

# Sicherheits- und Betriebskonzept (SBK)

Ausgabe April 2008

---

## 1. Sicherheit

Auf den Servern von **vemap** werden wichtige Daten verschiedener Unternehmen ausgetauscht. Um den Anforderungen an Datenschutz bei der Übertragung, Speicherung und Bereitstellung gerecht zu werden, beachten wir folgende Grundregeln:

- Unsere Server sollen für die berechtigten Nutzer in den Grenzen des technisch machbaren zur Verfügung stehen
- Daten dürfen Dritten nicht zugänglich gemacht werden
- Daten sollen nur von berechtigten Nutzern geändert werden können
- Daten sollen vom Absender zur angegebenen Zeit kommen.

## 2. System

Das System richtet sich nach den Sicherheitsgrundregeln und besteht im Wesentlichen aus den Basisfunktionalitäten Security, User Management und den Applikationen mit den Hauptmodulen eScreening, eSourcing, eProcurement und eReaction. Es sind vier getrennte Systemumgebungen vorhanden. Damit ist sichergestellt, dass der produktive Betrieb unabhängig von den Schulungen, den Tests und der Weiterentwicklung der Software laufen kann.

## 3. Betriebskonzept

### 3.1. Betrieb:

Das Serverhousing erfolgt in zwei getrennten Hochsicherheits-Rechenzentren und wird mit **folgenden Features durchgeführt:**

- Sicherheitsmassnahmen:
  - Sicherheitsmonitoring
  - Zertifizierte 128-Bit-SSL Verschlüsselung
  - Doppelte Firewall und Paketfilter
  - Dreifach redundante Serverfarmen an zwei verschiedenen Standorten
  - Physikalischer Schutz für das Gebäude um die Server durch
    - Zutrittskontrolle
    - Redundante Stromversorgung und Notstromgenerator
    - Überspannungsschutz, Filter gegen Stromschwankungen
    - Redundante Klimaanlage
    - Brand-Früherkennung
    - Brandmelde- und Löschanlage
    - Videoüberwachung und Bewegungssensoren mit Aufzeichnung
    - Leckwarnsystem
    - Definierte Berechtigungsverfahren beim Zutritt für Personal
  - Off-Site-Backup System über VPN mit Sicherheitsmonitoring
    - 1x täglich inkrementelles Backup
    - 1x wöchentlich Fullbackup
    - 1 Monat Speicherzeit
- Redundante Highspeed Internetanbindung an Backbone (multihomed).

### 3.2. Applikationen:

Die Lösung umfasst einen frei zugänglichen Bereich und einen nur für berechtigte Nutzer zugänglichen Privatbereich.

Im **frei zugänglichen Bereich** sind allgemeine Informationen, u. a. über **vemap**, über technische Voraussetzungen und über die Applikationen enthalten.

Die Zugangskontrolle für den **Privatbereich** erfolgt über eine individuelle Nutzerkennung (Login) und ein Passwort mit Passwort- Policy für automatisches abmelden nach Zeitüberschreitung. Die Passwörter der Nutzer können vom Nutzer beliebig oft geändert werden. Hat ein Nutzer sein Passwort vergessen, kann der Administrator für ihn das ursprüngliche Passwort generieren.

Die Anbieter benötigen für die Abgabe von Angeboten und für die Teilnahme an Auktionen Transaktionsnummern, die die Rechtmäßigkeit der Angebote bestätigen. Diese Transaktionsnummern werden vom Administrator des Kunden generiert und den Anbietern per E-Mail weitergeleitet.

**vemap** garantiert für Kunden mit der entsprechenden technischen Ausstattung eine Verschlüsselung mit 128 Bit Schlüssellänge.

Nach dem Administrationskonzept ist jeder Kunde für die Vergabe und Verwaltung von Zugangskennungen seiner Nutzer wie Administratoren, Verwalter, Beobachter, Anbieter, Besteller, und Lieferanten, selbst verantwortlich. Der individuelle Nutzer ist der Teilnehmer, der die eigentlichen Geschäfte als Käufer oder Verkäufer abwickelt. Die Abwicklung der Geschäfte erfolgt in einem in sich abgeschlossenen Bereich. Es haben nur jene Nutzer Zugang, die vom Kunden dafür frei geschaltet / eingeladen werden.

Alle Daten und Dokumente, die auf die Server von **vemap** transferiert werden, werden in elektronischer Form ein Jahr aufbewahrt, sofern mit einzelnen Kunden nichts anderes vereinbart ist und sofern sie von den Nutzern nicht schon früher gelöscht werden.

### 3.3. Supporthotline:

Die Hotline kann über eine zentrale Telefonnummer und über eine zentrale E-Mailadresse (Kontakt Button) kontaktiert werden.

Die Hotline beantwortet in 6 Sprachen inhaltliche und technische Fragen und sorgt bei speziellen Fragen für eine Beantwortung. Die Hotline verständigt die Kunden per E-Mail über eine geplante Nichtverfügbarkeit des Systems und über bekannte aktuelle Serverprobleme, die absehbar länger als 3 Stunden dauern werden.

Reaktionszeiten der Hotline:

Montag bis Freitag (werktags) von 08:00 Uhr bis 18:00 Uhr (CET).

Wien, im April 2008