3. Checkliste Zugangskontrolle

Abkürzungen: erf. = erfüllt, nicht erf. = nicht erfüllt, nicht erfdl. = nicht erforderlich / nicht zutreffend

Vorgabe		**erf.**	**nicht erf.**	**nicht erfdl.**	**Bemerkungen**
Zugangskontrolle					
3.1	**Passwortverfahren**				
3.1.1	Forderung einer unterschiedlichen Zeichenzusammensetzung	x			Groß- und Kleinschreibung, Zahlen
3.1.2	Mindestlänge 8 Zeichen	x			> 8 Zeichen
3.1.3	Regelmäßiger Wechsel	x			360 Tage
3.1.4	Erstanmeldeprozedur	x			Vergabe des ersten Passwortes durch Administratoren. Aufforderung zur Änderung durch System (GPO-Richtlinie)
3.1.5	Bildschirmsperre bei Pausen mit Passwort-Aktivierung	x			nach 5 Minuten
3.1.6	Zugangssperre bei mehr als 3 Anmeldeversuchen	x			Protokollierung über Eventlog / Zugriffsprotokoll
3.1.7	Passworthistorie	x			Historie 3 Passwörter
3.1.8	Verwendung Gruppen-Passwörter		x		Gruppen DTP & Druck gemeinsamer Zugriff, jedoch nicht auf personenbezogene Daten
3.1.9	Richtlinie, Merkblatt		x		
3.1.10	Aufbewahrung Administrator-Passwörter		x		Administrator Passwörter sind den Administratoren bekannt und nicht dokumentiert
3.1.11	Einmal-Passwörter			x	
3.1.12	BIOS-Passwörter			x	
3.1.13	Boot-Passwörter			x	
3.1.14	Single-Sign-On (SSO)?	x			Active Directory Anmeldung
3.2	**Andere Verfahren**				
3.2.1	Biometrische Verfahren (one-to-one)			x	
3.2.2	Biometrische Verfahren (one-to-many)			x	
3.2.3	Elektronische Signatur	x			z.T. im Email Verkehr, Clientseitig installiert
3.2.4	Chipkarten			x	PIN-Vergabe und -Änderung?
3.2.5	Magnetkarten			x	
3.2.6	Transponderkarten			x	
3.3	**Protokollierung des Zugangs (An-/Abmeldung)**	x			
3.4	Verschlüsselung mobiler Datenträger/Festplatten			x	
3.5	Zugang von außerhalb des Intranets	x			über verschlüsseltes Gateway
3.6	Wie erfolgt der Zugang ins Internet?				Glasfaser synchrone Anbindung, direkt über Router/Firewall

Vorgabe		**erf.**	**nicht erf.**	**nicht erfdl.**	**Bemerkungen**
3.6.1	Kommunikationsserver			x	
3.6.2	Proxy-Server			x	
3.6.2.1	Vergabe der Accounts?			x	
3.6.2.2	Verwaltung der Passwörter?			x	
3.6.3	Wechsel des Betriebssystems			x	
3.6.4	Wechsel zu einem Live-Betriebssystem (read only)			x	
3.6.5	Stand-alone-PC			x	
3.6.6	Ohne Schließen der aktiven Anwendung	x			
3.7	**Welcher Internet-Provider wird genutzt?**				
3.7.1	Corporate Network			x	
3.7.2	Internet-Provider (direkt)	x			Unitymedia
3.7.3	Dienstleister (Hosting)	x			Hosteurope
3.8	**Verwendete Technik**				
3.8.1	ISDN			x	
3.8.1.1	Karte			x	
3.8.1.2	Modem			x	
3.8.1.3	Router			x	
3.8.2	DSL			x	
3.8.2.1	Karte			x	
3.8.2.2	Modem			x	
3.8.2.3	Router	x			Router / Firewall Bintec, Glasfaser-Direktanbindung
3.9	**Firewall**				
3.9.1	Betreuung durch Dienstleister			x	
3.9.2	Zugriffsberechtigungskonzept	x			
3.9.3	Verantwortlich für Regelwerk	x			GF
3.9.3.1	Änderungsberechtigungen	x			Änderung nur durch Geschäftsführer
3.9.3.2	Nachvollziehbarkeit von Regeländerungen	x			Dokumentation
3.9.3.3	Prüfung des Regelwerks			x	Geringes Regelwerk
3.9.4	Proxy-Server mit Software-Firewall			x	
3.9.5	Software-Firewall	x			Trendmicro / Windows Firewall
3.9.6	Hardware-Firewall (Appliance)			x	
3.9.7	Hersteller			x	
3.9.7.1	Support und Wartung (Fernwartung?)	x			Keine Fremdwartung
3.9.8	Wie oft werden Updates installiert?				
3.9.8.1	Laufend, automatisiertes Verfahren	x			Clients, Windows Update Server
3.9.8.2	Laufend, manuell	x			Cluster-Nodes, Apple PCs
3.9.9	Wie werden Sicherheitslücken gehandhabt?	x			Trendmicro Security Advisor, OPENVAS
3.9.9.1	Benachrichtigung durch wen? automatisiert				

