TU Dresden
Stabsstelle für Informationssicherheit
Tel.: 0351 463 32839
Fax: 0351 463 39718
E-Mail: informationssicherheit@tu-dresden.de

Stabsstelle für Informationssicherheit

Antrag: Freischaltung in der zentralen Firewall

Struktureinheit		
Antragsteller	Name:	
	E-Mail:	Telefon:
Verantwortlicher Leiter	Name:	
	E-Mail:	Telefon:
Zuständiger Administrator (wenn nicht Antragsteller)	Name:	
	E-Mail:	Telefon:
Vertreter des Administrators	Name:	
	E-Mail:	Telefon:

Kurzbeschreibung des Dienstes

Vorgesehener Nutzerkreis		
DNS-Name(n)		
Benötigte Ports (z.B. TCP/443)		
Zeitliche Befristung	○ ja ○ nein	wenn ja, bis:
Verarbeitung personenbezogener Daten	○ ja ○ nein	
Maßnahmen zum IT-Grundschutz berücksichtigt (siehe Anlage)	○ ja ○ nein	

Unterschrift Antragsteller

Unterschrift verantwortlicher Leiter

Unterschrift Bereichs-Administrator

Genehmigung der Stabstelle für Informationssicherheit

Erledigungsvermerk des ZIH Datum, Unterschrift

Ist die geeignete Aufstellung des Servers gewährleistet?

Prüffragen	
Ist der Server im ZIH, Serverräumen oder abschließbaren Serverschränken aufgestellt?	☐
Existiert eine angemessene Zutrittsregelung zu den Serverräumen bzw. Serverschränken?	☐
Existiert eine angemessene Unterbrechungsfreie Stromversorgung (USV)?	☐
Anmerkungen	

Sind Berechtigungen / Zugangs- und Zugriffe hinreichend geregelt und technisch umgesetzt?

Prüffragen	
Existiert eine angemessene Benutzerverwaltung und Passwortrichtlinie?	☐
Existiert ein Berechtigungskonzept?	☐
Für Webserver: Wurde geprüft, ob Shibboleth eingesetzt werden kann?	☐
Anmerkungen	

Ist die Kommunikation ausreichend abgesichert?

Prüffragen	
Ist die Kommunikation zwischen Client und Server geschützt, bei Webservern mit https verschlüsselt?	☐
Werden Zertifikate der DFN-PKI verwendet?	☐
Anmerkungen	

Ist die Administration ausreichend abgesichert?

Prüffragen	
Ist eine sichere Administration über das Datennetz bzw. lokale Konsole, sowie im Server gewährleiste	☐
Sind abhängig von der genutzten Zugriffsart geeignete Sicherheitsvorkehrungen, z.B. 2- Faktor-Authentifizierung, getroffen worden?	☐
Anmerkungen	

Ist eine sichere Grundkonfiguration gewährleistet?

Prüffragen	
Ist die Software aus vertrauenswürdigen Quellen installiert worden?	☐
Sind ausschließlich die zwingend erforderlichen Dienste und Softwarekomponenten installiert und sicher konfiguriert?	☐
Ist der Grundsatz „Ein Dienst pro Server“ eingehalten worden?	☐
Wurde eine Regelung zur Protokollierung getroffen und implementiert (Speicherfristen)?	☐
Wurden alle Standardpasswörter geändert?	☐
Wird die Veröffentlichung von internen Serverinformationen restriktiv gehandhabt?	☐
Anmerkungen	

Erfolgt eine regelmäßige Schwachstellenprüfung und ist das Patch-Management ausreichend bestimmt und technisch umgesetzt?

Prüffragen	
Findet eine regelmäßige Prüfung auf Schwachstellen und sowie die Einleitung entsprechender Maßnahmen zur Behebung statt (Empfehlung: Einsatz des Greenbone Security Managers (GSM))?	☐
Wurde eine Regelung zum Umgang mit Patches und Updates getroffen und implementiert?	☐
Anmerkungen	

Existiert eine geeignete Netzinfrastruktur?

Prüffragen	
Wird der Server in einer Demilitarisierten Zone (DMZ) betrieben?	☐
Existiert eine strukturierte und geregelte Vergabe von IP-Adressen und Server-Namen(DNS)?	☐
Wurde der DNS-Name über das ZIH registriert?	☐
Anmerkungen	

Existieren ein Notfallplan und eine Dokumentation?

Prüffragen	
Sind eine aussagefähige Beschreibung und Regelung von Notfällen, um die Folgen eines Ausfalls (personell, technisch) zu minimieren, vorhanden?	☐
Liegt eine hinreichende Dokumentation der Server- und Netzinfrastruktur vor?	☐
Anmerkungen	

Werden personenbeziehbare Daten verarbeitet?

Prüffragen	
Liegt eine Verfahrensbeschreibung nach § 10 SächsDSG vor?	☐
Anmerkungen	