Grundzüge der Informationssicherheit

Informationssicherheits-Policy - Ebene 2

INHALT

1 Einleitung

Die Informationssicherheits-Policy (ISP) der Deutschen Rentenversicherung (DRV) hat das Ziel, eine rechtmäßige Aufgabenerledigung und Datenverarbeitung sowie sichere Arbeitsprozesse und Infrastrukturen zu gewährleisten. Maßgeblich für die nachfolgenden Regelungen zur Informationssicherheit sind die Standards des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und die Einhaltung der Datenschutzvorschriften.

Die Informationssicherheit[1] umfasst nicht nur Aspekte der Informations- und Kommunikationstechnologie, sondern schützt Informationen bzw. die den Informationen zugrunde liegenden Daten jeglicher Art und Herkunft (siehe auch Kapitel 4).

Das hier vorliegende Dokument *Grundzüge der Informationssicherheit (*GdIS*)*[2] bildet die Ebene 2 der ISP der DRV.

Die *GdIS* hat folgende Funktionen:

- Sie beschreibt gemeinsam mit der *Leitlinie zur Informationssicherheit* den Rahmen der ISP der DRV.
- Sie beschreibt grundlegende Festlegungen für die Dokumente der ISP (Kapitel 2).
- Sie benennt langlebige Sicherheitsziele und -grundsätze für die DRV (Kapitel 3).
- Sie beschreibt die Umsetzung der Informationssicherheitsstrategie (Kapitel 4).
- Sie beschreibt die Grundsätze für Geschäftsprozesse mit datenschutzrelevanten Informationen.
- Sie zielt auf eine Harmonisierung der organisatorischen und technischen Infrastruktur ab.
- Sie trägt zur Entwicklung der Sicherheitskultur bei.
- Sie beschreibt Grundsätze der Zusammenarbeit in der Informationssicherheit.

Die Regelungen der *GdIS* und der für verbindlich erklärten Richtlinien zur Informationssicherheit (Ebene 3) bilden Mindeststandards für die DRV, deren Sicherheitsniveau nicht unterschritten werden darf.

[1] Informationssicherheit umfasst insbesondere Datenschutz und IT-Sicherheit.
[2] Dokumenteigennamen sind kursiv gekennzeichnet.

Festlegungen zum Arbeits-, Gesundheits- und Brandschutz sowie zu wirtschaftlichen Betrachtungsweisen werden durch die *GdIS* nicht getroffen. Diese Themen können jedoch als Richtlinien in die Struktur der ISP aufgenommen werden.

Die in diesem Dokument beschriebenen Maßgaben und Zielsetzungen gelten unmittelbar und uneingeschränkt für alle Formen der Datenverarbeitung. Sie sind für alle Träger der Deutschen Rentenversicherung (RVTR) und deren Beschäftigten verbindlich.

2 Festlegungen

Die *GdIS* definiert den Rahmen, innerhalb dessen die weiteren Dokumente der ISP ausgestaltet werden dürfen bzw. sollen. Hierzu gehören neben den fachlichen Inhalten auch organisatorische sowie sprachliche Festlegungen. Im Rahmen der Neukonzeption der ISP wurde viel Wert auf einen durchgehend einheitlichen sowie unmissverständlichen Sprachgebrauch gelegt. Dieser Ansatz ist in den weiteren Dokumenten der ISP fortzuführen. Die folgenden Vorgaben gelten für alle Dokumente der ISP.

Die Regelungen der *GdIS* und der für DRV-weit verbindlich erklärten Richtlinien bilden Mindeststandards für die Informationssicherheit der DRV, deren Sicherheitsniveau nicht unterschritten werden darf. Eine Verschärfung oder Erweiterung der Regelungsinhalte ist hingegen zulässig.

Mit Einführung der neuen ISP kann es im Übergangszeitraum zu konkurrierenden Festlegungen mit der bisherigen IT-Security Policy kommen. In diesen Fällen ist stets die neue Festlegung maßgeblich. Die übrigen bisherigen Festlegungen gelten fort, bis sie entweder aufgehoben oder in die neue Struktur der ISP überführt wurden.

Alle weiteren übergreifend organisatorischen Festlegungen, die in unmittelbarem Zusammenhang mit den Ebenen der ISP stehen, sind in der Richtlinie *Organisation der Informationssicherheit* beschrieben. Dort sind alle Richtlinien, Konzepte und Handlungsanweisungen aufgeführt, die DRV-weit verbindlich sind.

Im Dokument *Definitionen und Abkürzungen* sind alle Begriffe definiert, die innerhalb der ISP bindend anzuwenden sind. Personen, denen die Erstellung von Regelwerken sowie IT-Sicherheitskonzepten obliegt, haben im jeweiligen Kontext ausschließlich diese Begriffe zu verwenden. Es sind keine Synonyme zu benutzen.

Es sind klare und verständliche Regelungen zu formulieren. Ausnahmen von einer Regelung sind transparent und prüfbar zu dokumentieren. Sie dürfen nicht dazu führen, dass der

beabsichtigte Regelungszweck unterlaufen wird. Die Entscheidungskriterien sind regelmäßig neu zu bewerten.

Alle Texte sind Gender-konform zu formulieren. Eine grammatikalisch feminine oder maskuline Form ist jedoch unbeachtlich.

3 Ziele und Grundsätze

Die Informationssicherheits-Policy (ISP) legt den Rahmen zum Erreichen von Informationssicherheit fest. Durch sie sollen eine Kultur und ein Bewusstsein für die Sicherheit von Daten, IT-Systemen und Geschäftsprozessen unterstützt und entwickelt werden. Dabei spielt es keine Rolle, ob die für die Aufgabenerledigung erforderlichen Daten nicht-automatisiert, teilweise automatisiert oder vollständig automatisiert verarbeitet werden.

Dieses Kapitel enthält die zentralen Ziele und Grundsätze der DRV für die Informationssicherheit.

3.1 Ordnungsmäßigkeit

Alle unmittelbar verbindlichen gesetzlichen Regelungen und die ISP bilden den ordnenden Rahmen, in dem alle Fachaufgaben zu erledigen sind. Sie sind in der jeweils gültigen Fassung zu beachten. Hierzu gehören insbesondere das Sozialgesetzbuch (SGB) und die Datenschutzgesetze.

