Domain-Policy		Konvention domainpol 1.0.1 Entwurf öffentlich
Kurzbeschreibung	Der Auftritt der öffentlichen Verwaltung im Internet ist nicht mehr wegzudenken. Diese Domain-Policy zielt nun darauf ab, das Bild nach außen einheitlich erscheinen zu lassen und die Einhaltung diverser Sicherheits- und organisatorischer Anforderungen zu garantieren. Aus diesem Grund werden im Speziellen Richtlinien und Best-Practice Angaben vorgegeben, die sich auf Inhalte, und sicherheitstechnische und organisatorische Vorgaben beziehen. Während die weiteren Dokumente der Internet-Policy eine Richtlinienmenge vorgeben, die meist von den Behörden eigens ausdefiniert werden müssen, werden hier bereits konkrete Vorschläge definiert.	
Autor(en)	**Bernd Martin** **Michael Liehmann**	**Projektteam / Arbeitsgruppe** **Internetpolicy**

Stelle	Vorgelegt am	Angenommen am	Abgelehnt am
IKT-Board **Länder** **Gemeindebund** **Städtebund**	03.05.2005 22.05.2005 22.05.2005 22.05.2005	13.05.2005	

Dokumentklasse: **Konvention** Erläuterung Information

Doku-Stadium: Entwurf **Entwurf** Empfehlung — intern **öffentlich**

Domain-Policy

Inhaltsverzeichnis[1]

[1] Im Maßnahmenkatalog werden Basisanforderungen mit einem B und optionale Anforderungen mit einem O markiert. Während Basisanforderungen verpflichtend in der behördeneigenen Domain-Policy zu behandeln sind, gelten optionale Anforderungen als Empfehlung.

(1) Einleitung

Ziel

Das Ziel der Domain-Policy ist es, den Auftritt der öffentlichen Verwaltung im Internet zu vereinheitlichen und entsprechende Standards und Minimalanforderungen zu empfehlen. Die Domain-Policy zielt weiters auf die Garantie und Einhaltung diverser Sicherheits- und organisatorischer Anforderungen ab. Dazu zählen unter anderem allgemein gültige Richtlinien für die Inhalte des Internetauftritts (was ist erlaubt, was nicht und was wird empfohlen), aber es werden auch infrastrukturelle Fragen beantwortet. In den Fragen werden Maßnahmen beschrieben, die bei einem sicheren Webauftritt zu beachten sind.

In diesem Papier wird jener Personenkreis, der das Angebot der Webseite konsumiert mit Nutzer bezeichnet[2]. Es wird nicht zwischen Homepageinhaber (jene Person, Organisation oder Organisationseinheit, die für die Inhalte und das Funktionieren verantwortlich ist) und Betreiber (jene Organisation, die die technische Infrastruktur zur Verfügung stellt und den Betrieb sichert) unterschieden, sondern nur Betreiber bzw. Diensteanbieter sinngemäß verwendet werden und ist im jeweiligen Anwendungsfall entsprechend anzupassen.

(2) Inhalte der behördeneigenen Domain-Policy

Das Ziel ist es folgende Themenbereiche abzuhandeln:

- Inhalte
- Layout
- Sicherheitsanforderungen
- Infrastruktur und Organisation

Während sich im ersten Teil allgemeine Richtlinien und Empfehlungen über mögliche Inhalte wieder finden, sind im Kapitel Layout bereits konkrete Maßnahmen angedacht, um das Bild nach außen einheitlich erscheinen zu lassen. Mit den Sicherheitsanforderungen soll es dem Nutzer aufgrund mehrerer Merkmale überhaupt erst ermöglicht und erleichtert werden, Auftritte der öffentlichen Verwaltung mit Gewissheit als solche (wieder-)erkennen zu können. Allgemeine infrastrukturelle und organisatorische Richtlinien sollen eindeutige Verantwortlichkeiten und ein reibungsloses Funktionieren des Betriebs des Internetauftritts garantieren helfen.

(3) Inhalte

Die Internetseiten einer Behörde müssen mindestens die im Folgenden angeführten Einträge aufweisen.

Speziell jene Punkte, die in (3.1) Policies, (3.2), (3.3), (3.5) und (3.6) (und sofern vorhanden auch (3.4)) angeführt sind, sollen an prominenter Stelle des Webauftritts platziert werden und leicht wiedergefunden werden können.

[2] Aus Gründen der einfacheren Lesbarkeit wird auf die geschlechtsneutrale Differenzierung, z.B. Nutzer/innen, verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für beide Geschlechter.

Best Practice:
Die eben angeführten Punkte sollen über die interne Suche des Webauftritts der Behörde unter den ersten Ergebnislinks auffindbar sein. Als mögliche Suchworte sollen dabei zumindest die hier angeführten Überschriften bzw. bei mehrsprachigen Auftritten deren jeweiligen Pendants verwendet werden können.

(3.1) Policies B

Die Vorgaben für Internetpolicies [INTPOL] sollen, nach Überarbeitung bzw. genauen Definition der Behörde, an einer prominenten Stelle des Webauftritts zu finden sein (vgl. [INTPOL], Punkt 9 und Best Practice unter (3)).

