



## Zentrum für sichere Informationstechnologie – Austria Secure Information Technology Center – Austria

A-1040 Wien, Weyringergasse 35  
Tel.: (+43 1) 503 19 63-0  
Fax: (+43 1) 503 19 63-66

A-8010 Graz, Inffeldgasse 16a  
Tel.: (+43 316) 873-5514  
Fax: (+43 316) 873-5520

<http://www.a-sit.at>  
E-Mail: [office@a-sit.at](mailto:office@a-sit.at)

DVR: 1035461

ZVR: 948166612

### >> NEWSLETTER 2007-02 <<

#### INHALT:

**Aktualisiert: "Österreichisches Informationssicherheits-Handbuch" (vormals "IT-Sicherheits-Handbuch")**

**Zur Auffrischung: "10 Grundsätze bei der Verwendung des Computers bei der Arbeit"**

**Zwischenbericht: EU-Projekt: "eGov Bus"**

**Onlineinformationen**

**Hinweise, Newsletter Abmeldung, Impressum**

---

#### Österreichisches Informationssicherheitshandbuch, Version 2.3

Im Auftrag des Bundeskanzleramtes (BKA) wurde das frühere "IT-Sicherheits-Handbuch" aufgrund der aktuellen internationalen Entwicklungen überarbeitet und zum "Österreichischen Informationssicherheitshandbuch" weiterentwickelt.

Dabei wurden die beiden Teile

- 1) "Informationssicherheitsmanagement" und
  - 2) "Informationssicherheitsmaßnahmen" um
- auf den neuesten Stand der Technik gebracht. Aktuelle E-Government Initiativen und Empfehlungen des IKT-Boards wurden eingearbeitet.

Das primäre Thema ist die Sicherheit der Information unter Verwendung sicherer Technologien, welche über die reine Informationstechnologie (IT) hinausgehen.

Die Themen sind bewusst allgemein formuliert und richten sich sowohl an die öffentliche Verwaltung als auch an die Wirtschaft bzw. Industrie sowie an interessierte Bürgerinnen und Bürger.

Online liegt das "Österreichische Informationssicherheitshandbuch" auch in XML vor. Damit wurde, über die rein textliche Aufarbeitung von Sicherheitsmaßnahmen hinausgehend, Funktionalität zur Unterstützung der Umsetzung möglich: Spezifische, der Situation einer Organisation angepasste Konfigurationen (öffentliche Verwaltung vs. Privatwirtschaft, große vs. kleine Organisationseinheit) werden unterstützt. Unterschiedliche Ansichten blenden die für eine Rolle (Entscheidungsträger, Umsetzer der Sicherheitsmaßnahmen oder Anwender/innen) unwesentlichen Informationen aus. Checklisten erlauben unter Nutzung von an die Organisation angepassten XML-Versionen die Darstellung und Dokumentation des Umsetzungsgrades.

Das "Österreichische Informationssicherheitshandbuch" steht für Sie im PDF- sowie XML-Format zum Download bereit: <http://demo.a-sit.at/siha-home/home/>



Akkreditierte Überwachungsstelle

© A-SIT, Partner für Sicherheitsfragen

## 10 Grundsätze bei der Verwendung des Computers bei der Arbeit

Unterschätzen Sie nicht die Bedrohungen Ihrer Infrastruktur und Ihrer Informationen:

- In den allermeisten Fällen führt eigenes, unachtsames Verhalten zu Schäden.
- Viren können großen Schaden oder sogar totalen Datenverlust zur Folge haben.
- Datenträger und Dokumente können gestohlen werden.
- Geknackte und gestohlene Passwörter öffnen Unberechtigten den Zugang zu sensitiven Informationen und Gebäuden.
- Telefonleitungen und Internetverbindungen können angezapft werden.

Achten Sie darauf, dass die größeren Schäden oft durch voreiliges Handeln entstehen.