Weitere Vorgaben durch nicht unmittelbar verbindlich geltendes Recht, wie beispielsweise DIN- / ISO-Normen, Ministerialerlasse, Beschlüsse des IT-Rates oder technische Richtlinien des BSI, sind zu beachten, soweit

- deren Geltung durch Rechtsvorschriften angeordnet ist,
- deren Beachtung von Gremien der DRV festgelegt wurde oder
- sie durch den RVTR selbst für verbindlich erklärt wurden.

3.2 Erforderlichkeit, Zweckbindung

Daten sollen nur beschafft und verwendet werden, wenn es zur Erledigung der dienstlichen Aufgaben erforderlich ist.

Die Nutzung von dienstlichen Daten zu anderen als zu dienstlichen Zwecken, insbesondere die private Nutzung sowie die unbefugte Weitergabe an Dritte, ist untersagt.

Wenn Daten für dienstliche Zwecke nicht mehr benötigt werden, sind sie zu löschen.

3.3 Wirtschaftlichkeit

Alle Maßnahmen in der DRV sind stets auch unter Berücksichtigung der Grundsätze der Wirtschaftlichkeit und Sparsamkeit zu bewerten.

Die Implementierung bzw. Umsetzung von Sicherheitsmaßnahmen verfolgt das Ziel, die Eintrittswahrscheinlichkeiten von Sicherheitsvorfällen zu verringern und Schäden im Falle des Eintritts zu minimieren. Diese Ziele generieren grundsätzlich keine monetären wirtschaftlichen Vorteile. Es ist daher wichtig, den „strategischen" Nutzen der Sicherheitsmaßnahmen adäquat zu bewerten und zu kommunizieren. Notwendige Sicherheitsmaßnahmen dürfen nicht allein aufgrund der fehlenden monetären Wirtschaftlichkeit unterbleiben.

3.4 Verantwortlichkeit

Die Geschäftsführungen bzw. das Direktorium[3] sind für die Aufgabenerfüllung im Allgemeinen und die Informationssicherheit im Besonderen verantwortlich (siehe Leitlinie zur Informationssicherheit).

Die Leitungen der nachgeordneten Organisationseinheiten tragen grundsätzlich die Verantwortung für die Organisation ihres zugewiesenen Aufgabengebietes und damit auch für die Informationssicherheit. Abweichungen von dem Grundsatz dieser Verantwortung sind transparent und revisionssicher zu dokumentieren. Die Verantwortung ist stets an Personen zu binden.

Alle Beschäftigten sind für ihre Handlungen im Rahmen des ihnen übertragenen Aufgabenbereichs verantwortlich. Ihnen soll bewusst sein, dass sie durch das eigene Verhalten und die vorgegebene Benutzung, insbesondere der IT-Systeme, die Informationssicherheit in entscheidendem Maß mitbestimmen und daneben aktiv an der Umsetzung der Sicherheitsziele und Schutzmaßnahmen mitwirken.

Durch geeignete Maßnahmen sind die Beschäftigten über die in ihrem Aufgabenbereich geltenden Informationssicherheitsmaßnahmen in Kenntnis zu setzen. Diese können neben transparenten und dokumentierten Regelungen auch Schulungen und Sensibilisierungsmaßnahmen sein. Die Kenntnisnahme ist zu dokumentieren.

In der Richtlinie *Organisation der Informationssicherheit* wird dokumentiert, welche Gremien oder Organisationseinheiten für die Erstellung und Pflege der verbindlichen Richtlinien zuständig sind.

[3] nach der aktuellen Fassung des § 36 SGB IV.

3.5 Fachkunde

Es ist sicherzustellen, dass für die Aufgabenerledigung die notwendige Fachkunde vorhanden ist. Für die Gewährleistung der Informationssicherheit ist in ausreichendem Umfang Personal mit der erforderlichen Fachkunde vorzuhalten. Die Fachkunde ist durch Schulung und Weiterbildung aktuell zu halten.

3.6 Dokumentation

Die für die ordnungsgemäße Aufgabenerfüllung der DRV erforderlichen Informationen sind stets zu dokumentieren. Diese Informationen haben adressatengerecht zur Verfügung zu stehen. Hierzu zählen insbesondere Handlungsanweisungen, Verfahrensdokumentationen, Betriebshandbücher und Dienstanweisungen. Die Dokumentation ist stets aktuell zu halten.

Ziel der Dokumentation ist es, neben dem sicheren Umgang mit IT-Systemen, IT-Services und IT-Verfahren auch Transparenz und Nachvollziehbarkeit zu gewährleisten.

IT-Systeme, IT-Services und IT-Verfahren dürfen nicht in den produktiven Betrieb genommen werden, wenn die für den sicheren Umgang erforderlichen Dokumente nicht zur Verfügung stehen. Dieser Aspekt ist bei der Freigabe zu prüfen.

3.7 Verbot der privaten Nutzung

Sowohl die Nutzung der dienstlichen IT-Systeme, IT-Services und IT-Verfahren für private Zwecke als auch die Nutzung privater IT-Systeme, IT-Services und IT-Verfahren für dienstliche Zwecke ist grundsätzlich untersagt.

3.8 Standardisierung

IT-Systeme, IT-Services und IT-Verfahren werden immer komplexer und erfordern ein hohes Maß an Fachkompetenz. Eine homogene IT-Infrastruktur sorgt dafür, dass diese Komplexität durch das Personal beherrschbar ist und bleibt. Dadurch erhöht sich auch die Sicherheit bei ihrem Betrieb nachhaltig. Es ist daher bei der Entwicklung neuer IT-Services und IT-Verfahren, bei der Beschaffung neuer IT-Systeme sowie bei der Anpassung bestehender IT-Systeme, IT-Services und IT-Verfahren stets auch darauf zu achten, dass sie sich gut in die bestehenden Strukturen der DRV einfügen bzw. die Standardisierung sukzessive umsetzen. Eine Ausnahme hiervon bildet der bewusste Einsatz von heterogenen IT-Systemen, IT-Services und IT-Verfahren, die zur Erhöhung der Sicherheit eingesetzt werden (z. B. beim Schutz vor Schadprogrammen).

