## 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*