Normgeber:	Justizministerium	**Quelle:**	
Aktenzeichen:	1510 - 103.232 [SH 6]		
Erlassdatum:	06.05.2014		
Fassung vom:	06.05.2014	**Gliederungs-Nr:**	31600
Gültig ab:	01.07.2014		
Gültig bis:	31.12.2019 AUSSER KRAFT	**Fundstelle:**	Nds. Rpfl. 2014, 180

Informationssicherheit (ISMS): "Informationssicherheitsleitlinie (ISLL) Justiz"

Nichtamtliches Inhaltsverzeichnis

Informationssicherheit (ISMS): „Informationssicherheitsleitlinie (ISLL) Justiz“

AV d. MJ v. 6. 5. 2014 (1510 – 103.232 [SH 6])
– Nds. Rpfl. S. –

VORIS 31600

Fundstelle. Rpfl. 2014, S. 180

1. Gegenstand und Geltungsbereich

1.1 Die Informationssicherheitsleitlinie der niedersächsischen Justiz (ISLL Justiz) beschreibt den Aufbau und den Betrieb eines Informationssicherheitsmanagementsystems (ISMS) in der niedersäch-

sischen Justiz auf Grundlage des Standards ISO/IEC 27001 und dient der langfristigen Gewährleistung der Informationssicherheit.

1.2 Das ISMS der Justiz ist selbstständiger Teil eines ressortübergreifenden Gesamt-ISMS der niedersächsischen Landesverwaltung in der niedersächsischen Justiz.

2. Sicherheitsziele

Oberstes Ziel dieser Leitlinie und sämtlicher auf ihr basierenden Dokumente ist die Gewährleistung und Aufrechterhaltung von Informationssicherheit in den Geschäftsprozessen der niedersächsischen Justiz.

Hierzu sind Sicherheitsrisiken durch angemessene Schutzmaßnahmen zu minimieren, das eventuell verbleibende Restrisiko klar zu beschreiben und dieses ggfs. zu verantworten.

3. Definitionen

Im Sinne dieser ISLL

3.1 umfasst der Begriff **„niedersächsische Justiz“** das Niedersächsische Justizministerium, die Gerichte, Staatsanwaltschaften und Justizvollzugseinrichtungen sowie die Norddeutsche Hochschule für Rechtspflege.

Ausgenommen ist der Bereich der Sicherheitstechnik im Strafvollzug;

3.2 ist **„Geschäftsprozess“** eine Folge von Einzeltätigkeiten, die schrittweise ausgeführt werden, um das Ziel eines gerichtlichen Verfahrens oder eines Verwaltungsakts zu erreichen;

3.3 ist **„Informationssicherheit“** die Herstellung und Aufrechterhaltung der folgenden Grundwerte

- **„Vertraulichkeit“,** d.h. die Gewährleistung des physikalischen bzw. logischen Zugangs zu Informationen nur für Zugriffsberechtigte,

- **„Verfügbarkeit“,** d.h. die Gewährleistung des bedarfsorientierten Zugangs zu Informationen und zugehörigen Werten für berechtigte Benutzerinnen und Benutzer,

– **„Integrität“,** d.h. die Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden;

3.4 ist **„Informationstechnik“** jedes technische Mittel zur Verarbeitung oder Übertragung von Informationen;

3.5 ist **„Informationssicherheitsmanagementsystem“** (ISMS) die Aufstellung von Verfahren und Regeln, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern;

3.6 ist **„Informationssicherheitsprozess“** ein sich dauerhaft wiederholender sukzessiver Ablauf von Planungs-, Umsetzungs-, Überprüfungs- und Verbesserungsphasen mit dem Ziel, die Informationssicherheit langfristig planvoll und standardisiert zu gewährleisten und weiterzuentwickeln;

3.6 ist **„Schutzbedarf“** das unter Berücksichtigung der Bedeutung einer Information angemessene Maß an Schutzbedürftigkeit (siehe Schutzkategorien);

3.7 sind **„Schutzkategorien“** Gruppen annähernd gleichen Schutzbedarfs, dabei bedeutet

– **„normaler Schutzbedarf“,** dass die Auswirkungen eines Schadens begrenzt und überschaubar wären,

– **„hoher Schutzbedarf“,** dass die Auswirkungen eines Schadens beträchtlich sein können,

– **„sehr hoher Schutzbedarf“,** dass die Auswirkungen eines Schadens ein existenzielles bzw. katastrophales Ausmaß erreichen können;

3.8 ist **„Sicherheitsdomäne“** – entsprechend der ISLL der niedersächsischen Landesverwaltung – ein abgrenzbarer Teil der Landesverwaltung mit einheitlichen Sicherheitsanforderungen und/oder einheitlicher Sicherheitsadministration, dabei kann eine Sicherheitsdomäne weitere, untergeordnete Sicherheitsdomänen enthalten. Eine untergeordnete Sicherheitsdomäne wendet grundsätzlich die Regeln der ihr übergeordneten Sicherheitsdomäne an, soweit sie sich in Abstimmung mit der übergeordneten Sicherheitsdomäne selbst keine spezielleren Regeln gibt;

3.9 sind **„Sicherheitskonzepte“** Dokumente, welche den Schutzbedarf von Informationen festlegen, die Angriffs- und Schadenszenarien eines bestimmten Geschäftsprozesses oder eines organisatorischen oder technischen Bereichs analysieren, um Risiken für die Informationen zu bestimmen, und Schutzmaßnahmen beschreiben, um diese Risiken zu behandeln;

3.10 ist **„Schutzmaßnahme“** eine technische oder organisatorische Lösung mit dem Ziel, ein bestehendes Risiko zu minimieren oder zu beherrschen;

3.11 ist ein **„Sicherheitsvorfall“** jeder Vorfall, bei dem die Grundwerte Verfügbarkeit, Vertraulichkeit oder Integrität in unzulässiger Weise verletzt werden;

3.12 ist die „IT-Infrastruktur“ die Gesamtheit aller Arbeitsplatzrechner, Server und Netzwerke sowie übrigen IT-Komponenten einschließlich Fachverfahren, die zur automatisierten Informationsverarbeitung durch den Zentralen IT-Betrieb der niedersächsischen Justiz zur Verfügung gestellt werden.