### 1. Ihr Computer

- Stellen Sie Ihren PC wenn möglich so auf, dass Unberechtigte keine Einsicht in sensitive Informationen erhalten.
- Aktivieren Sie immer einen Bildschirmschoner.
- Achten Sie darauf, dass dieser nur mit Passwort entsperrt werden kann.
- Lagern Sie sensitive Informationen auf entfernbaren Datenträgern und versperren Sie diese immer, wenn Sie nicht an Ihrem Arbeitsplatz sind. Im Zweifelsfall beenden Sie das System. Achten Sie auf geeignete Verwahrung von Daten, deren Verlust Ihnen schaden könnte.

### 2. Peripherie

- Lassen Sie externe Datenträger (z.B. USB-Sticks) nie unkontrolliert benutzen.
- Verwenden Sie Quarantänemechanismen bevor Sie Datenträger, die mit anderen Rechnern in Kontakt waren, weiter verwenden. Wo immer möglich verwenden Sie "read only" Modes.
- Aktivieren von Druckern kann ausführbare Elemente enthalten und soll daher nur in kontrollierten Umgebungen stattfinden.
- Drucken Sie sensitive oder vertrauliche Informationen nur in Ihrer Gegenwart. Entsorgen Sie Fehldrucke und Fehlkopien.
- Verwenden Sie Aktenvernichter selbst, um Missbrauch von Dokumenten zu verhindern.

### 3. Passwörter

- Vermeiden Sie triviale Passwörter (Namen, Vornamen, Geburtsdaten, ..).
- Schreiben Sie Passwörter nicht auf, da diese den Zugang zu Ihrer Information ermöglichen.
- Verwenden Sie Passwörter, die mehr als 7 Zeichen umfassen. Achten Sie dabei darauf, dass sowohl in den ersten 7 Zeichen wie auch im Rest Sonderzeichen vorkommen.
- Verwenden Sie nicht das gleiche Passwort in unterschiedlichen Sicherheitsbereichen.
- Wechseln Sie Ihre Passwörter in regelmäßigen Abständen.
- Geben Sie Passwörter nie weiter, auch nicht bei vorgegebenen Systemproblemen.

### 4. Viren

- Stellen Sie sicher, dass Ihr Computer bereits vor dem ersten produktiven Gebrauch einen aktiven Virenschutz besitzt.
- Aktualisieren Sie die Virenschutzdateien regelmäßig und automatisch.
- Schalten Sie den Virenschutz nie ab, auch dann nicht, wenn dies als Fehlerbehebung automatisch vorgeschlagen wird.

- Überprüfen Sie fremde Daten über Speicher und über Internet auf Viren, bevor Sie diese verwenden (Quarantänemechanismen).
- Wenn dennoch ein Virus auftritt, nehmen Sie Ihr Gerät vom Netzwerk, schalten Sie es ab und verständigen Sie die Hotline.

## 5. Sensible Daten

- Verwahren Sie sensible Daten immer verschlüsselt.
- Wenn Sie die Daten auf Backupmedien unverschlüsselt halten, stellen Sie die geeignete Verwahrung und den Schutz vor Zugriff sicher.
- Beachten Sie Regeln für den Autostart von Datenträgern.
- Betrachten Sie fremde Datenträger und Daten wie unsichere Informationen über das Internet.
- Bedenken Sie, dass bei Schlüsselverlust verschlüsselte Daten verloren sind.
- Sorgen Sie für ein vertrauenswürdigen Backup verschlüsselter Daten unter einem anderen Schlüssel.
- Beachten Sie, dass der Verlust von Signaturschlüsseln keinen Datenverlust mit sich bringt, sichern Sie daher Ihre Signaturschlüssel nie.

## 6. Intranet / Internet

- Vergewissern Sie sich bei allen Downloads, dass keine ungewollten Programme ausgeführt werden.
  - Achten Sie auf Dateitypen.
  - Kontrollieren Sie Ihre Einstellungen.
  - Laden Sie Programme nur in kontrollierten Umgebungen.
- Achten Sie auf möglichst restriktive Browsereinstellungen.
- Laden Sie von nicht mit SSL gesicherten und freigegebenen Sites nur passive Daten (.html, .txt, .tiff,...).
- Verschlüsseln Sie vertrauliche Daten vor dem Versand.
- Signieren Sie Ihre Mails, damit die Herkunft nachgewiesen werden kann.