Vorgabe		**erf.**	**nicht erf.**	**nicht erfdl.**	**Bemerkungen**
3.9.9.1.1	Regelmäßig, automatisiertes Verfahren	x			Trendmicro, OpenVAS, Auto-Updates
3.9.9.1.2	Regelmäßig, manuell	x			Monatlich, Security Updates auf Serverfarm
3.9.9.1.3	Manuell			x	
3.9.9.2	Einspielung Sicherheitspatches				
3.9.9.2.1	Laufend, automatisiertes Verfahren	x			Clients
3.9.9.2.2	Laufend, manuell	x			Server, Clusternodes, Apple PCs
3.9.10	Getrennte Administration der Komponenten?	x			Betriebssystem, Firewall
3.10	**Welcher Browser wird genutzt?**	x			Mozilla, Internet Explorer, Safari, Chrome, Edge
3.10.1	Wie oft werden Sicherheitspatches und/oder Updates installiert?				
3.10.1.1	Laufend, automatisiertes Verfahren	x			laufend, Update Server, 2x täglich synchronisiert
3.10.1.2	Laufend, manuell	x			Apple PCs monatlich
3.10.2	Verwaltung der Konfiguration?				
3.10.2.1	Durch Administration	x			
3.10.2.2	Durch Nutzer			x	IE: Sperrung durch Richtlinie
3.11	**Werden Sicherheitseinstellungen durch Penetrationstests regelmäßig überprüft?**	x			Ja, ca. alle 30 Tage openvas
3.12	**Systemadministration**				
3.12.1	Administrationsrichtlinie			x	
3.12.2	Administratoren sind tätig...				
3.12.2.1	...hauptamtlich			x	
3.12.2.2	...nebenamtlich	x			nur 2 Administratoren, GF + IT-Sicherheitsbeauftragter
3.12.2.3	...extern			x	
3.12.3	Aufgabenbezogene systemtechnische Trennung bei mehreren Administratoren			x	
3.12.4	Spezielle Passwortkonventionen zur Administration (abweichend von Nutzer-Passwörter)			x	
3.12.5	Getrennte Benutzerkonten für Systemadministration, Sachbearbeitung, persönlichen Nutzungen	x			
3.12.6	Anwendung des 4-Augen-Prinzips			x	
3.12.7	Protokollierung der Administrationsarbeit	x			
3.12.7.1	Protokoll-Server		x		
3.12.7.2	Eigener Protokoll-Bereich		x		
3.12.7.3	Vorkehrungen gegen Protokollmanipulation		x		
3.12.7.4	Wer wertet Protokolle ggf. aus?	x			Anlassbezogen durch Administratoren

Vorgabe		erf.	nicht erf.	nicht erfdl.	Bemerkungen
3.12.8	Sind Notfallpasswörter hinterlegt?			x	