Meine elektronische
Gesundheitsakte

ELGA GmbH

ELGA ISMS -

Informationssicherheitspolitik

Leitlinie 001

Datum: 28.09.2011

Version: 2.0

Inhaltsverzeichnis

Es wird ausdrücklich darauf hingewiesen, dass alle personenbezogenen Bezeichnungen jeweils als geschlechtsneutral formuliert zu verstehen sind.

Weiters ist zu beachten, dass die Begriffe „Patient", „Bürger" und „ELGA-Teilnehmer" synonym verwendet werden und auch Personen umfassen, die derzeit nicht an einem Behandlungs- oder Pflegeprozess teilnehmen.

1. Präambel

Hinsichtlich der erfolgreichen Umsetzung der Elektronischen Gesundheitsakte (ELGA) in Österreich ist es von entscheidender Bedeutung, dass sämtliche beteiligten Personen davon ausgehen können, dass es sich um ein sicheres System handelt, welches durch den Einsatz umfassender Datenschutz- und -Sicherheitsmechanismen bestens geschützt ist, und das Risiko von Datenmissbrauch so gut als möglich ausschließt.

Vor dem Hintergrund, dass Vertrauen in die Sicherheit von ELGA eine Grundvoraussetzung für deren Akzeptanz ist, wurde eine Arbeitsgruppe der Länder mit der Entwicklung eines Informationssicherheits-Managementsystems (ISMS) für ELGA beauftragt, damit Sicherheitsrisiken übergreifend erkannt und beseitigt werden können und ELGA gesamtheitlich den Anforderungen der heutigen Sicherheitsstandards entspricht.

Dieses wird vorab mit der ELGA GmbH akkordiert und anschließend mit den ELGA-Systempartnern abgestimmt.

2. Grundsätze

Die Informationssicherheit im Sinne dieser Leitlinie basiert auf den folgenden allgemein geltenden Grundsätzen:

- **Vertraulichkeit,** also dem Schutz gegen den unberechtigten Zugriff auf Daten und Informationen;
- **Integrität,** also der Sicherstellung der Unversehrtheit von im Zuge von Unternehmensprozessen entstehenden Daten und Informationen bzw. der korrekten Funktionsweise von Systemen;
- **Verfügbarkeit,** also der Sicherstellung einer im jeweilig festgelegten Umfang gegebenen Verwendbarkeit aller verarbeiteten Daten und Informationen. Dazu gehört die Erhaltung der Funktionstüchtigkeit der dafür notwendigen Systeme und Betriebsmittel. Davon unbenommen muss die Behandlung von Patienten jedenfalls auch ohne Verfügbarkeit von Teilen oder der gesamten ELGA möglich sein.
- **Nachweisbarkeit,** also der - den festgelegten Sicherheitsbedürfnissen entsprechenden - Dokumentation jeder Art der Handhabung von Daten und Informationen sowie der daran Beteiligten.

3. Zielsetzung

Das Ziel der ELGA-Informationssicherheitspolitik ist es, derzeitige und zukünftige Bedrohungen von ELGA durch organisatorische, technische bzw. persönlichkeitsbildende Maßnahmen in gesamtheitlicher Sicht erfassbar und beherrschbar zu machen.

Aufgrund der erheblichen strategischen Bedeutung sind Maßnahmen zur Verfolgung der Sicherheitspolitik als integrierter Bestandteil sämtlicher ELGA-Prozesse zu sehen.

Die Ziele der Sicherheitspolitik umfassen:

LL01_Z1 Die Verfügbarkeit und Kontinuität von ELGA ist, unter Berücksichtigung der jeweiligen Rahmenbedingungen, bestmöglich erfüllt.

LL01_Z2 Die Vertraulichkeit und Integrität der durch ELGA verfügbaren Informationen und Daten ist sichergestellt.

LL01_Z3 Die Einhaltung der rechtlichen Vorschriften unter Berücksichtigung der gesamtheitlichen Betrachtung der ELGA ist gewährleistet.

