MINISTERIUM FÜR INNERES, DIGITALISIERUNG UND MIGRATION

Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit (VwV Informationssicherheit)

Vom 7. April 2017 – 5-0275.0/25 –

INHALTSVERZEICHNIS

1 Zielsetzung

Für die Landesverwaltung Baden-Württemberg ist eine sichere Informations- und Kommunikationstechnik von höchster Bedeutung. Sie resultiert aus der Verpflichtung des Staates gegenüber den Bürgern und der Wirtschaft, verantwortungsvoll bei der Erhebung, Speicherung, Übermittlung und Nutzung von Daten vorzugehen.

Diese Verwaltungsvorschrift legt die Ziele, Grundsätze, Organisationsstrukturen und Maßnahmen fest, die für die Etablierung eines ganzheitlichen Informationssicherheitsprozesses in der Landesverwaltung Baden-Württemberg erforderlich sind. Die Vorgehensweise orientiert sich am IT-Grundschutz (IT = Informationstechnik) des Bundesamts für Sicherheit in der Informationstechnik (BSI) und entspricht einer Informationssicherheitsleitlinie in der Terminologie des IT-Grundschutzes. Diese Verwaltungsvorschrift soll auch eine sichere und verlässliche Kommunikation und Kooperation mit dem Bund, mit den Ländern und mit dem kommunalen Bereich gewährleisten.

Anstelle des in der Literatur oft synonym verwendeten Begriffs »IT-Sicherheit« wird hier die weitergehende Formulierung »Informationssicherheit« verwendet. Entsprechend der Empfehlung im BSI Standard 100-1 wird Informationssicherheit umfassend und ganzheitlich verstanden, sie umfasst auch die Begriffe »Informations- und Kommunikationstechnik« und »Informations- und Telekommunikationstechnik« und bezieht sich auf den Schutz von Informationen jeglicher Art und Herkunft, unabhängig davon, ob diese in technischen Systemen, auf Papier oder in Köpfen gespeichert sind.

Die Ziele im Einzelnen sind:

- Hohe Verlässlichkeit beim Umgang mit Informationen,
- Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen,
- Vermeidung von Datenverlust,
- Sicherung der Qualität der Informationen,
- Gewährleistung der Einhaltung der gesetzlichen Anforderungen,
- Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb der Landesverwaltung Baden-Württemberg und in der Zusammenarbeit mit anderen Stellen,
- Investitionsschutz, das heißt Erhaltung der in Technik, Informationen, Arbeitsprozesse und Wissen investierten Werte,
- Reduzierung der im Schadensfall entstehenden Kosten sowie
- Vermeidung von Reputationsschäden.

2 Geltungsbereich

Diese Verwaltungsvorschrift gilt für alle Dienststellen und Einrichtungen der Landesverwaltung Baden-Württemberg. Dem Landtag, dem Rechnungshof, dem Landesbeauftragten für den Datenschutz sowie dem kommunalen Bereich wird die Anwendung empfohlen. Sofern sich aus anderen Regelungen weitergehende Anforderungen an die Informationssicherheit ergeben, bleiben diese unberührt.

3 Sicherheitsgrundsätze

3.1 Alle Dienststellen und Einrichtungen der Landesverwaltung Baden-Württemberg setzen die Informationssicherheit gemäß IT-Grundschutz (BSI Standards 100-1 bis 100-3) um.

3.2 Für die Landesverwaltung Baden-Württemberg wird ein Informationssicherheitsmanagementsystem (ISMS) in Anlehnung an die internationalen Standards (ISO = International Standardization Organization) unter Berücksichtigung des nationalen BSI Standards 100-1 »Managementsysteme für Informationssicherheit« eingeführt (ISO 27001 in der Ausprägung BSI IT-Grundschutz). Dieses ISMS umfasst Ressourcen, Prozesse und Konzepte für die Informationssicherheit in der Landesverwaltung Baden-Württemberg.

3.3 Die ebenenübergreifende Zusammenarbeit zwischen Bund, Ländern und Kommunen wird berücksichtigt.

3.4 Die Notfallvorsorge und -bewältigung erfolgt gemäß den Vorgaben aus dem BSI Standard 100-4 »Notfallmanagement«.

3.5 Informationssicherheit erfordert personelle, organisatorische, rechtliche und technische Maßnahmen.

3.6 Informationssicherheit ist als kontinuierlicher Prozess zu gestalten. Der Prozess umfasst insbesondere die mindestens jährlich dokumentierte Überprüfung der Umsetzung und Wirksamkeit von Sicherheitsmaßnahmen und gegebenenfalls erforderliche Anpassungen.