(3.2) Internetveröffentlichungen B

§ 13 Abs. 1 und 5 des [AVG], BGBl. Nr. 51/1991 sehen vor, dass seitens der Behörden die Adressen sowie die allenfalls bestehenden besonderen technischen Voraussetzungen, unter welchen Anbringen rechtswirksam eingebracht werden können, im Internet bekannt zu geben sind (vgl. auch [EGOVG] 7. Abschnitt, Artikel 2).

(3.3) Kontaktadresse B

Um dem Bürger oder einer anderen Behörde die Möglichkeit zu bieten rasch und unkompliziert mit der Behörde in Kontakt zu kommen, muss zumindest eine der folgenden Kontaktmöglichkeiten leicht auffindbar sein. Die erste Variante mit dem elektronischen Formular ist zu bevorzugen.

(3.3.1) Elektronisches Formular B/O

Um sicherheitsrelevanten Problemen entgegenzuwirken, ist der Einsatz von Formularen als Kontaktmöglichkeit gegenüber E-Mail (vgl. (3.3.2)) zu bevorzugen. Hierbei sollte auf besondere Übersichtlichkeit und Anwendbarkeit Wert gelegt werden. Weiters muss dabei der Styleguide [STYLEGUIDE] zum Einsatz kommen.

Für elektronische Anbringen gelten zusätzliche Anforderungen, die in der Arbeitsgruppe Kommunikationsarchitekturen definiert werden (vgl. dazu [SGAD1.0.0]).

(3.3.2) E-Mail O

Die E-Mail-Adressen der organisationsspezifischen Postfächer müssen erkennbar sein. Eine Aufteilung in die jeweiligen spezifischen Bereiche ist anzudenken. Die Form der E-Mail Adressen wird in [EMAILPOL] geregelt. Es ist darauf zu achten, dass das Publizieren der E-Mail-Adressen keine Grundlage für Spammer bietet.

Best Practice:
Wie in der E-Mail-Policy [EMAILPOL] in Kapitel 5.1 beschrieben, kann man durch triviales Codieren der auf HTML-Seiten veröffentlichten E-Mail-Adresse den automatischen E-Mail-Erntemaschinen das Lesen der Adresse erschweren. Durch Formatieren bzw. durch Ersetzen einiger Zeichen der E-Mail-Adresse durch deren numerische Werte kann dies erschwert werden. Eine beispielhafte E-Mail-Adresse könnte wie folgt aussehen: `max&#46;mustermann&#64;bka&#46;gv&#46;at`

(3.4) Sitemap O

Um dem Nutzer des Webauftritts der Behörde die Navigation in demselben zu erleichtern, empfiehlt es sich eine Sitemap anzubieten, die in übersichtlicher Art und Weise eine Gesamtübersicht des Webauftritts der Behörde wiederspiegelt.

Best Practice:
Die Sitemap soll kurz, informativ und übersichtlich aufgebaut sein. Aus Gründen der Anwendbarkeit sollten Standard HTML Techniken bei der Erstellung der Sitemap verwendet werden.

(3.5) Suche B

Die Internetseiten einer Behörde müssen über eine leicht auffindbare Suchmöglichkeit verfügen, die über ein einfaches Texteingabefeld aufgerufen werden kann.

Best Practice:
Die Suche sollte über ein einfaches Texteingabefeld und einen zugehörigen Button auf der Startseite durchgeführt werden können.

(3.6) Über uns/Impressum B/O

Sofern nicht ohnedies eine Verpflichtung des §5 E-Commerce-Gesetz [ECG] besteht, sollten folgende Informationen in einem Impressum veröffentlicht werden:

- Namen des Eigentümers bzw. Diensteanbieters (wer ist für den Inhalt verantwortlich)
- die geografische Anschrift, unter der der Diensteanbieter niedergelassen ist
- Angaben, aufgrund deren die Nutzer rasch und unmittelbar mit der Behörde in Verbindung treten können, einschließlich der elektronischen Postadresse (z.B. Telefon, Fax, E-Mailadresse des Webmasters, Link zu einem Formular, etc.)

Des Weiteren können Information über die Behörde selbst, welche Mitarbeiter für welche Bereiche zuständig sind, welche interne Struktur und welchen gesetzlichen Auftrag eine Behörde verfolgt Bestandteil des Webauftritts der Behörde sein und mehr Transparenz in deren Struktur schaffen.

Best Practice:
Es wird empfohlen, dass der Webauftritt neben organisatorischen Informationen (interne Geschäftsstruktur, Aufbau der Abteilungen inkl. jeweiligen Fachrichtungen und Ansprechpartner) auch den gesetzlichen Auftrag und das Aufgabengebiet der Behörde beinhaltet. Damit wird es Bürgern erleichtert Zuständigkeiten und zugehörige Kontakte herauszufinden.

(3.6.1) Mitarbeiterverzeichnis O

Es besteht die Möglichkeit ein Mitarbeiterverzeichnis im Webauftritt zu integrieren. Sofern auch die die E-Mail-Adressen der Mitarbeiter veröffentlicht werden, sollten diese nach den E-Mail Policy Vorgaben [EMAILPOL] angeführt werden (Sicherheit, organisationsbasierte Postfächer, Kodierung, etc.). Eine Einteilung in Geschäftsbereiche ist anzudenken.

(3.6.2) Glossar O

Es wird empfohlen einen Link anzubieten, auf der die für die vorliegende Behörde maßgeblichen Begriffe und des Weiteren vielfach verwendete Abkürzungen kurz erläutert werden. Dies führt zum besseren und klareren Verständnis der Inhalte des Webauftritts.