LL01_Z4 Das mit den ELGA-Systembetreibern abgestimmte Informationssicherheitskonzept ist in ELGA umgesetzt.

4. Verantwortung

1. Die ELGA-Systempartner sind sich ihrer Verantwortung bewusst und haben aus diesem Grund die Einführung des ELGA ISMS beschlossen.
2. Im Rahmen des ELGA ISMS wird von allen ELGA-Systembetreibern und deren Mitarbeitern erwartet, dass sie sich entsprechend dieser Politik und den daraus abgeleiteten Vorgaben und ELGA ISMS-Leitlinien verhalten, sich der eigenen Verantwortung bewusst sind und eine hohe Sensibilität hinsichtlich der Informationssicherheit in ELGA aufweisen.
3. Es wird vorausgesetzt, dass die gemeinsam etablierte ELGA ISMS-Organisation und die mit der Ausführung beauftragten Verantwortlichen sowie andere Beauftragte (z.B. Datenschutzbeauftragte, Sicherheitsbeauftragte) bei der Ausübung ihrer ELGA ISMS-Tätigkeit durch das Management der jeweiligen ELGA-Systembetreiber aktiv unterstützt werden.
4. Die ELGA ISMS-Organisation ist entsprechend der ELGA ISMS-Leitlinien mit den erforderlichen Kompetenzen ausgestattet.

5. Die Informationssicherheitspolitik und die daraus abgeleiteten ELGA ISMS-Leitlinien sind für alle ELGA-Systembetreiber verbindlich und müssen allen Mitarbeitern, die mit ELGA befasst sind, nachweisbar zur Kenntnis gebracht werden.

6. Die Informationssicherheitspolitik bezieht sich auf sämtliche Tätigkeiten, Funktionen und Prozesse, die zur Erreichung der Ziele von ELGA ausgeführt werden, wobei sowohl auf Gefahrenpotentiale von innen (sei es durch den Betrieb technisch sensibler Geräte oder durch die Mitarbeiter) als auch auf Bedrohungen von außen Bedacht zu nehmen ist.

5. Geltungsbereiche

Der Geltungsbereich des ELGA ISMS ist in Abbildung 1 dargestellt:

