

## Sicherheitsmaßnahmen

Unser durchgängiges Sicherheitskonzept entspricht höchstem Standard und ermöglicht bei größtmöglicher Sicherheit dennoch bequemes Arbeiten.

### Rechenzentrum

AirITSystems betreibt die AWARO.NET®-Server in einem hochmodernen, nach ISO 27001 zertifizierten Rechenzentrum der TelecityGroup in Frankfurt, das höchsten Sicherheitsanforderungen genügt. Es verfügt über strenge Zugangskontrollen, aufwendige Brandschutzeinrichtungen, Klimaüberwachung, unterbrechungsfreie Stromversorgung mit Dieselgeneratoren, ausfallsichere redundante Mehrfach-Internetverbindungen und wird rund um die Uhr überwacht.

### Technische Serverspezifikation

Wir setzen ausschließlich professionelle Serverhardware ein.

Betriebssystem: **RedHat Enterprise Linux**

Datenbank: **Oracle™**

Application Server: **Apache Tomcat**

Webserver: **Apache HTTP Server**

### Firewall, Sicherheitsupdates, Monitoring

Die AWARO.NET®-Systeme sind zuverlässig durch Firewalls geschützt und werden ständig auf aktuellem Patch-Level gehalten. Mit auf Zuverlässigkeit optimierter Technik mit vollständig redundanter Serverhardware und einem automatisierten 24x7-Monitoring der wichtigsten Serverfunktionen erreichen wir aktuell Verfügbarkeiten von weit über 99%. Eventuell auftretende Probleme werden rund um die Uhr an unsere Administration gemeldet und umgehend beseitigt.

### Backup

Wir setzen in unseren Servern grundsätzlich per RAID gespiegelte Festplatten ein. Die Daten werden stündlich auf einem On-Site-Backupsystem gesichert und täglich in einem räumlich getrennten Rechenzentrum in Hannover auf Bandmedien gespeichert.

### Verschlüsselung

Die gesamte Kommunikation zwischen den AWARO.NET®-Servern und Ihrem Rechner wird über TLS (Transport Layer Security, früher SSL genannt) mit mindestens 128-Bit Schlüssellänge verschlüsselt. Schon die Anmeldung erfolgt verschlüsselt, so dass kein Passwort im Klartext übertragen wird. Die Anmeldung erfolgt über einen Aktivierungscode, der nach der Registrierung verfällt. Auf Wunsch kann die Aktivierung auch per Fax, Brief oder persönlich abgewickelt werden, um Versand von Zugangsdaten per E-Mail zu vermeiden.

Dateien werden nach dem Hochladen automatisch mit dem Verschlüsselungsalgorithmus „Blowfish“ verschlüsselt. Somit sind die Daten selbst auf Backups oder bei unbefugtem Zugriff auf das Dateisystem der Server zuverlässig gesichert.

### Passwortsicherheit

Bei der Passwortvergabe werden sowohl die Länge als auch die Komplexität geprüft. Zugänge werden nach mehreren Fehlversuchen temporär gesperrt. Die Speicherung der Passwörter erfolgt ausschließlich in verschlüsselter Form.

### Virenprüfung

Jede Datei wird vor der Ablage in AWARO.NET® auf Virenbefall überprüft und befallene Dateien abgelehnt. Virendefinitionen werden spätestens vier Stunden nach Erscheinen aktualisiert.

### Revisionssichere Änderungsverfolgung

Jeder Zugriff auf das System wird registriert und bis zu einzelnen Lesezugriffen auf Dokumente und Nachrichten protokolliert. Alle vorhandenen Versionen und Arbeitsstände eines Dokuments können lückenlos nachvollzogen werden. Ein einzigartiges, leistungsfähiges Rechtekonzept stellt zuverlässig sicher, dass jeder im Projekt nur die Information sieht, die für ihn bestimmt ist.

### Aktive Elemente

AWARO.NET® funktioniert vollständig ohne aktive Elemente wie ActiveX-Komponenten oder Java-Applets. Auf Wunsch lässt sich mit Java-Applets der Komfort erhöhen.

### Datenexporte

Datenexporte auf DVD werden mit Hilfe des Blowfish Verschlüsselungsalgorithmus mit einer Schlüssellänge von 128-Bit verschlüsselt. Das Passwort wird auf getrenntem Wege kommuniziert.

### Personal

Das gesamte mit dem technischen Betrieb und der Benutzerbetreuung befasste Personal ist zur Geheimhaltung aller Plattforminformationen verpflichtet worden und hat eine entsprechende Erklärung zum Datenschutz und zur Geheimhaltung unterzeichnet. Darüberhinaus sind alle unsere Mitarbeiter nach dem Luftfahrtsicherheitsgesetz §7 einer positiven Zuverlässigkeitsprüfung unterzogen worden.