(3.7) Mehrsprachigkeit O

Aufgrund der zunehmenden Globalisierung und dem Zusammenwachsen Europas wird empfohlen, Webseiten nicht nur in deutscher Sprache anzubieten, sondern in weiteren

Sprachen, die aufgrund des angesprochenen Aufgabengebietes von Bedeutung sind bzw. sein können. Die Sprachwahl muss einfach ersichtlich und auswählbar sein.

Best Practice:
Um eine Übersetzung in mehrere unterschiedliche Sprachen mit einer Kompromisslösung zu begegnen, ist die Bereitstellung von wichtigen Inhalten in englischer Sprache zu bevorzugen. Zur Unterscheidung der Sprachen kann die Flagge von Großbritannien für Englisch bzw. von Österreich für Deutsch, aber auch die Wörter „ENGLISH" bzw. „DEUTSCH" zur Anzeige des jeweilig zugehörigen Links verwendet werden.

(3.8) FAQs O

Häufig auftretende Fragen, Themen die einfachen und schnell zu leistenden Support verlangen oder Anliegen die eine Vielzahl von Bürgern betreffen, sollten in einer eigenen *Antwortseite* zusammengefasst werden.

Best Practice:
Um den Bürger bei der Suche nach einer Lösung zu unterstützen, kann diese Seite in behördenspezifische Themenbereiche aufgeteilt werden. Zur Vereinfachung des Auffindens dieser Seite, soll auf der Startseite der Behörde ein Link zu den FAQs verfügbar gemacht werden.

(3.9) Elektronische Formulare B

Die in der Behörde für E-Government Anwendungen verwendeten elektronischen Formulare müssen dem Styleguide [STYLEGUIDE] entsprechen. Etwaige Sicherheitsvorschriften bei der internen Übermittlung der Daten müssen gewahrt werden (vgl. auch Punkt (5) Sicherheitsanforderungen).

Für elektronische Anbringen gelten zusätzliche Anforderungen, die in der Arbeitsgruppe Kommunikationsarchitekturen definiert werden (vgl. dazu [SGAD1.0.0]).

(3.10) Informative Fehlerseiten B

Wird eine Seite des Webauftritts nicht gefunden und standardmäßig ein Fehler des Webservers retourniert (dh. es gibt einen HTTP-Fehler), darf keine Standardfehlermeldung angezeigt werden.

Der Inhalt der Fehlerseite muss übersichtlich und verständlich gestaltet sein. Der HTTP-Fehlercode des aufgetretenen Fehlers muss unverändert übergeben werden; keinesfalls darf HTTP Statuscode 200 (Erfolgreich/Successful) retourniert werden.

Best Practice:
Es wird empfohlen dem Nutzer auf Fehlerseiten eine leichte und unkomplizierte Art der Kontaktaufnahme anzubieten. Außerdem soll auf der jeweiligen Fehlerseite auch ein Link zur Startseite bzw. zur Suche enthalten sein. Die Fehlerseiten sollen den Nutzer bestmöglich unterstützen.

(3.11) URI für Testapplikationen O

Um diverse Testapplikationen technisch und organisatorisch einfach abwickeln zu können, soll ein vereinheitlichter URI dienen. Werden Behördenapplikationen getestet, können diese über die jeweilige Subdomäne angeboten werden:

http://test.<Domainname>.gv.at/

Somit wäre es innerhalb der Verwaltung einfach, Applikationen zB auch mit diversen Bürgerkarten (u. a. mit der A1-Signatur) unbürokratisch und kostenlos zu testen. Die entscheidenden Kriterien dafür sind die Endung .gv.at und die Subdomäne test. Die

Behörde verpflichtet sich mit dieser URI nur Applikationen zum Testen anzubieten und darüber keine Produktionssysteme zu betreiben. Sollen Tests aufgrund technischer oder sonstiger Restriktionen über andere URIs durchgeführt werden, so sind weitere Informationen zur Nutzung der jeweiligen Bürgerkarte unter http://www.cio.gv.at/identity/ auffindbar. Weitere Informationen zur Vereinheitlichung von Subdomänen gibt es im Kapitel „Vergabe von Subdomänen" in [DOMAINREG].

(4) Layout

In dieser Policy werden grundlegende Eigenschaften von Webseiten der öffentlichen Verwaltung definiert. Ziel ist es ein einheitliches Auftreten nach außen zu erzielen und die Inhalte für andere Organisationen der öffentlichen Verwaltung, Bürger und Wirtschaft barrierrefrei anzubieten.

(4.1) WAI Konformität B

Aufbauend auf dem Aktionsplan eEurope 2002 wurden vom Rat der Europäischen Union im Jahr 2002 zwei Entschließungen der WAI-Leitlinien (Web Accessability Initiative) [WAI-GUIDELINES] angenommen, die die Erleichterung des Zugangs zu Webinhalten und zur Wissensgesellschaft zum Ziel haben. Außerdem ist auch im E-Government-Gesetz [EGOVG] in §1, Absatz 3 verankert, *„… dass behördliche Internetauftritte, die Informationen anbieten oder Verfahren elektronisch unterstützen, spätestens bis 1. Jänner 2008 so gestaltet sind, dass internationale Standards über die Web-Zugänglichkeit auch hinsichtlich des barrierefreien Zugangs für behinderte Menschen eingehalten werden.*".