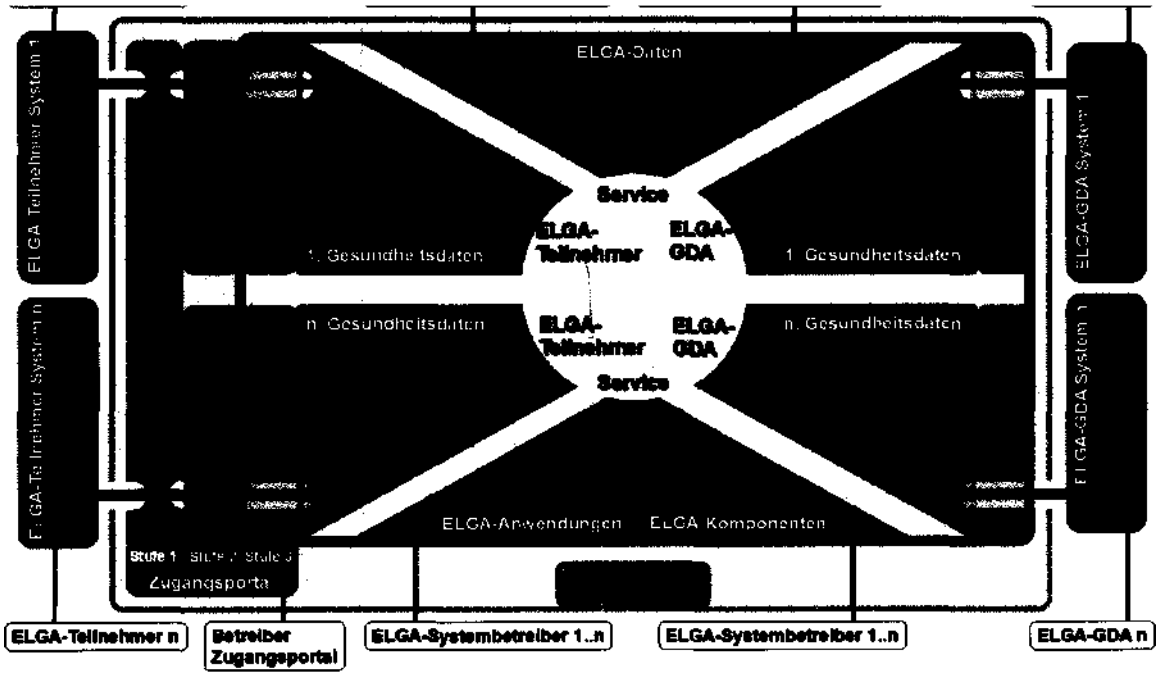

Abbildung 1: Sichtweise ELGA ISMS-Geltungsbereich

In der oberen Abbildung ist die Abgrenzung des ELGA ISMS zu beachten:

- ELGA stellt für ELGA-Teilnehmer und ELGA-Gesundheitsdiensteanbieter (ELGA-GDA) (dargestellt als blaue und grüne Elemente außerhalb des ISMS-Geltungsbereichs) eine zugangsgesicherte Kommunikationsinfrastruktur dar. Das ELGA ISMS hat keine Auswirkung auf eigene Systeme der ELGA-Teilnehmer bzw. ELGA-GDA.

Der Geltungsbereich des ELGA ISMS umfasst die gelb hinterlegten Infrastrukturelemente der ELGA-Systembetreiber:

1 ELGA-Daten

Durch die ELGA-Systembetreiber gespeicherte und bereitgestellte ELGA-Gesundheitsdaten, demographische Daten, Berechtigungs- und Protokolldaten.

2. ELGA-Komponenten

Sind jene Komponenten und Services, aus denen sich ELGA zusammensetzt. Sie werden eingeteilt in „logisch" Zentrale Komponenten (Z-PI, GDA-I, Berechtigungssystem, Protokollierung, Portal, Grundversorgungsbereich) und dezentral zur Verfügung zu stellende Komponenten (ELGA-Bereiche mit ihren Gateways, ihrer Einbindung ins Berechtigungssystem und die Protokollierung, L-PI, Register, Repositories).

3. ELGA-AnWendungen

Sind EDV-Anwendungen aus dem eHealth-Bereich, die auf Daten, die über die ELGA verfügbar sind, zugreifen oder Daten in ELGA bereitstellen. Beispiele: e-Medikation in der Österreichversion, Patientenverfügung.

4. Zugangsporta

Das Zugangsportal differenziert drei Stufen:

- Stufe 1 - allgemeine Daten: Beinhalten qualitätsgesicherte Informationen über medizinische Themen, das Gesundheitswesen und seine Leistungen, die im Rahmen des Österreichischen Gesundheitsportals (www.gesundheit.gv.at) bereitgestellt werden.
- Stufe 2 - personifizierte Daten: Ermöglicht es Benutzern nach einem Login (mittels Username und Passwort) am Österreichischen Gesundheitsportal und somit abseits von ELGA, bestimmte Anwendungen und Services des Österreichischen Gesundheitsportals zu nutzen.
- Stufe 3 - Authentifizierung: Stellt für authentifizierte ELGA-Teilnehmer und ELGA-GDA den Zugang zu ELGA dar.

Obwohl das Österreichische Gesundheitsportal nicht Teil von ELGA ist, umfasst der Geltungsbereich des ELGA ISMS ebenso die Stufen 1 und 2 des Zugangsportals, um die Sicherheit aller Daten und gegebenenfalls gemeinsam genutzter Ressourcen zu gewährleisten. Stufe 3 des Zugangsportals ist Teil des authentifizierten Sicherheitsbereichs (durch die rote Umrandung begrenzt).