3.7 Der Zugriff auf IT-Systeme, -Anwendungen, Daten und Informationen ist unter Abwägung des Schutzbedarfs und der Wirtschaftlichkeit auf den unbedingt

erforderlichen Personenkreis zu beschränken. Bedienstete erhalten nur auf diejenigen Daten und Informationen die Zugriffsberechtigungen, die zur Erfüllung der jeweiligen dienstlichen Aufgaben erforderlich sind.

3.8 Beim Einsatz von Informations- und Kommunikationstechnik sind Verfügbarkeit, Vertraulichkeit und Integrität im jeweils erforderlichen Maße zu erreichen. Dazu sind angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahmen zu ergreifen.

3.9 Notwendige Sicherheitsmaßnahmen sind auch dann anzuwenden, wenn sich daraus Beeinträchtigungen für die Nutzung von IT-Systemen ergeben.

3.10 Die angemessene Sicherheit der in der Landesverwaltung Baden-Württemberg eingesetzten IT-Verfahren ist neben der Leistungsfähigkeit und Funktionalität zu gewährleisten. Bleiben im Einzelfall trotz der Sicherheitsvorkehrungen Risiken untragbar, ist an dieser Stelle auf den IT-Einsatz zu verzichten.

3.11 Die Ressorts sorgen dafür, dass Sicherheitskonzepte sowohl für das jeweilige Ressort als auch für alle Dienststellen und Einrichtungen erstellt und regelmäßig bedarfsgerecht fortgeschrieben werden. Gleichermaßen sorgen sie für die notwendigen verfahrens- bzw. anwendungsbezogenen Sicherheitskonzepte. Soweit für einzelne Verfahren keine Sicherheitskonzepte erforderlich sind, wird dies jeweils aktenkundig begründet. Das Ziel ist, dass jedes Ressort und jede Dienststelle und Einrichtung jeweils die eigenen Verfahren und Anwendungen, die damit verarbeiteten Daten und deren Schutzbedarf kennt und darüber auskunftsfähig ist. Diese Anforderung ergibt sich insbesondere aus der EU-Datenschutz-Grundverordnung.

4 Sicherheitsstrategie

Die Sicherheitsstrategie der Landesregierung ist es, das jeweils notwendige Sicherheitsniveau mit wirtschaftlichem Ressourceneinsatz zu erreichen und zu halten. Hierzu wird durch die Einführung eines ISMS ein kontinuierlicher Prozess etabliert, der sicherstellt, dass das Sicherheitsniveau den jeweiligen Anforderungen jederzeit bedarfsgerecht angepasst und fortgeschrieben wird. Wesentliche Elemente dieses ISMS sind Planung, Umsetzung, Überprüfung und Aufrechterhaltung des Prozesses. Dabei kann anstelle der Umsetzung aller Maßnahmen des IT-Grundschutzes auch ein risikobasierter Ansatz gewählt werden. Dabei werden die Risiken klassifiziert und bewertet und in der Folge genau diejenigen Maßnahmen ergriffen, die notwendig sind, um das Risiko auf ein tragbares Maß zu reduzieren.

5 Sicherheitsorganisation

Die Sicherheitsorganisation in der Landesverwaltung Baden-Württemberg berücksichtigt die behördlichen Strukturen und weist dementsprechend Rollen und Aufgaben auf Landes-, Ressort- und Dienststellen- oder Einrichtungsebene zu. Sie zielt mit der proaktiven Einführung des ISMS auf eine effiziente und reaktionsstarke Vernetzung der für Informationssicherheit verantwortlichen Personen in den Strukturen und Gremien ab. Die Gesamtverantwortung für die ordnungsgemäße und sichere Aufgabenerfüllung und damit auch für die Informationssicherheit verbleibt jeweils bei der Leitung (Leitung des Landes, des Ressorts, der Dienststelle oder der Einrichtung). Dazu gehört auch die Verantwortung für eine angemessene Aus- und Weiterbildung und für die Sensibilisierung für Sicherheitsthemen (Security-Awareness). Bei der Festlegung und Umsetzung von Sicherheitsanforderungen in Dienststellen und Einrichtungen der Landesverwaltung Baden-Württemberg, die der Fachaufsicht durch mehrere Ressorts unterliegen, bedarf es der frühzeitigen Abstimmung und Zusammenarbeit dieser Ressorts.