## 7. Laptops

- Achten Sie auf unbewusstes / unerkanntes Networking (Infrarot, Bluetooth, WLAN) und deaktivieren Sie nicht benötigte Netzwerk-Kanäle.
- Vermeiden Sie unbeherrschte Services (File- & Printerservice, etc...).
- Aktivieren Sie immer eine persönliche Firewall.
- Verwenden Sie nur die für Ihre Umgebung / Ihren Arbeitsbereich freigegebenen Programme.
- Betreiben Sie Laptops immer im eingeschränkten Benutzermodus. Ein Administratorkonto soll nur in jenen Fällen verwendet werden, wo es unumgänglich ist.
- Beachten Sie die Gefahren der Synchronisation und Datenübernahme aus PDAs und Handys, da hier exekutierbare Elemente transferiert werden können.
- Verwenden Sie ein Startpasswort, um Ihre Festplatte zu schützen.
- Verwahren Sie Ihren Laptop immer in geeigneter Weise.
- Lassen Sie Ihren Laptop in öffentlichen Bereichen (Flughafen, Café, Hotel, ...) nie unbeobachtet.

- Verlassen Sie nie ein angemeldetes Gerät ohne den Zugriff zu sperren, auch nicht zum Holen einer Tasse Kaffee.

## 8. Dokumentenversand

- Beim Versand von Dokumenten übernehmen Sie Verantwortung:
  - für die Vertraulichkeit
  - für die Sicherheit und Freiheit von schädigenden Elementen
- Achten Sie auf Virenprüfung vor dem Versand.
- Vergewissern Sie sich, dass Dokumente weitergegeben werden dürfen.
- Beachten Sie Kopiereinschränkungen.
- Passworte, die in Dokumenten vergeben werden, sind in der Regel kein ausreichender Schutz.
- Verwenden Sie Verschlüsselung bei vertraulichen Dokumenten.
- Verwenden Sie nach Möglichkeit Formate, die keine Änderungen zulassen (z.B. PDF).
- Signieren Sie im elektronischen Versand, damit der Empfänger das Dokument auch vertrauenswürdig öffnen kann.
- Achten Sie auf zulässige Austauschformate und vermeiden Sie nach Möglichkeit Formate, die ausführbare Elemente erlauben.

## 9. Zutrittskarten / Schlüssel

- RF-Schlüssel (kontaktlose Karten, elektronische Schlüssel, etc...) können Aufschluss über die Identität und Rollen liefern. Beachten Sie die Aufbewahrungsvorschriften sorgfältig.
- Nehmen Sie Schlüssel und Zutrittskontrolltags nicht in die Freizeit mit. Lassen Sie diese nicht im Auto liegen.

Melden Sie jeden Verlust von Schlüsseln oder Zutrittskarten unverzüglich.

## 10. Was tun, wenn tatsächlich etwas vorfällt?

- Entscheiden Sie zuerst, wo Gefahr in Verzug ist - nur in diesen Bereichen sind Notmaßnahmen ohne externe Hilfe gerechtfertigt.
- Verständigen Sie unverzüglich alle Zuständigen - Systemadministratoren, Vorgesetzte, Verantwortliche für Warnsysteme, Hausverwaltung, etc.
- Protokollieren Sie den gesamten Hergang.
- Trennen Sie alle betroffenen Geräte vom Netzwerk.
- Achten Sie auf fachgerechte Datensicherung.
- Führen Sie keine Startversuche von betroffenen Geräten durch.

Die Folgen von Sicherheitsverletzungen können schwerwiegend sein, beachten Sie daher die Regeln genau.