Anmerkung: Die Bereitstellung und Nutzung privater Gesundheitsdaten der ELGA-Teilnehmer (blaue Bereiche innerhalb des ISMS Geltungsbereichs) ist derzeit nicht vorgesehen, wurde aber in die ISMS Darstellung aufgenommen, um für künftige Entwicklungen offen zu sein.

6. Verantwortungsbereiche

Die Entwicklung der zur Zielerreichung notwendigen Maßnahmen erfolgt zentral durch die ELGA-Sicherheitskommission[1] und dezentral durch die ELGA-Systembetreiber. Zentral werden insbesondere die Vorgaben bezüglich Informationssicherheitspolitik und -leitlinien erarbeitet, dezentral sind Vorgaben und Maßnahmen durch die ELGA-Systembetreiber zu erstellen, die im großen Maße situationsabhängig determiniert werden.

In der folgenden Abbildung werden die Verantwortungsbereiche in ELGA schematisch dargestellt:

[1] siehe ISMS-Leitlinie 002 „ELGA ISMS - Informationssicherheitsorganisation"

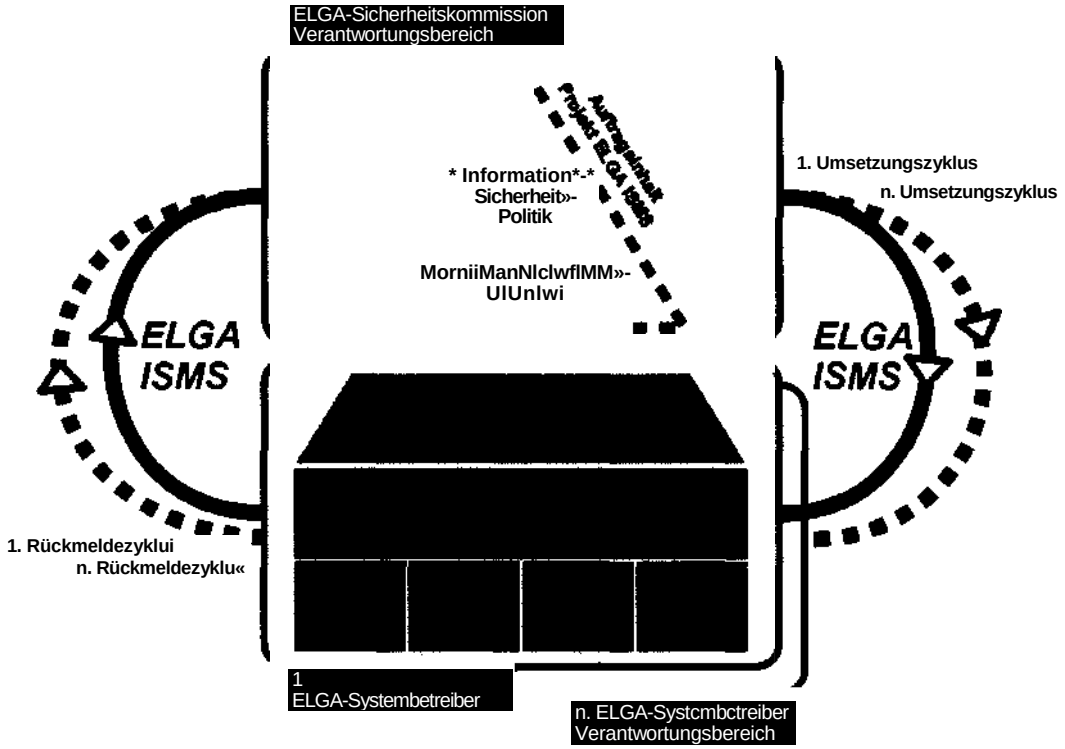

Abbildung 2: Verantwortungsbereiche in ELGA

Im Verantwortungsbereich der ELGA-Sicherheitskommission (blau umrandeter Bereich in Abbildung 2) werden die gesamtheitlichen ELGA ISMS Reglements, Methoden der Kontrolle und ELGA ISMS-Leitlinien für die ELGA-Systembetreiber abgestimmt. Im Verantwortungsbereich der ELGA-Systembetreiber (grün umrandete Bereiche) werden die ELGA ISMS-Leitlinien betrieblich angemessen und wirtschaftlich tragbar umgesetzt.

