# Technische und Organisatorische Maßnahmen (TOMs)

## TOMs der ITEG IT-Engineers GmbH

### Version 1.1 vom 4.6.2025

Hinweis: PDF-Downloads aller veröffentlichten Versionen finden sich am Beginn von Vereinbarungen über ITEG-Hosting als Auftragsverarbeitung nach Art. 28 DSGVO.

### Einleitung

Im Jahr 2018 hat ITEG IT-Engineers GmbH auf Basis der immer schon gelebten sicheren Prinzipien ein formelles Informationssicherheitsmanagement eingeführt. Dazu gehört diese DSGVO-konforme Liste der Technischen und Organisatorischen Maßnahmen (TOMs).

Am 18.12.2028 wurden unser Informationssicherheitsmanagement erfolgreich nach ISO-27001 zertifiziert. Ende 2022 wurde das wegen Unfinanzierbarkeit und teilweiser inhaltlicher Sinnlosigkeit wieder fallengelassen, die Informationssicherheit und diese TOMs werden aber weiter gelebt.

### Zugangskontrolle

Alle Hosting-Server befinden sich in Datencentern mit elektronischer Zutrittskontrolle sowie Videoüberwachung.

Die verschlüsselten Offline-Backups werden in einem versperrten Stahlschrank im ITEG-Büro aufbewahrt.

### Datenträgerkontrolle

Unverschlüsselt werden die Hosting-Daten nur auf den internen Festplatten der jeweiligen Server gespeichert.

Alle Backup-Spiegel (in 2 bis 3 Datacentern und im ITEG-Büro) sind verschlüsselt.

Die einzigen mobilen Datenträger, die externen Backup-Medien, sind verschlüsselt und werden in einem versperrten Stahlschrank gelagert.

### Benutzerkontrolle und Zugriffskontrolle

Die Daten-Verzeichnisse und Datenbanken verschiedener Shared-Hosting-Kunden sind vor gegenseitigem Zugriff durch entsprechende Vergabe der Verzeichnis-Berechtigungen geschützt. Dies wird gelegentlich überprüft.

Bei virtuellen Root-Hosts werden verschiedene Bereiche die von verschiedenen Webagenturen bzw. Entwicklern betreut werden nach Möglichkeit nach dem gleichen Schema vor gegenseitigem Zugriff geschützt.

Über Administratorenrechte auf physischen Hosts und virtuellen Server verfügen ITEG-seitig nur die beiden Geschäftsführer sowie ein angestellter System-Administrator, die sich alle ausschliesslich mit PIN-geschützten Hardware-Token (yubikey) einloggen können. Der Fern-Zugriff auf Server ist außerdem auf bestimmte Client-IP-Adressen (ITEG-Büro, Wohnung des CIO, ...) eingeschränkt.

Auf virtuellen Root-Hosts haben teilweise auch die jeweiligen Kunden (die Verwantwortlichen) bzw. von den Verantwortlichen beauftragte volle Administratorenrechte und sind für die Benutzerkontrolle mitverantwortlich.

Zugriff auf virtuelle Roothosts ist generell nur mit SSH möglich, FTP wird nur auf ausdrücklichen Wunsch ermöglicht und bei neuen Servern ab 2025 gar nicht mehr.

### Übertragungskontrolle, Eingabekontrolle

Die einzigen von ITEG durchgeführten Übertragungen erfolgen im Rahmen des Backups. Das nächtiche Backup auf ITEG-eigene Backup-Server wird geloggt, die Aktualisierung der externen Generationen-Backups wird intern und auf den Medien dokumentiert.

### Transportkontrolle

Der Transport von Daten zwischen ITEG-Systemen, z.B. imzuge der nächtlichen Backups, erfolgt ausschließlich SSH- bzw. HTTPS-verschlüsselt.

Die einzigen mobilen Datenträger, die externen Backup-Medien, sind LUKS-verschlüsselt bzw. Proxmox-verschlüsselt und werden - außer zur Aktualisierung des Backup-Standes - immer in einem versperrten Stahlschrank gelagert.

### Wiederherstellung

Alle Daten (Dateien, Datenbanken als Dumps) werden nächtlich auf einen Backup-Space gesichert der wiederum auf einen 2. Backup-Standort gespiegelt wird von dem aus 6 verschlüsselte externe Backup-Medien (je 2 Wochen-, Monats- und Jahres-Stände) befüllt werden.

Die Wiederherstellbarkeit von Daten aus den Backups wird durch entsprechende Kundenanfragen regelmäßig geprüft.

Parallel dazu erfolgen Vollsicherungen aller relevanten virtuellen Server auf 3 gegenseitig spiegelnde Proxmox Backup Server (und 2 externe Backup-Medien), wobei diese Backups individuell pro Proxmox-Cluster verschlüsselt sind.

### Datenintegrität

Auf den meisten Servern werden vom Hersteller verfügbare Sicherheitsupdates nächtlich automatisch eingespielt. Auf allen Servern werden mindestens einmal im Monat die vom Hersteller verfügbaren Sicherheitsupdates manuell eingespielt und etwaige Probleme mit Updates erkannt und behoben.

Bei Bekanntwerden von kritischen Lücken (die eine unberechtigte Übernahme von Systemen aus der Ferne ermöglichen) erfolgt die Absicherung binnen 24 h, durch Einspielen der entsprechenden Updates oder ggfs. durch Konfigurationsanpassungen.

## Disclaimer Alt-Software Betriebssysteme

Beim den für Hosting eingesetzten Betriebssystemen, Debian Linux und Ubuntu Linux, wird jede Generation nur für ca. 5 Jahre mit Updates versorgt. Gehostete Kundendienste (Webanwendungen, ...) müssen daher regelmäßig auf neuere virtuelle Server migriert werden um weiterhin sicher genug zu sein.

Für die Verarbeitung von Personenbezogenen Daten auf nicht mehr mit Sicherheits-Updates versorgten Betriebssystemen übernimmt ITEG keinerlei Verwantwortung.

Die Migration von bei ITEG gehosteten Projekten auf neuere Betriebssystem-Generationen wird von ITEG kostenlos durchgeführt und begleitet.

### Update 2025, Lösung durch Dockerisierung

Seit Herbst 2023 läuft die Umstellung von klassischem LAMP-Hosting auf Docker-Umgebungen, sodass Webserver, Datenbank-Server, PHP-FPM u.s.w. nicht mehr vom Betriebssystemhersteller sondern von den eigentlichen Herstellern kommen und unabhängig vom Betriebssysteme upgedatet und ggfs. in verschiedenen Versionen parallel betrieben werden können.

Dadurch entfällt künftig die ca. 4-jährliche Migration auf neuere Server.

### Disclaimer Web-Anwendungen

Bei allen häufig eingesetzten Frameworks (WordPress, Typo3, u.v.a.) werden regelmäßig Sicherheitslücken bekannt die nur durch Zeitnahe bzw. regelmäßige Updates der Frameworks geschlossen werden können bzw. müssen.
Auch individuell programmierte Web-Anwendungen enthalten oft typische Sicherheitslücken.
Die Zuständigkeit für diese Bereiche liegt beim Auftraggeber bzw. Verantwortlichen und es wird dringend zu entsprechenden Wartungsvereinbarungen mit den beauftragten Webagenturen geraten.

Eine Liste typischer Fehler bzw. Problembereiche samt Lösungsstrategien findet sich in den OWASP Top Ten auf https://www.owasp.org/.