3.9 Vertraulichkeit

Die Organisation ist so zu gestalten, dass nur diejenigen Organisationseinheiten oder Personen die Daten zur Kenntnis erhalten und verarbeiten, die sie für ihre dienstlichen Aufgaben benötigen (siehe Leitlinie zur Informationssicherheit).

Für die Daten der DRV sind Vertraulichkeitskategorien zu definieren und alle Daten sind diesen zuzuordnen. Entsprechend der Vertraulichkeitskategorie sind geeignete Maßnahmen zur Verschlüsselung sowie Maßnahmen zur Verhinderung von unerwünschtem bzw. unerlaubtem Abfluss von Daten umzusetzen.

Die einschlägigen Festlegungen zur Klassifizierung, Vorgaben zur Verschlüsselung und Vorgaben zur Verhinderung von Datenabfluss sind in DRV-weit verbindlichen Richtlinien zu treffen.

3.10 Integrität

Die Integrität ist die Sicherstellung der Vollständigkeit und Unversehrtheit von Daten (siehe Leitlinie zur Informationssicherheit).

Die Integrität umfasst auch die Authentizität von Daten und ist notwendige Voraussetzung für die Revisionsfähigkeit.

Die einschlägigen Festlegungen zur Gewährleistung der Integrität sind in Richtlinien zu treffen. Hierbei sind nachstehende Aspekte in Abhängigkeit des Schutzbedarfes der jeweiligen Daten besonders zu betrachten:

- Korrektheit des Inhalts und des Umfangs der Daten.
- Modifizierung der Daten und deren Nachvollziehbarkeit.
- Chronologie der Daten.
- Nachweis der Urheberschaft, erstellende und versendende Personen, Organisationseinheit oder IT-Systeme.

3.11 Verfügbarkeit

Verfügbarkeit bedeutet, dass Daten und technische Systeme dem berechtigten Personenkreis stets wie vorgegeben zur Verfügung stehen müssen (siehe *Leitlinie zur Informationssicherheit*).

Der Grad der Verfügbarkeit von Daten und daraus resultierend die Verfügbarkeit von IT-Systemen, IT-Services und IT-Verfahren, ist von den jeweiligen Anwendern bzw. den Auftrag gebenden Stellen festzulegen.

Die Modalitäten zur Bestimmung und Berechnung von Verfügbarkeit sind in einer DRV-weit verbindlichen Richtlinie festzulegen.

3.12 Grundsätze für personenbezogene Daten

Auch für die Verarbeitung personenbezogener Daten gelten die oben genannten Grundsätze. Die folgenden Grundsätze sind für personenbezogene Daten zusätzlich zu beachten.

3.12.1 Zulässigkeit – Verbot mit Erlaubnisvorbehalt

Es ist verboten, personenbezogene Daten zu verarbeiten, es sei denn, es ist rechtlich erlaubt oder die betroffene Person hat vorher eingewilligt (i. d. R. schriftlich).

3.12.2 Datenminimierung

Der Grundsatz der Datenminimierung verpflichtet dazu, dass nur für den Zweck erhebliche, erforderliche und angemessene Verarbeitungen stattfinden.

3.12.3 Direkterhebung

Personenbezogene Daten sind grundsätzlich direkt bei den Betroffenen und nur ausnahmsweise bei anderen Stellen zu erheben.

3.12.4 Zweckbindung

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke verarbeitet werden.

3.12.5 Transparenz und Intervenierbarkeit

Jede betroffene Person muss eine Verarbeitung ihrer Daten nachvollziehen und ihre Betroffenenrechte geltend machen können.

3.12.6 Nichtverkettbarkeit – Trennungsgebot

Personenbezogene Daten dürfen nur für den Zweck, für den sie erhoben wurden und nicht gemeinsam mit weiteren - für einen anderen Zweck erhobenen - Daten verarbeitet werden.

3.12.7 Technisch- organisatorische Maßnahmen

Es besteht die Verpflichtung zum Ergreifen von Sicherheitsmaßnahmen. Die Art und Weise der Verarbeitung personenbezogener Daten und die dabei einzusetzenden technisch-organisatorischen Maßnahmen sind konkret festzulegen.

Bei der Festlegung der Maßnahmen ist die Verhältnismäßigkeit zu beachten. Maßnahmen sind nicht erforderlich, wenn ihr Aufwand in keinem angemessenen (auch wirtschaftlichen) Verhältnis zu dem angestrebten Schutzzweck steht. In einem solchen Fall müssen immer noch angemessene Maßnahmen ergriffen werden. Ziel muss es sein, das Restrisiko eines denkbaren Schadensereignisses so zu minimieren, dass es im Fall des Eintretens mit angemessenem Aufwand bereinigt werden kann.

3.12.8 Richtigkeit

Die Verantwortlichen haben dafür Sorge zu tragen, dass die verarbeiteten Daten die Realität zutreffend abbilden.

3.12.9 Folgenabschätzung

Weist eine Verarbeitung besondere Risiken (z.B. bei der Verarbeitung besonderer Datenkategorien) für die Rechte der Betroffenen auf, so ist vor Beginn der Verarbeitung eine Folgenabschätzung durchzuführen.

3.12.10 Automatisierte Abrufverfahren

Werden Daten über ein automatisiertes Abrufverfahren übermittelt, unterliegt dies engen gesetzlichen Rahmenbedingungen.

3.12.11 Automatisierte Einzelfallentscheidungen

Sofern persönliche Aspekte einer natürlichen Person bei einer Einzelfallentscheidung beachtet werden müssen, besteht grundsätzlich das Verbot, diese ausschließlich automatisiert zu generieren.

4 Umsetzung der Informationssicherheitsstrategie

Informationssicherheit ist als Gesamtheit von Maßnahmen zu verstehen, die das Ziel anstreben, sichere Geschäftsprozesse und sichere Infrastrukturen bei allen zu erledigenden Aufgaben zu gewährleisten.