5.1 Die Grundsätze der Sicherheitsorganisation sind:

5.1.1 Für die Landesverwaltung Baden-Württemberg, für jedes Ressort und unter Berücksichtigung der behördlichen Strukturen grundsätzlich für jede Einrichtung und Dienststelle werden jeweils Informationssicherheitsbeauftragte bestellt.

5.1.2 Daneben können von den Leitungen der Dienststellen und Einrichtungen in Abstimmung mit den jeweiligen Ressorts Bereichs-Informationssicherheitsbeauftragte beziehungsweise Projekt- oder System-Informationssicherheitsbeauftragte gemäß BSI Standard 100-2 benannt werden.

5.1.3 Informationssicherheitsbeauftragte können Informationssicherheits-Management-Teams gemäß BSI Standard 100-2 bilden.

5.1.4 Die für die Sicherheitsprozesse erforderlichen Ressourcen werden im notwendigen Umfang durch die jeweils verantwortlichen Organisationseinheiten bereitgestellt.

5.2 Aufgabenträger und Organisationseinheiten für die Informationssicherheit in der Landesverwaltung Baden-Württemberg sind:

5.2.1 Eine übergeordnete Informationssicherheitsbeauftragte oder ein übergeordneter Informationssicherheitsbeauftragter für die Landesverwaltung Baden-Württemberg (Chief Information Security Officer, CISO). Die Inhaberin oder der Inhaber dieser Funktion wird vom Innenministerium Baden-Württemberg benannt. Die oder der CISO kann sich unmittelbar an die Landesregierung wenden. In der Zuständigkeit der oder des CISO liegt die landesweite Förderung, Koordinierung und Abstimmung aller erforderlichen Belange des ISMS. Zu ihren oder seinen Aufgaben gehört insbesondere:

5.2.1.1 Allgemeingültige Richtlinien und Grundsätze für Maßnahmen in der Informationssicherheit in der Landesverwaltung Baden-Württemberg in Abstimmung mit dem Arbeitskreis Informationstechnik (AK-IT) festzulegen und fortzuschreiben.

5.2.1.2 Die Beauftragte oder den Beauftragten der Landesregierung für die Informationstechnologie (CIO) bei ihrer oder seiner Aufgabenwahrnehmung bezüglich

der Informationssicherheit zu beraten und sie oder ihn bei der Umsetzung zu unterstützten.

5.2.1.3 Die Leitung der Koordinierungsgruppe Informationssicherheit der Landesverwaltung Baden-Württemberg (KG InfoSic).

5.2.1.4 Die Erstellung eines jährlichen Sicherheitsberichts in Abstimmung mit dem AK-IT zur Vorlage an die oder den CIO. Dieser enthält Angaben zum Stand der Umsetzung und Wirksamkeit von Sicherheitsmaßnahmen und der gegebenenfalls erforderlichen Fortschreibung der jeweiligen Leitlinien, Richtlinien und Sicherheitskonzepte. Dabei unterstützen sie oder ihn die jeweiligen Informationssicherheitsbeauftragten der Ressorts insbesondere durch Zulieferung der Beiträge aus ihren Ressorts. Sie werden dabei ihrerseits unterstützt von den Informationssicherheitsbeauftragten der Dienststellen oder Einrichtungen und den Informationssicherheitsbeauftragten für Verfahren, Informationen, IT-Systeme und -Anwendungen. Das Computer Notfallteam (Computer Emergency Response Team = CERT) CERT BWL unterstützt ebenfalls mit einem Lagebericht zu Sicherheitsvorfällen und zur aktuellen Situation.

5.2.2 *Eine Informationssicherheitsbeauftragte oder ein Informationssicherheitsbeauftragten für jeden Ressortbereich (Ressort-CISO)*

Die Inhaberin oder der Inhaber dieser Funktion wird vom jeweiligen Ressort benannt. Die oder der Ressort-CISO kann sich unmittelbar an die Ressortleitung wenden und ist Mitglied in der Koordinierungsgruppe Informationssicherheit der Landesverwaltung Baden-Württemberg.

In der Zuständigkeit der oder des Ressort-CISO liegt die Förderung, Koordinierung und Abstimmung aller erforderlichen Belange der Informationssicherheit für Verfahren, Anwendungen und Informationen im Ressortbereich. Zu ihren oder seinen Aufgaben gehört insbesondere:

5.2.2.1 Sicherheitstechnische Vorgaben und Maßnahmen für Informationssicherheitskonzepte der Dienststellen oder Einrichtungen im Ressortbereich festzulegen und fortzuschreiben.

5.2.2.2 Die jeweilige Ressortleitung bei ihrer Aufgabenwahrnehmung bezüglich der Informationssicherheit zu beraten und sie bei der Umsetzung zu unterstützen.

