Merkblatt für den Arbeitsplatz des Telearbeiters

Die sicherheitstechnischen Anforderungen an den Telearbeitsplatz richten sich nach dem Schutzbedarf der zu bearbeitenden Daten am Telearbeitsplatz. Je höher der Schutzbedarf, desto mehr Maßnahmen müssen ergriffen werden, um diesen Schutz zu gewährleisten. Allgemein ist sicherzustellen, daß am Arbeitsplatz des Telearbeiters und bei der Kommunikation zwischen Institution und Telearbeitsplatz die Vertraulichkeit der Daten gewährleistet ist, die Zugriffsmöglichkeiten auf betriebliche Daten von zu Hause aus nur Befugten ermöglicht wird und die zu Hause befindlichen dienstlichen Unterlagen hinreichend geschützt werden.

Schutz am Arbeitsplatz:

- Schützen des PC vor Unbefugten (einschließlich Familienangehörige), wenn möglich in einem abschließbaren Raum.
- Nutzen vorhandener Schutzmöglichkeiten für den PC (z. B. Abschließen des PC, Abschließen der Diskettenlaufwerke).
- Nutzen der vorhandenen Sicherheitsmaßnahmen im PC (z. B. Einsetzen von Paßwörter, falls vorhanden: Verschlüsselungsprogramme), um den Zugriff nicht autorisierter Personen auf die Daten im PC zu verhindern.
- Kein Einsatz von privater Soft- und Hardware.
- Regelmäßige Kontrolle durch Virensuchprogramme inkl. Makroviren.
- Regelmäßige Datensicherungen. Eine Generation der Datensicherung sollte aus Gründen der Verfügbarkeit in der Institution aufbewahrt werden.
- Sicheres Löschen nicht benötigter Daten und geregelte Entsorgung von Datenträgern.
- Sichere Aufbewahrung der Akten und Datenträger in verschließbaren Behältern, um die Einsichtnahme durch Unbefugte zu verhindern, aber auch Diebstahl oder die willentliche Beschädigung von Akten und/oder Datenträgern.
- Sicherer Aktentransport zwischen häuslichem Arbeitsplatz und Institution.
- Einhalten der einschlägigen Datenschutzvorschriften.
- Sofortiges Melden von Sicherheitsvorkommnissen an die systembetreuende Stelle oder dem IT-Sicherheitsbeauftragten.

Schutz bei der Übertragung von Daten:

- Schutz der zu übertragenen Daten vom Telearbeitsplatz zur Institution oder umgekehrt durch vorhandene oder zusätzlich installierte Soft- oder Hardware (z. B. durch Verschlüsselung der Daten).
- Überprüfen der neu eingegangen Daten mit Hilfe eines Virensuchprogramms inkl. Makroviren.
- Einhalten der festgelegten Datenübertragungswege (z. B. keine Datenübertragung über das Internet, wenn es eine eigene Übertragungsleitung zur Institution gibt).
- Sofortiges Melden von Sicherheitsvorkommnissen an die systembetreuende Stelle oder dem IT-Sicherheitsbeauftragten.