---

## EU-Projekt: "eGov Bus" - Advanced eGovernment Information Service Bus

eGov-Bus ist ein Forschungsprojekt, das unter dem 6. Rahmenprogramm von der Europäischen Kommission gefördert wird

Forschungsziele des Projektes sind:

- Die Entwicklung anpassbarer Prozess-Management Technologien, um neue E-Government Dienste dynamisch aus bestehenden Webservices der Verwaltungen zu kombinieren
- Das Unterstützen von grenzüberschreitenden Verwaltungsverfahren in spezifischen Lebenslagen der BürgerInnen über das Orchestrieren bestehender E-Government Web-Services
- Umfassende Workflow-Informationen und Erläuterungen für die Anwender
- Die Erweiterung von Web-Service Technologien um fortgeschrittene Funktionalitäten wie Service Level Agreements oder Audit-Trails
- Automatisierte Sprachverarbeitung, um benutzerfreundliche Freitext- oder Spracheingabe zu unterstützen
- Die Entwicklung neuer Virtual Repository Technologien für abstrahierte Zugänge zu E-Government Informationen
- Umfassende Lösungen zu Informationssicherheit und Datenschutz unter Einbeziehung elektronischer Identitätskarten (Bürgerkarten) und qualifizierter Signatur

Im Laufe des nächsten Jahres soll aus diesen Forschungsvorhaben ein Portal demonstriert werden, über das Bürger/innen Ihre Lebenslage angeben. In einem Dialog sollen die notwendigen Verwaltungsschritte identifiziert, die Information gesammelt und die Verfahren angestoßen werden. Am plakativen Beispiel einer Übersiedlung wären - je nach Situation des Bürgers bzw. der Bürgerin - einige notwendige Schritte: etwa die An- und Abmeldung des Wohnsitzes, die Ummeldung eines Kraftfahrzeugs, die Anmeldung der Kinder an einer neuen Schule, uvm. Diese Schritte sollen über das Portal aus dem Anfangsdialog identifiziert und notwendige Unterlagen gesammelt werden. Nach Simulation des Prozesses werden die konkreten E-Government Webservices aufgerufen.

Ausführliche Informationen bietet die Projekt-Webseite unter: <http://www.egov-bus.org/web/quest/home>.

---

### Onlineinformationen:

- [www.a-sit.at](http://www.a-sit.at) - Übersichtlich gegliederte Beschreibungen und Informationen zu den Tätigkeitsbereichen von A-SIT: Bestätigungsstelle, Überwachungsstelle, E-Government, Technologiebeobachtung, Sicherheitsbegleitung, Internationales - Aktivitäten, Newsletter An- und Abmeldung, mit einer Suchfunktion über die gesamte Site
- <http://demo.a-sit.at> - Tools und Demonstratoren für Experten oder Interessierte
- [www.buergerkarte.at](http://www.buergerkarte.at) - Alles rund um die österreichische Bürgerkarte

**"Klicken" Sie sich durch unser Angebot!**

Mit informationstechnologischen Grüßen - Ihr A-SIT Team

---

**Hinweise:**

Sie haben sich für unseren Newsletter via Homepage angemeldet oder sind in der Vergangenheit bereits von uns als Kunde oder Interessent kontaktiert worden und haben der Zusendung nicht widersprochen. Wir freuen uns über Ihr Interesse.


**Newsletter abmelden:** Sollten Sie in Zukunft jedoch keinen weiteren Newsletter von A-SIT erhalten wollen, können Sie sich auf unserer Homepage unter: <http://www.a-sit.at/de/allgemein/newsletter.php> jederzeit abmelden.

>>-<<--->>-<<--->>-<<--->>-<<

**Für den Inhalt verantwortlich:**

A-SIT Zentrum für sichere Informationstechnologie - Austria, Weyringergasse 35, 1040 Wien

[Impressum](#)

Signaturwert	zSrwPnLWcJlM/kK+9sGVfNnIJHSiTKag7MhAA8M7AVZYD00VvUVYt311bW03ArwF	
	Signator	Kommunikationsmanagement: Helga Spacek-Stangl
	Datum/Zeit-UTC	2007-11-08T09:52:01Z
	Aussteller	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	151051
	Methode	urn:pdfsigfilter:bka.gv.at:text:v1.0.0
	Kennung	1194515521-5582357@16850-359-9788-30512-18287
Hinweis	Informationen zur Signaturprüfung finden Sie unter: <a href="http://www.a-sit.at/de/dokumente_publicationen/a-sit_signaturen/index.php">www.a-sit.at/de/dokumente_publicationen/a-sit_signaturen/index.php</a> .	