Barrierefrei sind Systeme der Informationsverarbeitung, akustische und visuelle Informationsquellen und Kommunikationseinrichtungen, wenn sie für Menschen mit Behinderungen in der allgemein üblichen Weise, ohne besondere Erschwernis und grundsätzlich ohne fremde Hilfe zugänglich und nutzbar sind.

Als Empfehlung gilt, dass bei der Gestaltung und Implementierung von Webseiten der öffentlichen Verwaltung zumindest WAI Level A erreicht werden muss. Ergänzend dazu sind für veröffentlichte, downloadbare Dokumente die Formate PDF (Portable Data Format) bzw. RTF (Richt Text Format) zu verwenden. Die jeweiligen Versionen sind aus dem Dokument Dokumentenformate [DOKFORMATE] zu entnehmen.

Best Practice:
Eine Checkliste über die notwendigen umzusetzenden Eigenschaften kann in der [WAI-CHECKLIST] gefunden werden.

Eine automatische Validierung kann zB. unter
http://bobby.watchfire.com/bobby/html/en/index.jsp oder http://webxact.watchfire.com/
durchgeführt werden.

Best Practice:
Grundsätzlich wird empfohlen, jeglichen möglichen Inhalt in HTML anzubieten; damit kann der höchste Grad in Richtung WAI erreicht werden.

(4.2) HTML-Standardkonformität und Zeichensätze B

Bei der Verwendung von Dokumententypen ist auf offene und bewährte Standards Rücksicht zu nehmen. Es ist darauf zu achten, dass zumindest HTML 4.01 Transitional [HTML] oder XHTML 1.0 Transitional [XHTML] unterstützt wird. Werden mehrere Kanäle angeboten, dh. die Webseiten stehen auch für PDAs bzw. Mobiltelefone zur Verfügung, kann dafür der Dokumententyp XHTML Basic (eingeschränktes XHTML) herangezogen werden (vgl. dazu auch (6.1) Multichannel).

Best Practice:

Frames
Frames sollten grundsätzlich vermieden werden. Kommen sie dennoch zum Einsatz, ist der entsprechende Dokumententyp zu setzen und auf jeden Fall das NOFRAMES Element zu verwenden (siehe [HTML] bzw. [XHTML]).

Unterschiedliche Stylesheets
Ist die Bildschirmansicht aufgrund der Formatierung unterschiedlich zur Druckansicht oder wäre die gewünschte Information nur ein *Nebenprodukt* am ausgedruckten Papier (zB. aufgrund sehr viel begleitenden und beschreibenden Textes, Menüeinträgen, oder ähnlichen) bzw. passt der Inhalt gar nicht auf die Seitenbreite, so sind eigene Stylesheets für die unterschiedlichen Zwecke anzuwenden.

Validierung von HTML-Source
Zur Überprüfung der korrekten Syntax stehen im Internet Validatoren zur Verfügung. Eine empfehlenswerte Adresse, unter der das Markup Validation Service des W3C Konsortiums zu finden ist, ist http://validator.w3.org.

(4.3) Dublin Core Metadaten O

Immer öfter werden Metainformationen herangezogen, um Datenquellen bestmöglich zu beschreiben und wieder zu finden. Webseiten stellen dafür wohl die am meisten genutzte Informationsressource dar. Es wird empfohlen bei den erstellten Webseiten Metainformationen nach Dublin Core [DCMI] einzufügen. Damit können Suchmaschinen, Content Management Systeme und dgl. mehr Informationen indizieren und damit qualitativ höherwertige Resultate liefern. Das Dublin Core Metadata Element Set [RFC 2413] war auch der erste Metadata Standard. Damit wird ein Vokabular angeboten, welches die Kerneigenschaften beschreiben lässt.

(4.4) Formularstyleguide B

Wie unter (3.9) bereits angeführt ist bei der Bereitstellung von Formularen der österreichische E-Government Styleguide [STYLEGUIDE] einzuhalten. Dieser Styleguide für elektronische Formulare für E-Government stellt zusammen mit der Beschreibung von Standarddaten die Grundlage für ein einheitliches Layout von elektronischen Formularen der öffentlichen Verwaltung Österreichs dar.

Best Practice:
Die Vorgaben des Formularstyleguides können – sofern anwendbar – für die gesamte Homepage herangezogen werden.

(4.5) Browser- und Bildschirmauflösungskompatibilität B

Es ist darauf zu achten, dass die Webseiten browserunabhängig entwickelt werden. Aus diesem Grund empfiehlt es sich zumindest mit den gängigen Browsern entsprechende Funktionalitätstests durchzuführen. Es darf nicht vorkommen, dass Informationen gar nicht bzw. unvollständig angezeigt werden und Seitenfunktionalitäten in (Skript-) Fehlern resultieren.

Ein ebenso unerwünschtes Verhalten ist, wenn die angebotenen Webseiten nur für bestimmte Bildschirmauflösungen entwickelt wurden. Es ist darauf zu achten, dass alle Informationen auch bei unterschiedlichen Auflösungen lesbar bleiben. Die Informationen sollten so dargestellt werden können, dass bei einer gängigen Bildschirmauflösung (dem Stand der Technik entsprechend) und einem mittleren Schriftgrad kein horizontales Scrollen notwendig wird.

