Anlage: „Technische und organisatorische Maßnahmen zum Datenschutz“.

Vertraulichkeit:

Zutrittskontrolle
Digitales Schließsystem - Dokumentation der Vergabe von Schüsseln
Gesonderte Zutrittskontrolle für Räume mit kritischer IT-Infrastruktur (zusätzliche Schlüssel)
Rückgabe von Schüsseln nach Austritt von Mitarbeitern
Verwendung einer Video-Überwachung (relevante Flure, Eingangsbereich)
Verwendung einer Zutrittskontrolle bei Nacht
Verwendung sicherer Türen und Fenster

Zugangskontrolle
Anwendung von Maßnahmen zur Verschlüsselung von lokalen Daten
Automatisches Sperren von PCs nach 10 Minuten
Verwendung personalisierter Logins im Unternehmensnetzwerk
Verwendung sicherer und individueller Passwörter

Zugriffskontrolle
Dokumentation eingerichteter Zugänge für Mitarbeiter
Einführung von Benutzer- und Rollenkonzepten für interne Systeme
Sperrung von Zugängen nach Austritt von Mitarbeitern
Zentrale Verwaltung von Benutzerzugängen und -rechten

Weitergabekontrolle
Nutzung SSL-verschlüsselter Übertragungswege im Internet
Sicherung von Dokumenten beim Versand auf dem Postweg
Verschlüsselter Versand von E-Mails
Verwendung von VPN-Systemen zum Login in das Firmennetzwerk (innerhalb Organschaft)

Trennungskontrolle
Einführung von Zugriffsberechtigungen für interne Systeme
Trennung von internem WLAN und Gäste-WLAN

Verschlüsselung
Verwendung verschlüsselter Übertragungswege für den Datenaustausch
Verwendung von Maßnahmen zur verschlüsselten Datenspeicherung
Verwendung von SSL-Zertifikaten für Hostingumgebungen

Integrität

Eingabekontrolle
Einführung von Benutzer- und Rollenkonzepten für interne Systeme
Einführung individueller Zugänge für interne Systeme
Protokollierung von Zugriffen im Firmennetzwerk
Verwendung personalisierter Logins im Unternehmensnetzwerk

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle
Klimatisierung von Räumen mit kritischer IT-Infrastruktur
Regelmäßige Aktualisierung der Virendefinitionen
Regelmäßige Durchführung von Datensicherungen
Regelmäßige Durchführung von Updates
Regelmäßige Überprüfung der erstellten Datensicherungen
Verwendung einer Brandmeldeanlage
Verwendung einer Firewall (Sophos)
Verwendung eines Virenscanners (ESET)
Verwendung einer unterbrechungsfreien Stromversorgung (USV) für interne Systeme
Verwendung eines Überspannungsschutzes für interne Systeme
Verwendung von RAID-Systemen

Rasche Wiederherstellbarkeit
Dokumentation und Test von Datenwiederherstellungen
Erstellung von Notfallplänen zu kritischen Prozesse

Weitere Maßnahmen

Datenschutz-Managementsystem
Dokumentation von datenschutzrelevanten Zwischenfällen
Löschen nicht mehr benötigter Daten
Sichere Entsorgung defekter/nicht mehr benötigter Hardware
Sichere Entsorgung von Dokumenten
Zuteilung von datenschutzrelevanten Verantwortungsbereichen gem. Organigramm

Auftragskontrolle
Abschluss von AV-Verträgen mit Dienstleistern, Partnern und Kunden
Auswahl geeigneter Dienstleister und Partner unter Datenschutzaspekten
Beauftragung zertifizierter Dienstleister
Benennung eines Datenschutzbeauftragten
Beratung/Aufklärung der Kunden zum Thema Datenschutz
Durchführung von stichprobenartigen Überprüfungen bei Dienstleistern
Kommunikation von Verhaltensrichtlinien zum Thema Datenschutz an alle Mitarbeiter
Regelmäßige Unterweisung und Fortbildung der Mitarbeiter zum Thema Datenschutz
Unterzeichnung einer Verschwiegenheitserklärung durch alle Mitarbeiter