Seite

Sanierung der Kreuzbachbrücke bei Aßlar-Werdorf, Lahn-Dill-Kreis, im Zuge der A 45 (Baubeginn von Netzknoten [NK] 5215 029 nach NK 5215 038, Stat. km 2+300; Bauende von NK 5215 029 nach NK 5215 038, Stat. km 2+600) . . 135

Sanierung der Marbachbrücke bei Dillenburg, Lahn-Dill-Kreis, im Zuge der A 45 (Baubeginn von Netzknoten [NK] 5215 015 nach NK 5215 016, Stat. km 1+460; Bauende von NK 5215 015 nach NK 5215 016, Stat. km 1+900) 135

Sanierung der Talbrücke Kalteiche bei Haiger-Allendorf, Lahn-Dill-Kreis, im Zuge der A 45 (Baubeginn von Netzknoten [NK] 5214 402 nach NK 5215 015, Stat. km 0+200; Bauende von NK 5214 402 nach NK 5215 015, Stat. km 0+620) 135

Seite

Neubau einer Autobahnmeisterei in Wildeck OT Hönebach, Landkreis Hersfeld-Rotenburg 136

Hessischer Verwaltungsschulverband

Fortbildungsveranstaltung des Verwaltungsseminars Wiesbaden 136

Buchbesprechungen 137

Öffentlicher Anzeiger 138

Andere Behörden und Körperschaften

Zweckverband Oberhessische Versorgungsbetriebe, Friedberg (Hessen); hier: Beschluss über den Nachtragswirtschaftsplan 2009 und Bekanntmachung sowie Beschluss über den Wirtschaftsplan 2010 und Bekanntmachung 158

Wasser- und Bodenverband „Marburger Land“ in Amöneburg im Landkreis Marburg-Biedenkopf; hier: Neufassung der Satzung 159

Seite

Wasserbeschaffungsverband Taunus, Oberursel; hier: Beschluss über die Jahresrechnung 2008 und die Entlastung des Verbandsvorstandes für das Haushaltsjahr 2008 sowie die öffentliche Auslegung der Jahresrechnung 2008 164

Zweckverband Tierkörperbeseitigung in Rheinland-Pfalz, im Saarland, im Rheingau-Taunus-Kreis und im Landkreis Limburg-Weilburg, Rivenich; hier: Bekanntmachung einer öffentlichen Verbandsversammlung 164

Verband Region Rhein-Neckar, Mannheim; hier: 14. Sitzung des Ausschusses für Regionalentwicklung und Regionalmanagement sowie Haushaltssatzung für das Haushaltsjahr 2010 165

Öffentliche Ausschreibungen 166

Stellenausschreibungen 166

HESSISCHE STAATSKANZLEI

84

Verleihung des Verdienstordens der Bundesrepublik Deutschland

Der Bundespräsident hat auf meinen Vorschlag an folgende verdiente Frauen und Männer den Verdienstorden der Bundesrepublik Deutschland verliehen:

	Urkundendatum:
Großes Verdienstkreuz	
Hay Keong Yang, Bad Soden am Taunus	21. 9. 2009
Verdienstkreuz 1. Klasse	
Berthold Weikert, Hadamar	19. 8. 2009
Verdienstkreuz am Bande	
Margurit Aßmann, Frankfurt am Main	4. 12. 2009
Peter Friis, Rockenberg	8. 9. 2009
Erwin Gerhardt, Ulrichstein	25. 9. 2009
Gitta Hentschker-Kranixfeld, Felsberg	8. 9. 2009
Waldemar Högen, Selters (Taunus)	24. 8. 2009
Karin Müller, Weilrod	11. 8. 2009
Konrad Pätzold, Witzenhausen	8. 9. 2009
Dipl.-Ing. Henner Reiße, Kassel	8. 9. 2009
Verdienstkreuz am Bande	
Reinhold Schmidt, Solms	8. 5. 2009
Manfred Seibert, Groß-Gerau	8. 5. 2009
Raimer Thienhaus, Hasselroth	25. 9. 2009
Josef Welzel, Hadamar	11. 8. 2009
Jacqueline Wörner-van Munster. Erbach (Odenwald)	17. 3. 2009
Karl Dietrich Wolff, Frankfurt am Main	8. 9. 2009
Verdienstmedaille	
Dagmar Adomeit, Frankenberg (Eder)	19. 8. 2009
Gertrud Blumenauer, Breitenbach am Herzberg	25. 9. 2009
Roselinde Hartmann, Korbach	6. 6. 2009
Elfriede Lienert, Rüsselsheim	8. 9. 2009
Edith Paul, Offenbach am Main	14. 10. 2009
Birgit Quiel, Oestrich-Winkel	24. 8. 2009
Willy Welsch, Biedenkopf	12. 8. 2008
Irmgard Zuhse, Neuenstein	14. 10. 2009