Best Practice:
Als gängige Browser haben sich der Internet Explorer (ab Version 5) und Mozilla ab Version 0.9, sowie Netscape ab Version 6 und Opera ab Version 7 etabliert.

Best Practice:
Da die Einhaltung von HTML, CSS, ECMAScript [ECMASCRIPT] und WAI Standards in der bestmöglichen Interoperabilität resultiert, ist darauf besonders Wert zu legen.

(4.6) Dokumentendownload

Wie in (4.1) WAI Konformität angegeben, sollen von der jeweiligen Webseite downloadbaren und veröffentlichten Dokumente in PDF oder RTF angeboten werden. Andere Dokumentenformate sind im Sinne der Interoperabilität nicht anzubieten.

Best Practice:
Es sei angemerkt, dass ein Publizieren auf der Webseite direkt in HTML das beste Ergebnis im Hinblick auf die WAI-Richtlinien liefert.

(5) Sicherheitsanforderungen

An dieser Stelle werden grundsätzliche Anforderungen an die Sicherheit behandelt und entsprechende Richtlinien empfohlen.

(5.1) Datenübertragung via SSL B

Werden einfache Formulare angeboten, empfiehlt es sich TLS/SSL (Transport Layer Security/Secure Sockets Layer) für die Datenübertragung zu wählen. Aus den Sicherheitsstufen [SiSt] wäre hierfür zumindest die Sicherheitsstufe I zu wählen.

Sollen auch sensiblere Daten übertragen werden und bedarf es einer Identifizierung des Nutzers, so ist Sicherheitsstufe II zu wählen. Damit können die Verwaltungseinrichtung eindeutig identifiziert und der Nutzer identifiziert und authentifiziert werden. Eine Authentifizierung mit Bürgerkarte ist in jedem Fall anderen schwächeren Verfahren vorzuziehen. Werden personalisierte Services Angeboten, so ist den Anforderungen des Datenschutzgesetzes [DSG2000] sowie jenen des E-Government-Gesetzes [EGOVG] zu folgen (siehe Abschnitt 2, §2ff.)

Ein Testtool zum Überprüfung der jeweiligen SSL-Einstellungen wird von A-SIT bereitgestellt [ASIT-SSLTOOL]. Die A-SIT SSL Toolsuite besteht aus zwei Teilen: Mit einem Teil lassen sich die SSL Fähigkeiten von Webbrowsern testen und evaluieren, mit dem anderen die Fähigkeiten von HTTPS fähigen Webservern. Neben den Eigenschaften wird eine Klassifikation ausgegeben, aus der abzulesen ist, ob und in welcher Form sich die getestete Komponente für den Einsatz im E-Government eignet.

Die serverseitig von der Verwaltung zu verwendenden Zertifikate müssen den Vorgaben aus [PKI] bzw. [SERVERZERT] entsprechen. Speziell hervorzuheben ist hier die Verwaltungseigenschaft, die mit dem Object Identifier ausgedrückt wird. Für eine genaue Erläuterung dieser Eigenschaft sei auf das Dokument [OID] verwiesen (vgl. auch FAQs zur Amtssignatur [AMTSSIGFAQ] und Informationen zu Amtssignaturzertifikaten [AMTSSIGZERT] und [AMTSSIGATRUST]).

Best Practice:
Webserver sollten bei Verwendung von Formularen immer eine TLS/SSL Verbindung ermöglichen (https). Die implementierte Sicherheitsstufe solle Stufe I nicht unterschreiten und die Cipher Suites keine Schlüssellängen unter 100 Bit zulassen.

(5.2) Aktive Skriptingelemente B

Aufgrund von WAI Anforderungen und Sicherheitsgründen ist darauf zu achten, dass angebotene Webseiten von Behörden auch ohne aktive Skritpingelemente funktionieren müssen. Somit müssen alle im Internet angebotenen Informationen auch für Browser, die zB. kein Javascript oder ActiveX erlauben, erreichbar bleiben. (vgl. auch Punkt (4) Layout).

Cookies sollen, sofern überhaupt notwendig, am Ende der Browsersession wieder ungültig und verworfen werden und keine längere Gültigkeit aufweisen.

Best Practice:
Die Verwendung von Javascript, ActiveX und anderen aktiven Skriptingelemente sollte – sofern notwendig – nur äußerst sparsam erfolgen und darf nur der Vereinfachung dienen.

Best Practice:
Kommen Cookies zum Einsatz empfiehlt es sich aufklärend anzuführen, wo bzw. warum diese verwendet werden müssen und welche Informationen damit gespeichert werden.

(5.3) Organisatorisches B

Es muss selbstverständlich sein, den Zugang zum Webserver für Administratoren und andere dafür vorgesehene Personen entsprechend abgesichert zu gestalten.

Den dafür relevanten Vorgaben des jeweilig geltenden Sicherheitshandbuchs soll dabei entsprochen werden.

Best Practice:
Als allgemeine Referenz kann dafür das Österreichische Sicherheitshandbuch [SiHB] empfohlen werden.

Ist die Wartung vom Internet aus möglich, dann darf diese nur nach einer angemessenen Authentifizierung und über einen verschlüsselten Kanal erfolgen.