Das Wort Informationssicherheit ist in der Policy bewusst als weit aufzufassender Begriff gewählt.

Es geht nicht allein um die IT-Sicherheit, die Sicherheit einzelner technischer Systeme oder die Sicherheit einzelner Arbeitsschritte. Sicherheitsüberlegungen sind bei jeglichem Umgang mit Sozialdaten, sonstigen personenbezogenen Daten, Geld- und Finanztransaktionen oder anderen schutzwürdigen Daten anzustellen. Allerdings werden die Geschäftsprozesse zunehmend ganz oder teilweise IT-technisch umgesetzt.

Mit dem hohen Anspruch an eine sichere und funktionierende IT werden in der DRV die IT-Sicherheitsmaßnahmen auf der Grundlage des sogenannten IT-Grundschutzes betrachtet und umgesetzt. Kern des IT-Grundschutzes sind die einschlägigen Standards und Kataloge des BSI. Diese beruhen im weitesten Sinne auf dem allgemein und weltweit gültigen IT-Sicherheitsregelwerk ISO 27001. Dieses wird durch das BSI mit weiteren Maßnahmen ergänzt, welche die Anforderungen des nativen Standards ISO 27001 konkretisieren und somit ein nahezu eigenständiges Regelwerk „ISO 27001 mit der Erweiterung IT-

Grundschutz“ für die Betrachtung und Umsetzung eines sicheren IT-Betriebs darstellen. In der DRV wird aufgrund der heterogenen Struktur eine modifizierte Vorgehensweise bei der Umsetzung des Grundschutzes angewandt.

Die Strategie der Informationssicherheit in der DRV basiert auf drei Säulen, die im Folgenden beschrieben werden.

Abbildung 1: Säulen der Informationssicherheitsstrategie der DRV

4.1 Informationssicherheits-Management

Informationssicherheit ist eine Aufgabe der Geschäftsführung bzw. des Direktoriums. Diese Aufgabe, nicht jedoch die Gesamtverantwortung, kann delegiert werden. Im Rahmen der Sicherheitskonzeption ist bei jedem RVTR neben der bzw. dem gesetzlich zu bestellenden Datenschutzbeauftragten eine IT-Sicherheitsbeauftragte oder ein IT-Sicherheitsbeauftragter zu bestellen. Die IT-Sicherheitsbeauftragten sind zuständig für die Belange der IT-Sicherheit innerhalb des jeweiligen RVTR (siehe *Leitlinie zur Informationssicherheit*). Die ihnen übertragenen Aufgaben, Zuständigkeiten und Kompetenzen sind klar zu definieren und in Textform festzulegen. Um ihre Aufgabe wahrnehmen zu können, sind sie bei allen IT-Verfahren und vor Entscheidungen hierüber zu beteiligen.

Für die IT-Sicherheitsbeauftragten sind die folgenden Punkte zu gewährleisten:

- Die IT-Sicherheitsbeauftragten berichten direkt an die jeweilige Geschäftsführung bzw. an das Direktorium.
- In der Ausübung der Fachkunde auf dem Gebiet der IT-Sicherheit sind sie weisungsfrei.
- Es ist sicherzustellen, dass es zu keiner Interessenskollision kommt, wenn weitere Rollen oder Funktionen wahrgenommen werden.
- Die IT-Sicherheitsbeauftragten sind frühzeitig über geplante (auch übergreifende) IT-Maßnahmen einschließlich der damit zusammenhängenden baulichen und sonstigen infrastrukturellen Maßnahmen zu unterrichten.

Der Aufgabenbereich der IT-Sicherheitsbeauftragten umfasst mindestens:

- Zuständigkeit für den Aufbau und die Weiterentwicklung der Organisation der Informationssicherheit innerhalb der RVTR.
- Erstellung von und Mitwirkung bei Regelungen, die die Informationssicherheit betreffen, unter anderem bei den Ebenen der ISP.
- Beratung der Geschäftsführung bzw. des Direktoriums in allen Fragen der IT-Sicherheit.
- Regelmäßige und anlassbezogene Berichte über Vorkommnisse und den aktuellen Stand der IT-Sicherheit.
- Beteiligung bei der Untersuchung und Analyse sicherheitsrelevanter Vorfälle (siehe Kapitel 4.4).
- Prüfung von IT-Sicherheitskonzepten, insbesondere auf Vollständigkeit, Konsistenz und lückenlose Integration in die Sicherheitskonzeption der DRV.
- Initiierung sowie Kontrolle der Umsetzung von Sicherheitsmaßnahmen.
- Ausarbeitung und Weiterentwicklung eines zielgruppenorientierten Sensibilisierungs- und Schulungskonzepts für den RVTR.
- Regelmäßige Teilnahme an Fortbildungen und Qualifizierungsmaßnahmen.
- Wahrnehmung der in nachgelagerten Ebenen der ISP festgelegten Entscheidungsbefugnisse.

Die IT-Sicherheitsbeauftragten sollen durch ein Informationssicherheitsmanagement-Team unterstützt werden. Die vielfältigen fachlichen Aufgaben der DRV sind eng mit dem Datenschutz

und der Informationssicherheit verknüpft. Aus diesem Grund sollte der bzw. die Datenschutzbeauftragte Mitglied des Informationssicherheitsmanagement-Teams sein.

Das Informationssicherheitsmanagement-Team unterstützt die Etablierung und Weiterentwicklung der Organisation der Informationssicherheit und Informationssicherheitspolitik sowie die Umsetzung von Maßnahmen.

Das Informationssicherheitsmanagement-Team wird von dem IT-Sicherheitsbeauftragten bzw. der IT-Sicherheitsbeauftragten geleitet.

Das Informationssicherheitsmanagement-Team ist berechtigt, Aufträge in die jeweiligen Fachabteilungen zu geben und übergreifende Maßnahmen der Informationssicherheit zu koordinieren.

Letztendlich müssen die Anwender und Benutzer sowie die IT-Systemverantwortlichen für die Einhaltung der Sicherheitsmaßnahmen sorgen (siehe Abschnitt 3.4 Verantwortlichkeit).