Wiesbaden, 8. Januar 2010

Der Hessische Ministerpräsident
PV 2.1 – PRO 04

StAnz. 4/2010 S. 106

HESSISCHES MINISTERIUM DES INNERN UND FÜR SPORT

85

Informationssicherheitsleitlinie für die Hessische Landesverwaltung

Im Jahre 2005 hat die Hessische Landesregierung erstmals verbindliche IT-Sicherheitsleitlinien in Kraft gesetzt. Diese Leitlinien, orientiert an den Grundschutzempfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), haben ihre Wirkung entfaltet und zu einem insgesamt höheren Sicherheitsniveau in der Landesverwaltung beigetragen.

Der technische Wandel, Erfahrungen bei der Nutzung der Leitlinie sowie Veränderungen in den nationalen und internationalen Regelwerken und Standards für die IT-Sicherheit machten eine Überprüfung und Neufassung dieser Leitlinien erforderlich. Auch der Hessische Rechnungshof empfahl eine Überarbeitung der Leitlinie.

Die IT-Sicherheitsleitlinie wurde daher im Rahmen des von der Staatskanzlei und allen Ressorts getragenen Arbeitskreises der IT-Sicherheitsbeauftragten überprüft und als IT-Informationssicherheitsleitlinie einvernehmlich neu gefasst. Der Hessische Datenschutzbeauftragte hat an dieser Neufassung mitgewirkt und ihr zugestimmt.

Das Kabinett hat die im Folgenden wiedergegebene Leitlinie zur Kenntnis genommen und bittet die Ressorts die Leitlinie in den Dienststellen der hessischen Landesverwaltung umzusetzen.

1. Vorbemerkung

Die Prozesse zur Aufgabenerfüllung in der hessischen Landesverwaltung werden durch die Informations- und Telekommunikationstechnologie (ITK) in miteinander vernetzten Systemen unterstützt. Vor diesem Hintergrund ist eine angemessene Informationssicherheit nachhaltig zu gewährleisten. Danach sind

- organisatorische Rahmenbedingungen zur Gewährleistung der Informationssicherheit aufrechtzuerhalten und weiterzuentwickeln,
- das Informationssicherheitsmanagement kontinuierlich zu verbessern,
- abgestimmte Sicherheitsstandards einschließlich der Definition von Verantwortlichkeiten und Befugnissen fortzuschreiben,
- Komponenten zur Steigerung der Informationssicherheit zu zentralisieren und standardisieren und alle Sicherheitsvorkehrungen und -maßnahmen hinreichend zu dokumentieren.

Die Regelungen dieser Informationssicherheitsleitlinie sind vom zentralen Informationssicherheitsmanagement der Hessischen Landesverwaltung zu erstellen und orientieren sich sowohl an den Grundschutz-Standards und Grundschutzkatalogen des Bundesamts für Sicherheit in der Informationstechnik (BSI) als auch an den Empfehlungen der DIN ISO/IEC 27001 beziehungsweise 27001 ff. Sie wurden von der Landesregierung gebilligt und sind mit ihrer Veröffentlichung für den Einsatz in der ITK der Landesverwaltung verbindlich.

2. Grundsätze

In Abwägung der Werte der zu schützenden Informationen, der Risiken sowie des Aufwands an Personal und Finanzmitteln für Informationssicherheit soll für eingesetzte und geplante ITK-Systeme in der Hessischen Landesverwaltung ein angemessenes Informationssicherheitsniveau angestrebt und erreicht werden. Für ITK-Systeme mit normalem Schutzbedarf sind Sicherheitsmaßnahmen – ausgehend von den Grundschutz-Standards und Grundschutzkatalogen des BSI sowie von den internationalen Normen DIN ISO/IEC 27001 ff. – vorzusehen und umzusetzen. Für Bereiche, in denen ein höherer Schutzbedarf festgestellt wird, müssen ergänzende Sicherheitsmaßnahmen eingeführt und dokumentiert werden.