4. Dokumentenhierarchie

4.1 Die Informationssicherheitsleitlinie der niedersächsischen Justiz (ISLL Justiz) ist das übergeordnete strategische Basisdokument zur Gewährleistung der Informationssicherheit und dient insbesondere der Initiierung und Aufrechterhaltung des ISMS.

4.2 Die Informationssicherheitsrichtlinien der niedersächsischen Justiz (ISRL Justiz) legen für einzelne organisatorische oder technische Bereiche Standards und Verantwortlichkeiten fest.

4.3 Dienstanweisungen legen fest, wie die Bestimmungen der Informationssicherheitsrichtlinien konkret umzusetzen sind.

5. Grundsätze der Sicherheitsstrategie

5.1 Informationsklassifizierung

Alle Informationen mit Relevanz für die Geschäftsprozesse der niedersächsischen Justiz sind in Schutzkategorien zu klassifizieren. Normkonform geschieht dies durch das Risikomanagement im Rahmen des ISMS, hilfsweise durch Sicherheitskonzepte.

5.2 Risikoanalyse

Im Rahmen einer Risikoanalyse sind mögliche Schadenereignisse, deren Ursachen und Auswirkungen wie deren Eintrittswahrscheinlichkeit zu untersuchen und Maßnahmen zur Risikobehandlung zu entwickeln. Das verbleibende Risiko (Restrisiko) ist zu beschreiben und durch zuständige Entscheidungsträger zu verantworten.

5.3 **Angemessenheit von Schutzmaßnahmen**

Finanzieller und organisatorischer Aufwand von Schutzmaßnahmen müssen in einem angemessenen Verhältnis zum verfolgten Ziel stehen. Dem Gebot der Wirtschaftlichkeit und Sparsamkeit ist stets Rechnung zu tragen.

5.4 **Sicherheitskonzepte**

Einzelfall- oder anlassbezogen können bis zur Etablierung eines ISMS für die gesamte Justiz Sicherheitskonzepte für einzelne Geschäftsprozesse, technische oder organisatorische Bereiche erstellt werden, in das übergeordnete ISMS zu überführen sind.

6. Organisation

Für die sichere Abwicklung der Geschäftsprozesse in der niedersächsischen Justiz sind im Informationssicherheitsprozess verantwortlich:

6.1 **Alle Bediensteten**

Alle Bediensteten der niedersächsischen Justiz haben im Rahmen ihrer jeweiligen Zuständigkeiten und Verantwortungsbereiche für die Erhaltung der unter 3.3 beschriebenen Grundwerte in Bezug auf die ihnen anvertrauten Informationen und Prozesse Sorge zu tragen.

6.2 **Niedersächsisches Justizministerium**

Das Niedersächsische Justizministerium legt die strategische Ausrichtung des ISMS und die zu erreichenden Ziele fest. Es schafft die personellen, organisatorischen und materiellen Voraussetzungen und führt eine regelmäßige Bewertung des ISMS durch.

6.3 **Behördenleitung**

Die Behördenleitung ist im Rahmen ihrer Zuständigkeit für die Gewährleistung der Informationssicherheit verantwortlich. Sie hat insbesondere zu veranlassen, dass organisatorische und technische Maßnahmen zur Gewährleistung von Informationssicherheit umgesetzt werden.

6.4 **Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter (ISB) der niedersächsischen Justiz**

Die oder der Informationssicherheitsbeauftragte dar niedersächsischen Justiz initiiert und verantwortet als unabhängige Instanz die Einführung und Fortentwicklung eines ISMS in der Justiz. Sie oder er berät und unterstützt die jeweils zuständigen Entscheidungsträgerinnen und Entscheidungsträger bei der Aufgabenwahrnehmung im Hinblick auf die Informationssicherheit.

Die oder der Informationssicherheitsbeauftragte hat

– insbesondere die Aufgabe, das ISMS fortzuentwickeln.

– ein unmittelbares Vortragsrecht bei der Staatse kretärin oder dem Staatssekretär des Justizminis teriums.

6.5 **Zentraler IT-Betrieb (ZIB)**

Der zentrale IT-Betrieb betreibt die IT-Infrastruktur der niedersächsischen Justiz und verantwortet insoweit die Gewährleistung der Informationssicherheit.

7. Schlussbestimmung

Die AV zur Informationssicherheitsleitlinie der niedersächsischen Justiz (ISLL Justiz) tritt am 1. 7. 2014 in Kraft und mit Ablauf des 31. 12. 2019 außer Kraft.

Diese Vorschrift wird von folgenden Dokumenten zitiert

Verwaltungsvorschriften der Länder
Niedersachsen
Justizministerium, i. d. F. v. 20.11.2019, Az.:1510-ISMS.5