Best Practice:
Auch bei netzwerktechnisch abgesicherten Servern (zB. durch IP-Adressen) soll ein authentifizierter und verschlüsselter Zugang eingerichtet werden.

Best Practice:
Das Resultat aus der regelmäßigen Auswertung der Logfiles kann als Indikator herangezogen werden, um die Webseiten einem ständigen Verbesserungsprozess zu unterziehen.

(6) Infrastrukturelle und organisatorische Maßnahmen

In diesem Punkt sollen alle jene infrastrukturellen und organisatorischen Vorgaben aufgeführt werden, die für einen optimalen behördlichen Internetauftritt notwendig sind.

(6.1) Multichannel O

Die zunehmende Mobilität und neue Technologien erlauben es Nutzern mit mehreren unterschiedlichen Endgeräten das Webservice zu nutzen. Zu diesen Endgeräten zählen zB. Smart Phones, PDAs, etc. Damit der Webauftritt auch auf diesen Geräten vernünftig

nutzbar ist, müssen infrastrukturelle Maßnahmen getroffen werden. Dazu zählt zB. ein Multichannel Server, unterschiedliche Designs, die Verwendung von XHTML Basic, etc.

(6.2) Domänenname und Registrierung B

Mit dieser Domain-Policy wird festgehalten, dass für Webauftritte von Behörden Domänennamen entsprechend den Vorgaben der Internetdomänenverwaltung gv.at - Naming- und Domänenregistrierungs-Policy [DOMAINREG] anzuwenden sind. Behörden müssen ihre gesamten Internetseiten unter dem vorgesehen Domänennamen erreichbar machen.

Best Practice:
Werden derzeit Webseiten unter einer Domäne betreut, die nicht dem Domänennamen laut [DOMAINREG] entspricht, so kann durch ein einfaches Redirect und ohne weitere gravierende Änderungen vornehmen zu müssen, trotzdem der korrekte Domänenname zum Einsatz kommen.

Best Practice:
Werden Nicht-gv.at Adressen von Behörden eingesetzt, so sollte eine Umleitung auf die zugehörige .gv.at Adresse gemacht werden. Damit wird sichergestellt in den Genuß von Synergien zu kommen, die zur Abgrenzung zu anderen Internetdiensten außerhalb der Verwaltung auf den Adressbereich *.gv.at aufbauen. Spezielle Behördendienste können somit nur über .gv.at Adressen angeboten werden. Beispielsweise darf eine Amtssignatur nur von einer Behörde ausgestellt werden. Beim Anbringen der Amtssignatur auf ein Dokument wird ein Signaturzertifikat benötigt, das eindeutig der Behörde zugeordnet werden kann (via den OID (Object Identifier) der Behörde). Neben dem OID stellt auch der Servername ein eindeutiges Merkmal dar (vgl. dazu (5.1) Datenübertragung via SSL).

(6.3) Verantwortlichkeiten B/O

Dem Bürger sollte in jedem Fall ein Kontakt für Fragen zum Webauftritt angeboten werden – vergleiche dazu die Kontaktmöglichkeiten unter (3.2).

Werden Applikationen und Services über die Webseite angeboten, ist in jedem Fall ein Kontakt für Probleme und technische Fragen anzubieten.

Um dem Bürger die Möglichkeit zu bieten sich mit einem inhaltlichen Problem oder mit einer inhaltlichen Frage zu einem speziellen Webinhalt an die entsprechende Person wenden zu können, kann auf allen Seiten ein inhaltlicher Ansprechpartner bzw. dessen Organisationspostfach vorhanden sein. Damit wird die Kontaktaufnahme sofort in die richtigen Kanäle geleitet.

Best Practice:
Während die Kontaktmöglichkeit für Fragen zum Webauftritt selbst über einen Hinweis bzw. über einen Link zur Kontaktseite bzw. über einen E-Mail-Link angeboten werden soll, kann die Kontaktmöglichkeit für Fragen zu speziellen Webinhalten über Metainformationen (vgl. (4.3) Dublin Core) gelöst sein.

(6.4) Einlaufadresse B

Wie in der E-Mail-Policy [EMAILPOL] in Kapitel 5.1 beschrieben, dürfen Anträge im Regelfall nur über die vorgesehenen Organisationspostfächer entgegen genommen werden. Dies ist entweder in der Domain-Policy zu dokumentieren und in der E-Mail-Policy zu referenzieren oder umgekehrt. Nach einer ordnungsgemäßen Entgegennahme bei diesen Organisationspostfächern (d.h. nach Viren- und Spamprüfung) muss sichergestellt sein, dass eine Benachrichtigung über den Erhalt bis spätestens zum Ende des nächsten Werktages an den Absender erfolgt bzw. über sonstige gleichwertige organisatorische

Maßnahmen die Entgegennahme dem Anbringenden garantiert werden (vgl. auch (3.3.1)). Für Anbringen über Webformulare an eine Behörde sei auf (3.3.1) verwiesen.