5.2.3 *Informationssicherheitsbeauftragte für jede Dienststelle oder Einrichtung (Dienststellen-CISO)*

Die Inhaberin oder der Inhaber dieser Funktion wird von der jeweiligen Dienststelle oder Einrichtung unter Berücksichtigung der organisatorischen Besonderheiten (zum Beispiel Bündelung der Funktion für mehrere Dienststellen oder Einrichtungen) in Abstimmung mit dem jeweiligen Ressort benannt. In der Zuständigkeit der oder des Dienststellen-CISO liegt die Förderung, Koordinierung und Abstimmung aller erforderlichen Belange der Informationssicherheit für die Dienststelle oder Einrichtung. Die oder der Dienststellen-CISO kann sich unmittelbar an die Leitung der Dienststelle oder Einrichtung wenden. Zu ihren oder seinen Aufgaben gehört insbesondere:

5.2.3.1 Das Informationssicherheitskonzept der Dienststelle oder Einrichtung fortzuschreiben.

5.2.3.2 Die Leitung der Dienststelle oder Einrichtung bei der Umsetzung der festgelegten Maßnahmen zu unterstützen, um damit ein angemessenes und dem Stand der Technik entsprechendes Informationssicherheitsniveau der Dienststelle oder Einrichtung zu erreichen und zu halten.

5.2.4 *Verantwortliche Personen für Verfahren, Informationen und IT-Systeme und -Anwendungen*

Bei Bedarf können weitere spezifische Informationssicherheitsbeauftragte benannt werden. Im nachgeordneten Bereich ist hierzu das Einvernehmen mit dem jeweiligen Ressort erforderlich. Diese Personen sind für die Informationssicherheit der jeweiligen Anwendungen, Verfahren, Systeme oder spezifischer Informationen zuständig. Sie arbeiten dabei eng mit den jeweils zuständigen übergeordneten Landes-, ressortspezifischen oder Dienststellen-Informationssicherheitsbeauftragten zusammen.

5.2.5 *Informationssicherheits-Management-Team der Dienststelle oder Einrichtung*

Die oder der Dienststellen-CISO kann Informationssicherheits-Management-Teams gemäß BSI Standard 100-2 bilden. Das Informationssicherheits-Management-Team unterstützt die oder den Dienststellen-CISO bei ihren oder seinen Aufgaben. Es setzt sich zusammen aus der oder dem Informationssicherheitsbeauftragten, den Zuständigen für IT-Sicherheit bei Verfahren, Informationen und IT-Systemen beziehungsweise IT-Betrieb und gegebenenfalls in angemessenem Umfang aus Vertretungen der Abteilungen. Die oder der behördliche Datenschutzbeauftragte ist angemessen zu informieren und bei Bedarf hinzuzuziehen.

5.2.6 *Koordinierungsgruppe Informationssicherheit der Landesverwaltung Baden-Württemberg (KG InfoSic)*

Das Innenministerium richtet eine ständige Koordinierungsgruppe Informationssicherheit der Landesverwaltung Baden-Württemberg für die Informationssicherheitsbeauftragten der Ressorts ein.

Diese ist bei der Ausgestaltung von Richtlinien zu beteiligen. Zu ihren Aufgaben gehören insbesondere:

5.2.6.1 Erarbeitung des jährlichen Berichts gemäß Nummer 5.2.1.4 an den AK-IT und an den CIO,

5.2.6.2 Koordination der landesweiten Sicherheitsprozesse insbesondere bei der Einführung des ISMS und Fortschreibung des Umsetzungsplans,

5.2.6.3 Unterstützung und Beratung zur Informationssicherheit in den Ressorts,

5.2.6.4 Koordination von ressortübergreifenden, gemeinsamen Maßnahmen zur Informationssicherheit.

5.2.7 *Computer Emergency Response Team der Landesverwaltung Baden-Württemberg (CERT BWL)*

Das CERT BWL ist zentrale Anlaufstelle in der Landesverwaltung für präventive und reaktive Maßnahmen in Bezug auf sicherheitsrelevante Vorfälle. Es übernimmt die Weiterleitung von sicherheitsrelevanten Informationen vom und zum Verwaltungs-CERT-Verbund von Bund und Ländern unter angemessener Einbeziehung des kommunalen Bereichs in Baden-Württemberg. Im Rahmen des ressortübergreifenden ISMS unterstützt das CERT BWL die Arbeit der oder des CISO. Zu den Aufgaben des CERT BWL gehören insbesondere:

5.2.7.1 Verteilen von Sicherheitsinformationen,

5.2.7.2 Prüfung und Bewertung von Meldungen zu Sicherheitsvorfällen,

5.2.7.3 Ansprechpartner und Beratung zu Informationssicherheit,

5.2.7.4 übergeordnete Koordination von Abwehrmaßnahmen und laufende Erstellung eines Lageberichts zur Informationssicherheit in Baden-Württemberg.