4.2 Informationssicherheits-Policy (ISP)

Die DRV hat sich zur Umsetzung der Informationssicherheit ein umfassendes Regelwerk gegeben, die Informationssicherheits-Policy (ISP). Sie dokumentiert die Informationssicherheitsziele und legt Standards und Methoden zur Umsetzung der Sicherheitsstrategie fest.

Sie ist ein in fünf Ebenen hierarchisch gegliedertes Regelwerk, siehe **Abbildung 2**.

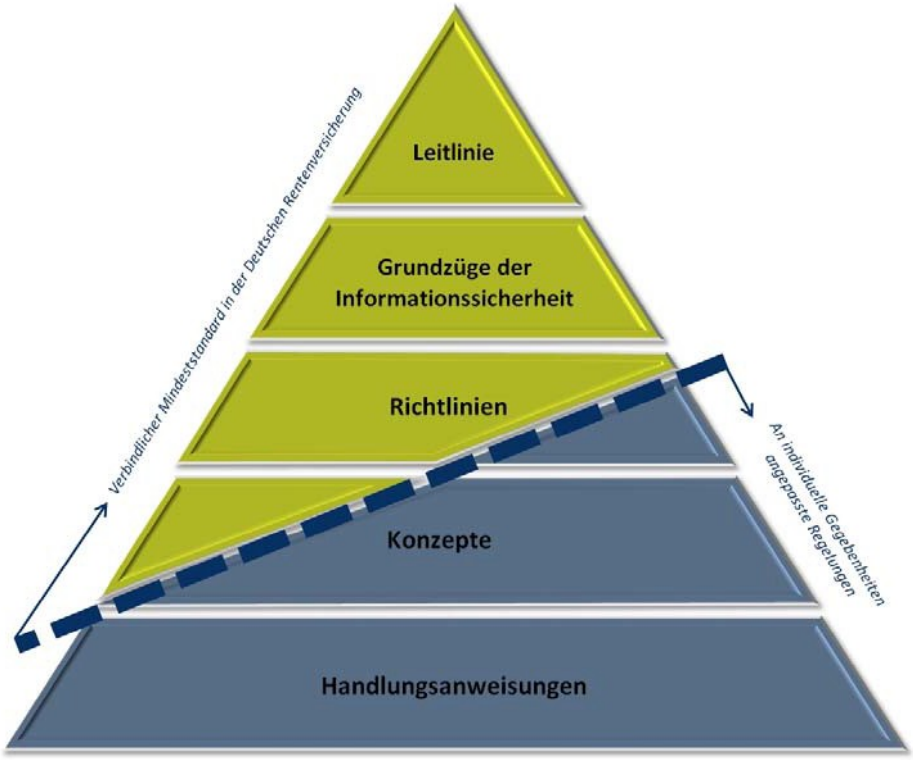

Abbildung 2: Ebenenmodell der Informationssicherheits-Policy

Die einzelnen Ebenen der ISP regeln die Umsetzung der Informationssicherheit vom Allgemeinen in der *Leitlinie zur Informationssicherheit* und *GdIS* zum Konkreten in Richtlinien, Konzepten und Handlungsanweisungen. Wegen der Vielfältigkeit der Sicherheitsaspekte und der Eigenheiten verschiedener Vorgehensweisen und insbesondere der sich ständig wandelnden und sich vernetzenden Technologien werden die allgemeinen Sicherheitsziele durch Richtlinien, Konzepte und Handlungsanweisungen konkretisiert.

Die Verfahren zur Änderung und Neuerstellung von Dokumenten dieser fünf Ebenen, die Zuständigkeiten und die Wege zur Inkraftsetzung sind in der Richtlinie *Organisation der Informationssicherheit* beschrieben.

Die ISP beschreibt im Einzelnen:

- den Rahmen zur Sicherheit bei der Informationsverarbeitung in der DRV (*Leitlinie zur Informationssicherheit, GdIS*),
- in den Richtlinien themen- und zielgruppengerecht die einzuhaltenden Mindeststandards für bestimmte Technologien oder Vorgehensweisen (zum Beispiel Mindeststandards für die Verschlüsselung in Datennetzen oder Richtlinien zur

Datenverarbeitung durch Dritte oder Richtlinie zur Erstellung von IT-Sicherheitskonzepten),

- in Konzepten soll themenspezifisch dargestellt und festgelegt werden, welche Daten in welcher Art und Weise und von welchen Stellen zu erheben und zu verarbeiten sind, welche Rechtsgrundlagen dabei einzuhalten sind, welche Technologien wie zum Einsatz kommen sollen und welche Richtlinien (Ebene 3) dabei zu berücksichtigen sind,
- die Handlungsanweisungen sollen zielgruppengerecht den Umgang mit IT-Systemen, IT-Verfahren, IT-Services etc. konkret beschreiben.

4.2.1 Leitlinie zur Informationssicherheit

Die *Leitlinie zur Informationssicherheit* bildet die Ebene 1 der ISP. Sie enthält strategische Aussagen zur Informationssicherheit und zur Gesamtverantwortung der Geschäftsführung bzw. des Direktoriums. In der Leitlinie sind die langfristigen Sicherheitsziele festgelegt. Sie ist für alle RVTR verbindlich.

4.2.2 Grundzüge der Informationssicherheit

Die im Dokument *Grundzüge der Informationssicherheit* (*GdIS)* enthaltenen Festlegungen zur Informationssicherheit bilden die Ebene 2 der ISP und stellen verbindliche Mindeststandards dar.

Die in der *GdIS* formulierten Regelungen geben den ordnenden Rahmen für die nachfolgenden Ebenen vor, um die Ziele der DRV zur Informationssicherheit zu erreichen. Die Anforderungen sind möglichst kurz und mit hohem Abstraktionsgrad formuliert und um Verweise auf gegebenenfalls vorhandene weiterführende Dokumentationen ergänzt.

4.2.3 Richtlinien

In den Richtlinien werden auf Ebene 3 der ISP die in der *GdIS* vorgegebenen Sicherheitsanforderungen für abgegrenzte Themengebiete konkretisiert. Sie beinhalten spezifische Anforderungen, deren Umsetzung in den nachfolgenden Ebenen beschrieben ist und setzen dadurch einen Mindeststandard, der nicht unterschritten werden darf.