(7) Referenzen

[AMTSSIGFAQ]

Stabsstelle IKT-Strategie des Bundes: Häufig gestellte Fragen zur Amtssignatur. Abgerufen aus dem World Wide Web am 20.12.2004 unter http://www.cio.gv.at/faq/Amtssignatur/

[AMTSSIGZERT]

Gregor Karlinger: Amtssignaturzertifikate (ASZ) - Allgemeine Richtlinien für Amtssignaturzertifikate in der Verwaltung. Entwurf öffentlich, Version 1.0.0, 06.04.2005. Abgerufen aus dem World Wide Web am 10.05.2005 unter http://www.cio.gv.at/it-infrastructure/pki/officecertificates/

[AMTSSIGATRUST]

Gregor Karlinger. Amtssignaturzertifikate A-Trust (ASZ-ATRUST) - Prozessabläufe für Amtssignaturzertifikate beim Zertifizierungsdiensteanbieter A-Trust. Entwurf öffentlich, Version 1.0.0, 06.04.2005. Abgerufen aus dem World Wide Web am 10.05.2005 unter http://www.cio.gv.at/it-infrastructure/pki/officecertificates/

[ASIT-SSLTOOL]

SIT: A-SIT Toolsuite zur Evaluierung SSL fähiger Webbrowser und Server, Version 1.0 vom 02. Juni 2003. Abgerufen aus dem World Wide Web am 29.06.2004 unter http://demo.a-sit.at/ssltool/

[AVG]

Kundmachung: Wiederverlautbarung des Allgemeinen Verwaltungsverfahrensgesetzes. BGBlBGBl.Nr. 51/1991 ST0022. Ausgegeben am 31. Jänner 1991. Inkl. aller Änderungen. Abgerufen aus dem World Wide Web am 28. Februar 2005 unter http://ris.bka.gv.at/taweb-cgi/taweb?x=d&o=d&v=bgbl&d=BGBL&i=5750&p=1&q=und%2819830101%3C%3DDATUM%20und%2020031231%3E%3DDATUM%29%20%20%20und%20%2851/1991%29%3APORG%20%20

[DCMI]

Dublin Core Metadata Initiative, DCMI Metadata Terms bzw. Dublin Core Metadata Element Set, Version 1.1: Reference Description. Abgerufen aus dem World Wide Web am 29.06.2004 unter http://dublincore.org/documents/dcmi-terms/ bzw. http://dublincore.org/documents/1999/07/02/dces/

[ECG]

Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz – ECG). BGBl. I Nr. 152/2001. Ausgegeben am 21. Dezember 2001. Abgerufen aus dem World Wide Web am 29.06.2004 unter http://www.ris.bka.gv.at/taweb-cgi/taweb?x=d&o=r&v=bgblpdf&d=BGBLPDF&i=2648&p=5

[ECMASCRIPT]

ECMA Standardizing Information and Communication Systems: Standard ECMA-262, ECMAScript Language Specification, 3rd edition (December 1999). Abgerufen aus dem World Wide Web am 29.06.2004 unter http://www.ecma-international.org/publications/standards/Ecma-262.htm

[EGOVG]

Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen - E-Government-Gesetz (EGovG), BGBl. I Nr. 10/2004. Abgerufen aus dem World Wide Web am 01.06.2004 unter http://ris1.bka.gv.at/authentic/findbgbl.aspx?name=entwurf&format=pdf&docid=COO_2026_100_2_30412?name=entwurf&format=pdf&docid=COO_2026_100_2_30412

[EMAILPOL]

Micheal Liehmann, Bernd Martin: E-Mail-Policy. Konvention / Empfehlung, Version 2.0.2. Abgerufen aus dem World Wide Web am 31.05.2004 unter http://www.cio.gv.at/it-infrastructure/intpol/

[DOKFORMATE]

Michael Liehmann, Bernd Martin, Robert Wollendorfer: Dokumentenformate. Konvention / Empfehlung, Version 1.0.2. Abgerufen aus dem World Wide Web am 31.05.2005 unter http://www.cio.gv.at/it-infrastructure/intpol/

[DOMAINREG]

Helmut Hummer, Bernd Martin, Gerhard Schwarz: Internetdomänenverwaltung gv.at Naming- und Domänenregistrierungs-Policy. Konvention / Empfehlung, Version 1.0.0. Abgerufen aus dem World Wide Web am 31.05.2005 unter http://www.cio.gv.at/it-infrastructure/intpol/

[DSG2000]

Bundesgesetz über den Schutz personenbezogener Daten. (Datenschutzgesetz 2000 - DSG 2000). BGBl. I Nr. 165/1999. Ausgegeben am 17. August 1999. Abgerufen aus dem World Wide Web am 03.01.2005 unter http://www.ris.bka.gv.at/taweb-cgi/taweb?x=d&o=r&v=bgblpdf&d=BGBLPDF&i=593&p=1

[HTML]

Raggett, Dave; Le Hors, Arnaud; Jacobs, Ian: HTML 4.01 Specification W3C Recommendation 24 December 1999, Abgerufen aus dem World Wide Web am 29.06.2004 unter http://www.w3.org/TR/html4/

[INTPOL]

Bernd Martin, Robert Wollendorfer: Internet-Policy. Konvention / Empfehlung, Version 1.0.3. Abgerufen aus dem World Wide Web am 31.05.2005 unter http://www.cio.gv.at/it-infrastructure/intpol/

[OID]

Hollosi, Arno: Object Identifier und ihre Verwendung in X.509 Zertifikaten. Konvention zum e-Government Austria erarbeitet vom CIO des Bundes, Operative Unit. Öffentlicher Entwurf, Version 1.0.1, 06. August 2002. Abgerufen aus dem World Wide Web am 25. September 2002 unter http://reference.e-government.gv.at/