7. Vorgehensweise

Grundlage für das ELGA ISMS bildet die *International Standardisation Organisation* (ISO) *Normserie 27000.* Diese Normserie wurde adaptiert, da sie auf eine juristische Person und nicht auf ein Konstrukt von mehreren juristischen und natürlichen Personen ausgerichtet ist. Damit ist die ISO 27000 zwar nicht direkt anwendbar, trotzdem wird systematisch und methodisch danach vorgegangen. Die ISMS-Leitlinien sind so aufgebaut, als ob ELGA von einer juristischen Person betrieben wird, wobei die einzelnen beteiligten ELGA-Systembetreiber als Teilorganisationen gesehen werden. Die daraus resultierenden Verpflichtungen sind über Verträge abzusichern.

Ausgehend vom prozessorientierten Ansatz der ISO 27000 werden nach dem Plan-Do-Check-Act-Modell (PDCA) die Informationssicherheitsanforderungen und -erwartungen von den ELGA-Systembetreiben erhoben und eine Informationssicherheitspolitik für ELGA festgelegt, welche die Grundlage für die weiteren Sicherheitsüberlegungen darstellt. Anschließend wird durch das Festlegen von Aktionen und Prozessen jene Informationssicherheit erzielt, die den Anforderungen und Erwartungen entspricht.

In Abbildung 3, welche der ISO 27001 [1, S.6] entnommen ist, wird der PDCA-Prozess schematisch dargestellt:

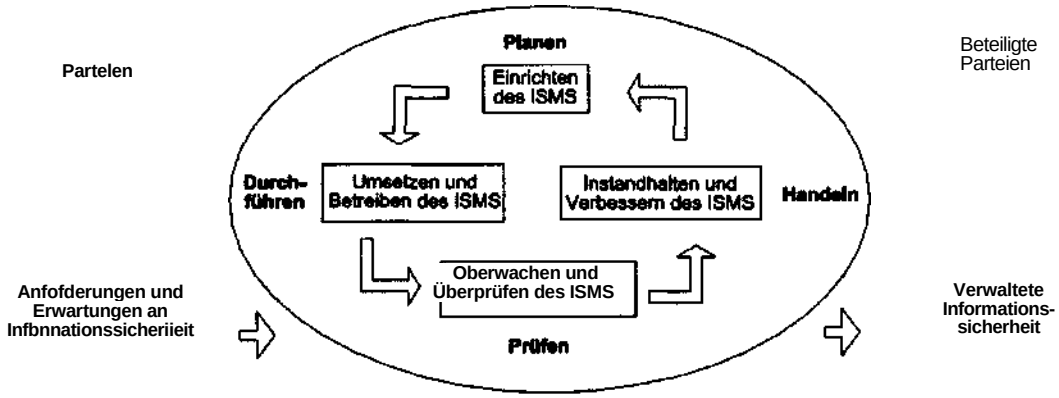

Abbildung 3: PDCA-Modell der ISO

Um der organisationsübergreifenden Verantwortung und der daraus resultierenden Erhöhung der Komplexität Rechnung zu tragen, wurde das PDCA-Modell erweitert, indem im Wirkungsbereich der ELGA GmbH (Leitung der ELGA-Sicherheitskommission) und zwischen den ELGA-Systembetreibern ein übergreifendes Vorgehensmodell für die Etablierung, den Betrieb und die kontinuierliche Verbesserung eines Informationssicherheits-Managementsystems geschaffen wird.

In Abbildung 4 wird die übergreifende Sichtweise im ELGA l SMS-Vorgehensmodell dargestellt.