Es wird unterschieden zwischen

- für die gesamte DRV verbindliche Richtlinien (z. B. Richtlinie zur Datenverarbeitung durch Dritte, Richtlinie zur Datensicherung, Richtlinie zur Erstellung von IT-Sicherheitskonzepten) und

- regional- bzw. trägerspezifische Richtlinien (z. B. Richtlinie zum Betrieb von Servern, Richtlinie zur Behandlung von Sicherheitsvorfällen).[4]

Die Erstellung und Pflege der Richtlinien ist von den jeweils fachlich oder technisch zuständigen Organisationseinheiten sicherzustellen.

Die jeweils gültige Fassung einer DRV-weit verbindlichen Richtlinie ist in einer Anlage zur Richtlinie *Organisation der Informationssicherheit* dokumentiert.

Über die Zuständigkeit und transparente Veröffentlichung regional- bzw. trägerspezifischer Richtlinien entscheiden die RVTR selbst.

In jeder Richtlinie ist die verantwortliche Stelle benannt.

4.2.4 Konzepte

Konzepte bilden die Ebene 4 der ISP. In einem Konzept wird die konkrete technische (und bedingt organisatorische) Umsetzung von themenspezifischen Aufgabenstellungen unter Beachtung aller dafür maßgebenden Richtlinien beschrieben. Sie enthalten konkrete Regelungen und Vorgaben und beschreiben die praxisgerechte Realisierung der Anforderungen.

Es wird unterschieden zwischen

- für die gesamte DRV verbindlichen Konzepten und
- regional- bzw. trägerspezifische Konzepte (z. B. Virenschutzkonzept, Konzept zur IT-Sicherheitssensibilisierung und -schulung).

IT-Sicherheitskonzepte sind keine Konzepte im Sinne der Ebene 4 der ISP, sondern stellen eigenständige Dokumente dar (vgl. hierzu Kapitel 4.3)

Die jeweils gültige Fassung eines DRV-weit verbindlichen Konzeptes ist in einer Anlage zur Richtlinie *Organisation der Informationssicherheit* dokumentiert.

4.2.5 Handlungsanweisungen

Die auf Ebene 5 angesiedelten Handlungsanweisungen (Dienstanweisungen, Dienstverfügungen, Geschäftsanweisungen etc.) enthalten die konkreten Anweisungen für die Beschäftigten zur praktischen Umsetzung der Regelungen und Vorgaben aus den Ebenen 1 bis 4 der ISP. Handlungsanweisungen werden nicht DRV-weit festgelegt, sondern individuell für die jeweiligen RVTR.

[4] Mit „regional“ sind Zusammenschlüsse von RVTR zur Aufgabenerledigung im Rahmen der DRV gemeint.

4.3 Sicherheitskonzeption und standardisierte Vorgehensweise bei IT-Sicherheitskonzepten

Dieses Kapitel beschreibt die grundlegende Struktur der IT-Sicherheitskonzeption in der DRV und ist gültig für alle IT-Verfahren, IT-Services und IT-Systeme. Hierfür werden IT-Sicherheitskonzepte erstellt. Die DRV orientiert sich dabei an den Standards des BSI. Die Vorgehensweise für die Erstellung von IT-Sicherheitskonzepten wurde aufgrund der heterogenen Struktur und der Arbeitsteilung innerhalb der DRV angepasst. Daraus resultiert die Sicherheitskonzeption der DRV. Im Ergebnis wird durch Basis-IT-Sicherheitskonzepte und IT-Verfahrenssicherheitskonzepte die Umsetzung des IT-Grundschutzes vollumfänglich erreicht.

4.3.1 Sicherheitskonzeption der DRV

Alle IT-Systeme, IT-Services und IT-Verfahren der DRV sind zu erfassen. Die Modellierung stellt die Basisobjekte und deren Verzahnungen mit den einzelnen IT-Services und IT-Verfahren dar. Durch eine klare Abgrenzung der Verantwortung sollen mehrfache IT-sicherheitstechnische Bewertungen für dieselben Objekte vermieden werden. Es ist sicherzustellen, dass die Verantwortlichen die Bewertung innerhalb ihres Zuständigkeitsbereiches auf einem einheitlichen und verlässlichen Niveau vollziehen. Hierbei sind Maßnahmen zur Qualitätssicherung vorzusehen.

Bei der Erstellung der IT-Sicherheitskonzepte sind die einheitliche Nomenklatur und der einheitliche Aufbau zu beachten. Die IT-Sicherheitskonzepte der DRV-IT sind mit einer einheitlichen Kennzeichnung hinsichtlich Umfang und Reifegrad zentral zu dokumentieren. Weitere organisatorische Details sind der Richtlinie *Organisation der Informationssicherheit* zu entnehmen.

4.3.2 Basis-IT-Sicherheitskonzepte

Jeder RVTR hat ein Basis-IT-Sicherheitskonzept zu erstellen, in dem alle Objekte zu betrachten sind. Dies sind insbesondere organisatorische Gegebenheiten, Gebäude, Räume, Infrastruktur und IT-Systeme. Die Verantwortung für die Erstellung und Pflege des Basis-IT-Sicherheitskonzepts liegt bei den jeweils sachlich verantwortlichen Betreibern (z. B. IT-Betrieb, Gebäudeverwaltung). Der Schutzbedarf ist dabei mit „hoch“ einzustufen. Neben diesen Basis-IT-Sicherheitskonzepten ist das gemeinsame WAN der DRV aufgrund seiner besonderen und zentralen Bedeutung in einem eigenen Basis-IT-Sicherheitskonzept zu beschreiben.

Wird im Nachgang durch IT-Verfahren ein höheres Schutzniveau erforderlich, sind die Schutzmaßnahmen für die davon betroffenen Objekte entsprechend anzupassen.

Die genaue Vorgehensweise und die einschlägigen Festlegungen zur Erstellung und Umsetzung von Basis-IT-Sicherheitskonzepten sind in einer eigenen Richtlinie vorzugeben.