3. Ziele

3.1 Alle Beschäftigten gewährleisten die Informationssicherheit durch ihr verantwortliches Handeln und halten die für die Informationssicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen ein.

3.2 Für den ITK-Einsatz sind die Sicherheitsziele Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität und weiter die Ziele Verbindlichkeit und Verkehrsfähigkeit im jeweils erforderlichen Maße zu erreichen. Die daraus abgeleiteten Sicherheitsmaßnahmen sind auch dann anzuwenden, wenn sich daraus Beeinträchtigungen für die ITK-Nutzung ergeben.

3.3 Die Sicherheit der ITK-Verfahren ist neben der Leistungsfähigkeit und Funktionalität zu gewährleisten. Bleiben im Einzelfall trotz der Sicherheitsvorkehrungen Risiken untragbar, ist an dieser Stelle auf den ITK-Einsatz zu verzichten.

4. Maßnahmen

4.1 Für bereits betriebene und für geplante Informations- und Telekommunikationstechnik sind IT-Sicherheitskonzepte zu erstellen. Im Rahmen dieses Verfahrens sind die personalvertretungsrechtlichen Beteiligungsrechte zu wahren.

4.2 Um den möglichen Risiken und Schäden vorzubeugen, sind rechtliche, organisatorische, technische, personelle und infrastrukturelle Maßnahmen zur Informationssicherheit auf Grundlage einer Bewertung umzusetzen.

4.3 Die Verantwortlichen haben bei Verstößen und Beeinträchtigungen die zur Aufrechterhaltung des ITK-Betriebes und der Informationssicherheit geeigneten und angemessenen Maßnahmen zu ergreifen.

4.4 Der Zugriff auf ITK-Systeme, -Anwendungen und Daten und Informationen ist auf den unbedingt erforderlichen Personenkreis zu beschränken. Jeder/jede Bedienstete erhält nur auf diejenigen Daten und Informationen die Zugriffsberechtigungen, die zur Erfüllung der dienstlichen Aufgaben erforderlich sind.

4.5 Sofern Verfahren und Tools eingesetzt werden, sind sie nach dem jeweiligen Stand der Technik auszuwählen und einzusetzen.

4.6 Die für die Umsetzung der Informationssicherheitsmaßnahmen erforderlichen Ressourcen und Investitionsmittel sind bereitzustellen.

4.7 Die Wirksamkeit der Sicherheitsmaßnahmen ist im Sinne eines kontinuierlichen Verbesserungsprozesses regelmäßig zu kontrollieren, zu dokumentieren und weiterzuentwickeln.

5. Verantwortlichkeiten

5.1 Die Dienststellenleitung trägt in dem Bereich, den sie beeinflussen kann, die Verantwortung für eine angemessene Informationssicherheit.

5.2 Ein IT-Sicherheitsbeauftragter/eine Sicherheitsbeauftragte wird in jeder Dienststelle eingesetzt und im Geschäftsverteilungsplan ausgewiesen. Der/die Sicherheitsbeauftragte ist verantwortlich für die Wahrnehmung aller Belange der Informationssicherheit innerhalb seines Zuständigkeitsbereiches, kann sich unmittelbar an die Dienststellenleitung wenden und leitet das IT-Sicherheitsmanagementteam.

5.3 Ein IT-Sicherheitsmanagementteam besteht aus dem beziehungsweise der IT-Sicherheitsbeauftragten, dem beziehungsweise der behördlichen Datenschutzbeauftragten, dem beziehungsweise der Zuständigen für den ITK-Service/ITK-Betrieb und in angemessenem Umfang Vertreterinnen beziehungsweise Vertretern der Fachanwendungen. Es gehört unter anderem zu seinen Aufgaben, das ITK-Sicherheitskonzept der Dienststelle fortzuschreiben und Maßnahmen umzusetzen, die zu einem angemessenen und dem Stand der Technik entsprechenden Informationssicherheitsniveau in seinen Bereich führen.