[RFC 2413]

S. Weibel, J. Kunze, C. Lagoze, M. Wolf: Dublin Core Metadata for Resource Discovery, Network Working Group, September 1998. Abgerufen aus dem World Wide Web am 15. Januar 2005 unter http://www.ietf.org/rfc/rfc2413.txt

[SGAD1.0.0]

Dr. Maria Wimmer, Mag. Franz Koch: Elektronische Übermittlung von Anbringen: Abschlussdialog, Konvention. *Noch nicht veröffentlicht.*

[SiHB]

Chief Information Office, IKT-Stabsstelle, Österreichisches IT-Sicherheitshandbuch Teil 1: IT-Sicherheitsmanagement Version 2. November 2004 und Teil 2: IT-Sicherheitsmaßnahmen Version 2, November 2004. Abgerufen aus dem World Wide Web am 15. Januar 2005 unter http://www.cio.gv.at/securenetworks/sihb/

[SiSt]

Besenmatter, Wolfgang: Sicherheitsstufen für die Kommunikation Bürger – Behörde im Bereich E-Government, Version 1.3 vom 24. Juli 2003. Abgerufen aus dem World Wide Web am 15. Juni 2004 unter http://www.cio.gv.at/securenetworks/si-stu/

[SERVERZERT]

Martin, Bernd: Serverzertifikate - Richtlinien für Serverzertifikate, Version 1.0.4 vom 11.04.2003. Abgerufen aus dem World Wide Web am 15. Juni 2004 unter http://www.cio.gv.at/it-infrastructure/pki/

[STYLEGUIDE]

Mittheisz, Johann, Wiesner, Harald: E-Government: Styleguide für E-Formulare, Version 1.3 vom 1. Juni 2004. Abgerufen aus dem World Wide Web am 29.06.2004 unter http://reference.e-government.gv.at/Styleguide stg 1 3 0 - Versi.505.0.html

[PKI]

Posch, Reinhard; Leiningen-Westerburg, Alexander: Allgemeine Richtlinien für den Einsatz von PKI in der Verwaltung, Version 0.9 vom 10. April 2003. Abgerufen aus dem World Wide Web am 15. Juni 2004 unter http://www.cio.gv.at/it-infrastructure/pki/

[WAI-CHECKLIST]

Wendy Chisholm, Gregg Vanderheiden, Ian Jacobs: Checklist of Checkpoints for Web Content Accessibility Guidelines 1.0, 1999. Abgerufen aus dem World Wide Web am 29.06.2004 unter http://www.w3.org/TR/WAI-WEBCONTENT/full-checklist.html

[WAI-GUIDELINES]

Wendy Chisholm, Gregg Vanderheiden, Ian Jacobs: Web Content Accessibility Guidelines 1.0, W3C Recommendation 5-May-1999. Abgerufen aus dem World Wide Web am 29.06.2004 unter http://www.w3.org/TR/WAI-WEBCONTENT/wai-pageauth.html

[XHTML]

Pemberton, Steven; Austin, Daniel; Axelsson, Jonny; Çelik, Tantek; et. al: XHTML™ 1.0 The Extensible HyperText Markup Language (Second Edition), A Reformulation of HTML 4 in XML 1.0, W3C Recommendation 26 January 2000, revised 1 August 2002. Abgerufen aus dem World Wide Web am 29.06.2004 unter http://www.w3.org/TR/xhtml1/

[XHTMLBasic]

Baker, Mark; Ishikawa, Masayasu; Matsui, Shinichi; Stark, Peter; Wugofski, Ted; Yamakami, Toshihiko: XHTML™ Basic W3C Recommendation 19 December 2000. Abgerufen aus dem World Wide Web am 29.06.2004 unter http://www.w3.org/TR/xhtml-basic/

Historie

<table>
<tr><td>Version
1.0.0</td><td>Datum
03.05.2005</td><td rowspan="2">Kommentar
Initialversion erstellt.</td></tr>
<tr><td colspan="2">Ersteller
Bernd Martin
Michael Liehmann</td></tr>
<tr><td>Version
1.0.1</td><td>Datum
25.08.2005</td><td rowspan="2">Kommentar
• Punkt (3): Entfernen von Linkempfehlungen und Aufnahme generelle Vorgabe für Veröffentlichung bzw. Platzierung der Inhalte (inkl. Best Practice)
• Punkt (3.1): Verweis auf Internet-Policy anstelle Kopie des Inhalts. Entfernen des vorgeschlagenen Links.
• Punkt (3.1): Entfernen des vorgeschlagenen Links.
• Punkt (3.2): Entfernen des vorgeschlagenen Links.
• Punkt (3.3): Entfernen des vorgeschlagenen Links.
• Punkt (3.6.1): Klarstellung, dass E-Mail-Adressen nur optional anzuführen sind.
• Punkt (3.11): Bessere Formulierung des 2ten Absatzes.
• Punkt (4.5): Bildschirmauflösung wurde auf Stand der Technik definiert.
• Punkt (5.3): Klarstellung, dass nur das jeweils geltende Sicherheitshandbuch anzuwenden sei.</td></tr>
<tr><td colspan="2">Ersteller
Bernd Martin</td></tr>
</table>