4.3.3 IT-Verfahrenssicherheitskonzepte

Die individuellen Maßnahmen und Methoden zur Absicherung eines Fachverfahrens sind durch die Fachverantwortlichen in eigenständigen IT-Verfahrenssicherheitskonzepten zu dokumentieren. Dabei kann eine erneute Betrachtung bereits in den Basis-IT-Sicherheitskonzepten enthaltener Objekte unterbleiben. Jedoch ist sicherzustellen, dass die jeweiligen verfahrensspezifischen Sicherheitsanforderungen durch die genutzten Objekte des Basis-IT-Sicherheitskonzepts erfüllt werden. Sind hier keine weitergehenden Sachverhalte zu behandeln, ist eine Referenzierung auf die einzelnen System- und Anwendungsobjekte zulässig. Ferner kann auf bereits beschriebene Verfahren, die Teil des eigenen zu beschreibenden Fachverfahrens sind, ebenfalls verwiesen werden. Auch hier hat dann eine entsprechende Referenzierung zu erfolgen.

Den zuständigen IT-Sicherheitsbeauftragten obliegt dabei, die lückenlose Betrachtung der Verfahrensstrukturen innerhalb der verschiedenen IT-Sicherheitskonzepte zu prüfen und für die vollständige Umsetzung durch die verantwortlichen Beteiligten zu sorgen.

Die genaue Vorgehensweise und die einschlägigen Festlegungen zur Erstellung und Umsetzung von IT-Verfahrenssicherheitskonzepten sind in einer eigenen Richtlinie vorzugeben.

Für nicht-IT-gestützte Geschäftsprozesse sind in gleicher Weise Sicherheitskonzepte zu erstellen.

4.3.4 Zentrale und trägerspezifische IT-Verfahren

Die oben beschriebenen IT-Verfahren gliedern sich in IT-Services und originäre IT-Verfahren. Ferner wird hier zwischen zentralen Verfahren und Services (DRV-IT) und trägerspezifischen Verfahren[5] unterschieden.

4.3.5 Gemeinsame IT-Anwendung zum Informationssicherheitsmanagement (ISM-Tool)

Zur Abbildung der oben beschriebenen Sicherheitskonzeption und zur Unterstützung des IT-Sicherheitsmanagements kommt einer gemeinsamen und zentral implementierten IT-Anwendung eine wesentliche Bedeutung zu. Die Basis-IT-Sicherheitskonzepte und die IT-Verfahrenssicherheitskonzepte der DRV-IT sowie entsprechende regionalspezifische IT-Verfahrenssicherheitskonzepte sind hier zu dokumentieren. Trägerspezifische IT-Verfahrens-sicherheitskonzepte sollten hier ebenfalls dokumentiert werden.

[5] Dazu gehören auch regionale IT-Verfahren, die von RVTR gemeinsam betrieben werden.

Organisatorische Details zum ISM-Tool sind der Richtlinie *Organisation der Informationssicherheit* zu entnehmen.

4.4 Umgang mit Sicherheitsvorfällen

4.4.1 Störung, Notfall, Krise

Sicherheitsvorfälle können die Vertraulichkeit, Verfügbarkeit und Integrität von IT-Systemen oder Datennetze beeinträchtigen. Eine lokale und/oder zeitlich begrenzte Störung kann sich zu einem Notfall oder einer Krise verschärfen.

Für diese Szenarien sind unter Berücksichtigung der hier einschlägigen Standards zum Notfallmanagement entsprechende Richtlinien, Konzepte und Handlungsanweisungen zu entwickeln, damit schnellstmöglich die Störung behoben, weitere Schäden vermieden und der Normalbetrieb wieder aufgenommen werden kann. Dies beinhaltet den Aufbau einer entsprechenden Organisationsstruktur sowie die Planung und Realisierung technischer Notfallsysteme (z. B. redundante Strukturen).

4.4.2 Meldepflichten und Untersuchung

Sicherheitsvorfälle sind unverzüglich der zuständigen Organisationseinheit zu melden, um den Schaden zu begrenzen, die Daten zu schützen und den Betrieb aufrechtzuerhalten. Unabhängig davon sind die zuständigen IT-Sicherheitsbeauftragten schnellstmöglich zu informieren und ggf. einzubinden. Wenn personenbezogene Daten betroffen sind oder sein könnten, gilt dies ebenso für die zuständigen Datenschutzbeauftragten. Die gesetzlichen Meldepflichten und die innerhalb der DRV geltenden Informationsvereinbarungen bleiben davon unberührt.

Es ist sicherzustellen, dass die Behandlung von Sicherheitsvorfällen strukturiert erfolgt und dokumentiert wird. Dabei ist darauf zu achten, dass möglichst keine Spuren gelöscht oder unbrauchbar gemacht werden.

Einem Sicherheitsvorfall gleichgestellt ist die Konstellation, wenn innerhalb des Datennetzes der DRV IT-Systeme oder Datennetze betrieben werden, die nicht die Mindestanforderungen der ISP einhalten und deshalb eine mögliche Gefährdung für andere IT-Systeme oder Datennetze darstellen.

Die Vorgehensweise und Zuständigkeiten sind in einer Richtlinie oder einem Konzept zu regeln. Dabei sind die nachstehend aufgeführten Mindestanforderungen zu beachten.

4.4.3 IT-Systeme

Stellt ein IT-System durch einen Sicherheitsvorfall eine Gefährdung dar, sind Maßnahmen zu treffen, um das Datennetz und weitere IT-Systeme zu schützen (z. B. bei einer Kompromittierung durch Schadsoftware).

4.4.4 Datennetz

Wird durch einen Sicherheitsvorfall ein Teil des eigenen Datennetzes oder des der DRV kompromittiert oder kompromittierbar, sind zusätzliche Sicherheitsmaßnahmen zum Schutz der nicht betroffenen Segmente zu treffen.

5 Aufgabenerledigung durch Dritte

Die Aufgaben der DRV werden zum Teil arbeitsteilig oder durch Dritte erledigt.