5.4 Die Beschäftigten sind dafür verantwortlich, dass die Sicherheitsmaßnahmen in dem von ihnen beeinflussbaren Bereich umgesetzt werden. Hierbei werden sie durch wiederholte sensibilisierende Schulung und Benutzerbetreuung am Arbeitsplatz unterstützt. Im Rahmen der jeweiligen Möglichkeiten sollen die Beschäftigten Sicherheitsvorfälle von innen und außen vermeiden sowie sicherheitsrelevante Ereignisse den Zuständigen umgehend melden, damit schnellstmöglich Abhilfemaßnahmen eingeleitet werden können.

5.5 Für alle Verfahren, Informationen, ITK-Anwendungen und ITK-Systeme werden verantwortliche Personen benannt, die den jeweiligen Schutzbedarf und die Zugriffsberechtigungen bestimmt. Dabei sind – unter Berücksichtigung von Finanzierbarkeit und Wirtschaftlichkeit – die jeweils angemessenen Sicherheitsmaßnahmen zu ergreifen.

5.6 Ein Auftragnehmer (vergleiche § 4 HDSG), der für die Verwaltung Leistungen erbringt, hat Vorgaben des Auftraggebers zur Einhaltung der Informationssicherheitsziele (Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität) und der weiteren Ziele Verbindlichkeit und Verkehrsfähigkeit gemäß dieser Informationssicherheitsleitlinie einzuhalten. Der Auftraggeber hat Sicherheitsanforderungen vertraglich festzulegen und deren Einhaltung zu kontrollieren. Der Auftraggeber hat den Auftragnehmer zu verpflichten, bei erkennbaren Mängeln oder Risiken eingesetzter Sicherheitsmaßnahmen den Auftraggeber zu informieren.

5.7 Die Einhaltung der Informationssicherheit bei der Verarbeitung, Nutzung und Kontrolle von Daten und Informationen ist zu überprüfen. Art und Umfang der Kontrolle sind von der Dienststellenleitung auf der Grundlage des jeweiligen Sicherheitskonzeptes festzulegen. Eine Kontrolle kann durch unabhängige Dritte erfolgen. In diesem Fall ist zu gewährleisten, dass keine unzulässige Kenntnisnahme von Daten und Informationen damit verbunden ist.

5.8 Zur Koordination der landesweiten Sicherheitsprozesse und zur Unterstützung und Beratung des IT-Sicherheitsmanagements in den Ressorts sowie zur Abstimmung und Koordination ressortübergreifender, gemeinsamer Maßnahmen zur Informationssicherheit richtet das HMdIS einen ständigen Arbeitskreis für die IT-Sicherheitsbeauftragten der Ressorts ein.

6. Verstöße und Folgen

Verhalten, das die Sicherheit von Daten, Informationen, ITK-Systemen oder des Netzes gefährdet, kann disziplinar- oder arbeitsrechtlich geahndet werden. Unter Umständen kann das Verhalten als Ordnungswidrigkeit oder als Straftat verfolgt werden. Als Straftat kommen insbesondere in Betracht:

- das unbefugte Verschaffen von Daten anderer, die gegen unberechtigten Zugang besonders gesichert sind (§§ 202a, 274 Abs. 1 Nr. 2 StGB)
- die Verletzung von Privatgeheimnissen (§ 203 StGB)
- die Verletzung von Fernmeldegeheimnissen (§ 206 StGB)
- der Computerbetrug durch unrichtige Gestaltung eines Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder durch unbefugte Einwirkung auf den Ablauf (§ 263a StGB)
- die fälschliche Beeinflussung einer Datenverarbeitung (§§ 270, 269 StGB), das rechtswidrige Löschen, Unter-

drücken, Unbrauchbarmachen oder Verändern von Daten (§ 303a StGB)

- das Zerstören, Beschädigen, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers (§ 303b StGB)
- die Verwendung personenbezogener Daten entgegen den Vorschriften des HDSG (§ 40 HDSG).

Beschäftigte, die die Sicherheit von Daten, Informationen, ITK-Systemen oder des Netzes gefährden und einen Schaden für das Land oder einen Dritten verursachen, können darüber hinaus zum Schadenersatz (§ 48 BeamtStG, § 3 Abs. 7 TV-H, § 823 BGB) herangezogen werden oder einem Rückgriffanspruch (Art. 34 GG in Verbindung mit § 839 BGB) ausgesetzt sein.

