nochmals auf Richtigkeit zu überprüfen.

**4.** Die Möglichkeit einer zeitversetzten Versendung per Faxgerät sollte grundsätzlich nicht genutzt werden, da Fehleingaben schlechter rekonstruiert werden können.

**5.** Im Vorfeld an eine Faxübersendung sollte sich über die datenschutzrechtlichen Handhabungen mit dem Empfänger des Faxes verständigt worden sein (z.B. Zulässigkeit einer Faxübermittlung, vorheriger Anruf).

**6.** Sensible personenbezogene Daten sollten grundsätzlich nicht mit dem Faxgerät oder in Form eines eingescannten Druckes als Anhang mit unverschlüsselter E-Mail übermittelt werden.

**7.** Es ist sinnvoll konkrete Nutzungsbedingungen für das Faxgerät festzulegen und den Mitarbeiter in einer Einweisung zu vermitteln.

**8.** Falls die Möglichkeit besteht, sollte die Ausgabe bei Sammelgeräten mit einer Autorisierung mittels Pin oder Chip verknüpft werden. Ansonsten sind die Faxe, Drucke oder Kopien schnellstmöglich abzuholen, auch Falschdrucke sind abzuholen und selbständig ordnungsgemäß zu entsorgen.

**9.** Hinweise für die Administration:

- Die Standardpasswörter mit denen die Geräte beim Hersteller ausgeliefert werden müssen geändert werden (das Wartungs-/Servicepasswort sollte mit Masterpasswort geschützt werden).

- Es dürfen nur solche Dienste nach dem konkreten Einsatzzweck aktiviert sein und nichtbenötigte Netzwerkdienste sind zu deaktivieren.
- Die Datenspeicherung sollte möglichst verschlüsselt erfolgen (z.B. bei einem Diebstahl wären die Daten dann geschützt) - Security Kit.
- Daten auf den Geräten sollten im internen Speicher automatisch gelöscht werden, wenn diese nicht mehr benötigt werden.
- Weiterhin sollten regelmäßige Sicherheitsupdates durchgeführt werden, wenn der Drucker im Computernetzwerk betrieben wird.
- Entsprechende Hilfestellungen können beim Bundesamt für Sicherheit in der Informationstechnik (BSI) abgerufen werden unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b03/b03406.html.