Durch die Einbindung von Dienstleistern darf das Sicherheitsniveau der DRV nicht abgeschwächt oder gefährdet werden. Die Schutzmaßnahmen sind bei Dienstleistern stets abzufragen und grundsätzlich zu überprüfen.

Es ist weiterhin zu prüfen, ob nach den geltenden Datenschutzvorschriften ein Vertrag über die Datenverarbeitung im Auftrag zu schließen ist.

Die Aufgabenerledigung durch Dritte wird in einer Richtlinie geregelt.

6 Betriebssicherheit

6.1 Sicherheit im Datennetz

Die Sicherheit des Datennetzes der DRV wird bestimmt durch ein hohes Maß an Vertraulichkeit, Integrität und Verfügbarkeit. Diese muss durch angemessene technische und organisatorische Maßnahmen gewährleistet sein. Die Zuständigkeit und damit die Verantwortung für Planung, Bereitstellung und Betrieb des Datennetzes sind eindeutig festzulegen.

Der zuständige IT-Bereich hat dabei sicherzustellen, dass bei Planung, Bereitstellung und Betrieb des Datennetzes die einschlägigen Festlegungen und Grundsätze für einen sicheren Betrieb eingehalten werden. Die Mitwirkung der IT-Sicherheitsbeauftragten ist sicherzustellen.

Beim Datentransport über Datennetze, die der DRV von externen Providern bereitgestellt werden, ist zu beachten, dass Daten durch geeignete Verschlüsselungsmechanismen zu schützen sind. Die Verwaltung der Verschlüsselungskomponenten und des

Schlüsselmaterials ist dabei als sicherheitskritisch einzustufen. Deshalb dürfen die Schlüsselverwaltung und die Verwaltung der Verschlüsselungskomponenten ausschließlich durch Beschäftigte der DRV erfolgen.

Die Anforderungen der technischen und organisatorischen Maßnahmen, die zur Sicherheit des Datennetzes getroffen werden müssen, sind in einer DRV-weiten Richtlinie zu regeln.

Datennetzübergänge und -zugänge werden ausschließlich vom jeweils zuständigen IT-Bereich bzw. der DRV-IT bereitgestellt und betrieben. Andere Datennetzübergänge und -zugänge dürfen nicht eingerichtet oder genutzt werden.

6.2 Sicherheit auf Systemebene

6.2.1 Anforderungen an die Systemsicherheit

Die Regelungen der ISP gelten unmittelbar für alle Systeme aus den Bereichen der Informations- und der Kommunikationstechnik (IT-Systeme). Die grundsätzlichen Festlegungen, die bei Absicherung der IT-Systeme zur Umsetzung der IT-Sicherheitsstrategie getroffen werden müssen, sind in einer übergreifend gültigen Richtlinie vorzugeben. Die speziellen Sicherheitsmaßnahmen sind dabei in den jeweiligen Basis-IT-Sicherheitskonzepten der verantwortlichen Betreiber zu dokumentieren. Auf Systemebene ist dabei die Zugangs- und Zugriffskontrolle besonders zu beachten.

6.2.2 Verantwortlichkeiten

Die Administration der IT-Systeme obliegt vollständig den dafür verantwortlichen Stellen des IT-Betriebs. Diese sind für die Einhaltung der einschlägigen Schutzmaßnahmen sowie der weitergehenden Regelungen zum Betrieb von IT-Systemen verantwortlich, auch wenn in Abstimmung bestimmte Aufgaben an weitere Personen oder Organisationseinheiten übertragen werden.

6.2.3 Rollentrennung, Administratorenkonzept

Insbesondere bei Host-, Speicher- und Serversystemen gibt es systemseitig Administrationsrollen („Root“, „Superadmin“), die sämtliche Zugriffsrechte des Systems in sich vereinigen. An diesen Systemen soll eine technisch-organisatorische Aufteilung mindestens in eine Betriebssystemebene und eine Anwendungsebene vorgenommen werden.

Dies bedeutet, dass soweit möglich die Rollen von System- und Fachadministration technisch getrennt sind und die Rolle eines „Root“-Administrators so abgesichert ist, dass sie nur im Notfall benutzt werden kann (z. B. geteiltes Passwort im Tresor).

6.2.4 Sicherheit auf Verfahrensebene

Für den sicheren Betrieb und die sichere Nutzung von IT-Verfahren sind bereits während der Entwicklungs- bzw. der Planungsphase eine Vielzahl von organisatorischen und technischen Sicherheitsmaßnahmen zu beachten, gerade auch, wenn die Einführung und der Betrieb trägerübergreifend erfolgen. Solche Maßnahmen sind insbesondere:

- Beachtung der maßgeblichen Gesetze, Richtlinien und weiteren Vorgaben,
- Einhaltung von Lizenz- und Urheberrechten,
- Frühzeitige Beteiligung der Verantwortlichen aus dem Bereich IT-Sicherheit und Datenschutz,
- Erstellen von IT-Sicherheitskonzepten,
- Festlegungen für Arbeitssicherheit und Benutzerfreundlichkeit,
- Beachtung weiterer Informations- und Beteiligungsrechte (z. B. Personal- und Schwerbehindertenvertretung, Aufsichtsbehörde).

Die grundsätzlichen technischen und organisatorischen Anforderungen zur Sicherheit von IT-Verfahren sind bezüglich Entwicklung und Betrieb in verbindlichen Richtlinien DRV-weit und regional- bzw. trägerspezifisch festzulegen.

7 Beschaffung

Bei der Beschaffung von IT-Systemen und IT-Anwendungen sind die Verantwortlichkeiten klar zu regeln.

Innerhalb des Beschaffungsvorgangs sind sicherheitsrelevante Aspekte insbesondere zur Vertraulichkeit, Integrität und Verfügbarkeit sowie mögliche Aspekte zu einer Datenverarbeitung im Auftrag frühzeitig zu berücksichtigen.

Weiterhin sind die entsprechenden Informations- und Beteiligungsrechte zu beachten.

Die detaillierten Anforderungen zum Thema Beschaffung sind in einer Richtlinie oder in einem entsprechenden Dokument außerhalb der ISP festzulegen.