7. Umsetzung

Diese Informationssicherheitsleitlinie ist allen Beschäftigten in geeigneter Weise bekannt zu geben. Auf der Grundlage dieser Leitlinie haben die Ressorts ihre Informationssicherheit umzusetzen.

8. Bekanntgabe

Diese Informationssicherheitsleitlinie tritt am 1. Januar 2010 in Kraft.

Wiesbaden, 6. Januar 2010

Hessisches Ministerium des Innern und für Sport
VII 3 W 020 103
– Gült.-Verz. 300 –
StAnz. 4/2010 S. 106

HESSISCHES MINISTERIUM DER FINANZEN

86

Anpassung des Basiszinssatzes des Bürgerlichen Gesetzbuches (BGB) zum 1. Januar 2010;

hier: Erhebung von Verzugszinsen (VV zu § 34 LHO)

Laut Pressenotiz der Deutschen Bundesbank vom 29. Dezember 2009 beträgt der Basiszinssatz nach § 247 BGB mit Beginn des 1. Januar 2010 unverändert 0,12 Prozent.

Ich bitte, diesen Zinssatz ab 1. Januar 2010 bei der Berechnung von Verzugszinsen auch weiterhin zugrunde zu legen.

In Kürze wird diese Bekanntmachung in das Mitarbeiterportal des Landes Hessen unter Finanzen > Basiszinssatz § 247 BGB eingestellt.

Wiesbaden, 8. Januar 2010

Hessisches Ministerium der Finanzen
H 1007 B – 001/2010 – III 1.2
StAnz. 4/2010 S. 108

HESSISCHES MINISTERIUM DER JUSTIZ, FÜR INTEGRATION UND EUROPA

87

Einundzwanzigste Verordnung zur Änderung der Verordnung über die Ortsgerichte im Lande Hessen

Vom 29. Oktober 2009

Aufgrund des § 1 Abs. 2 Satz 1 des Ortsgerichtsgesetzes in der Fassung vom 2. April 1980 (GVBl. I S. 114), zuletzt geändert durch Gesetz vom 17. Dezember 1998 (GVBl. I S. 562), wird im Benehmen mit dem Minister des Innern und für Sport verordnet:

Artikel 1

In § 4 Satz 2 der Verordnung über die Ortsgerichte im Lande Hessen vom 1. September 1980 (JMBl. S. 792, 1039), zuletzt geändert durch Verordnung vom 8. Januar 2009 (JMBl. S. 195), wird die Zahl „2009“ durch „2014“ ersetzt.

Artikel 2

Diese Verordnung tritt am Tage nach der Verkündung in Kraft.

Wiesbaden, 29. Oktober 2009

Der Hessische Minister der Justiz, für Integration und Europa
gez. H a h n
– Gült.-Verz. 28 –
JMBl. 2009 S. 559
StAnz. 4/2010 S. 108

88

Geschäftsverteilungsplan des Oberlandesgerichts Frankfurt am Main für das Geschäftsjahr 2010

A. Senate

1. Strafsenat

Er bearbeitet:

a) die Revisionen in Strafsachen (Ss- und Vs-Register) aus dem Landgerichtsbezirk Frankfurt am Main, mit Ausnahme der Verkehrsstrafsachen, sowie aus den Landgerichtsbezirken Limburg a. d. Lahn und Fulda, einschließlich der sie betreffenden Entscheidungen,

b) die Haftbeschwerden und die Beschwerden gegen die einstweilige Unterbringung nach § 126a StPO und Beschwerden im Rahmen des § 275a Abs. 5 StPO – mit Ausnahme der Fälle des § 275a Abs. 5 S. 2 StPO, wenn auch über die Erledigung der Unterbringung zu entscheiden ist – hierfür ist der 3. Strafsenat zuständig –, sowie die Entscheidungen nach § 122 StPO und § 122 StPO analog in Verbindung mit § 126a Abs. 2 S. 2 StPO aus dem ganzen Oberlandesgerichtsbezirk, soweit nicht der 4. oder 5. Strafsenat nach § 120 GVG und § 121 Abs. 4 S. 1 StPO sowie § 121 Abs. 4 StPO analog in Verbindung mit § 126a Abs. 2 S. 2 StPO zuständig ist,

c) alle Entscheidungen, die die Wiederaufnahme des Verfahrens betreffen, aus dem ganzen Oberlandesgerichtsbezirk, soweit nicht der 5. Strafsenat zuständig ist,