6 **Pflichten und Berichtswege**

6.1 Die Leitungen aller Dienststellen und Einrichtungen der Landesverwaltung wirken darauf hin, dass diese Verwaltungsvorschrift umgesetzt wird.

6.2 Alle Beschäftigten haben Sicherheitsvorfälle möglichst zu vermeiden und sicherheitsrelevante Ereignisse soweit diese für sie erkennbar sind, unverzüglich über die von der jeweiligen Leitung der Dienststelle oder Einrichtung der Landesverwaltung bekannt gegebenen Wege zu melden, damit schnellstmöglich Abhilfemaßnahmen eingeleitet werden können. Ein Sicherheitsvorfall liegt vor, wenn mindestens eins der unter Nummer 1 genannten Ziele verletzt werden. Ein sicherheitsrelevantes Ereignis liegt vor, wenn mindestens eines der in Nummer 1 genannten Ziele gefährdet erscheint.

6.3 Sicherheitshinweise und -Handlungsanleitungen sind unverzüglich an alle Betroffenen im eigenen Zuständigkeitsbereich weiterzuleiten. Zusätzlich ist die oder der zuständige Informationssicherheitsbeauftragte zu informieren.

6.4 Die jeweils verantwortlichen Organisationseinheiten sensibilisieren die Beschäftigten für das Thema Informationssicherheit.

6.5 Bei Beeinträchtigungen der Informationssicherheit ergreifen die jeweils Verantwortlichen unverzüglich die zur Aufrechterhaltung bzw. Wiederherstellung des IT-Betriebs und der Informationssicherheit geeigneten und angemessenen Maßnahmen.

6.6 Soweit Dritte als Auftragnehmer für die öffentliche Verwaltung Leistungen erbringen, sind diese bei der Auftragserteilung auf die Vorgaben dieser Verwaltungsvorschrift im notwendigen Umfang zu verpflichten. Dies ist über einzelvertragliche Regelungen oder Rahmenverträge sicher zu stellen und vom Auftraggeber zu kontrollieren.

7 **Umsetzungsplan**

Basis für den Umsetzungsplan ist insbesondere der Beschluss des IT-Planungsrats vom 8. März 2013, der die Verpflichtung begründet, bis zum 8. März 2018 ein ISMS einzuführen.

Die KG InfoSic erstellt den Umsetzungsplan. Der Umsetzungsplan beschreibt die zur Einrichtung und Aufrechterhaltung des ISMS erforderlichen Maßnahmen und einen Zeitplan für die Umsetzung.

Er enthält auch eine Abschätzung der damit verbunden Aufwände und Kosten. Der Umsetzungsplan wird in Abstimmung mit den IT-Gremien bedarfsgerecht fortgeschrieben. Diese Gremien sind der IT-Rat Baden-Württemberg und der AK-IT.

8 **Inkrafttreten**

Diese Verwaltungsvorschrift tritt am 1. Mai 2017 in Kraft und am 30. April 2024 außer Kraft.

GABl. S. 214

Verwaltungsvorschrift des Innenministeriums zur Änderung der Verwaltungsvorschrift des Ministeriums für Integration über Zustimmungserfordernisse im Staatsangehörigkeitsrecht (VwV ZustStAR)

Vom 7. April 2017 – Az.: 7-1010.1/1 –

1.

Die VwV ZustStAR vom 08. Juli 2013 (GABl. S. 330) wird wie folgt geändert:

1. In der Überschrift werden die Wörter »Ministeriums für Integration« durch das Wort »Innenministerium« ersetzt.
2. Die Nummer 1 wird wie folgt geändert:
   a) In der Überschrift und in Satz 1 werden die Wörter »Ministeriums für Integration« durch das Wort »Innenministeriums« ersetzt.
   b) In Nummer 1.2.2 wird das Wort »besonderen« durch das Wort »herausragenden« ersetzt:

2. Inkrafttreten, Außerkrafttreten

Diese Verwaltungsvorschrift tritt am Tag nach ihrer Bekanntmachung in Kraft. Sie tritt am 31. Juli 2020 außer Kraft.

GABl. S. 217