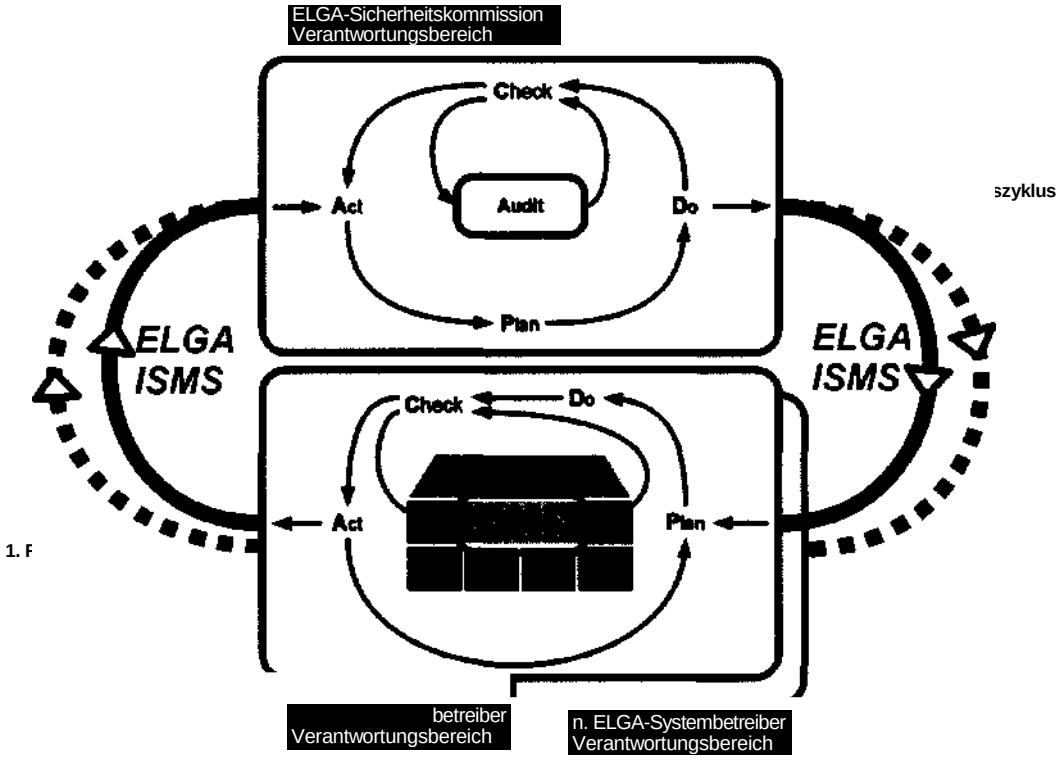

Abbildung 4: ELGA I SMS-Vorgehensmodell

7.1. PDCA-Zyklus der ELGA-Sicherheitskommission

Der jeweilige Status des PDCA-Zyklus im Verantwortungsbereich der ELGA-Sicherheitskommission (blau umrandeter Bereich in Abbildung 4) ist dabei wie folgt zu verstehen:

1. Plan-Status (ELGA-Sicherheitskommission)

   In diesem Status wird eine Bearbeitung der inhaltlichen Themen (Informationssicherheitspolitik und Informationssicherheitsleitleitlinien) angestoßen und unter Berücksichtigung der Aktionen aus dem Act-Status weiterentwickelt.

2. Do-Status (ELGA-Sicherheitskommission)

   In diesem Status wird der Plan umgesetzt.

3. Check-Status (ELGA-Sicherheitskommission)

   In diesem Status wird die Umsetzung gemessen und bewertet. Externe Faktoren, wie gesetzliche oder technische Änderungen und „Best Practices", fließen hier ein.

4. Act-Status (ELGA-Sicherheitskommission)

In diesem Status werden für alle Verantwortungsbereiche der gesamten ELGA auf Basis des Prüfberichtes aus dem Check-Status und unter Berücksichtigung der Rückmeldungen der ELGA-Systembetreiber vorbeugende und korrigierende Maßnahmen gesetzt.

7.2. PDCA-Zyklus der ELGA-Systembetreiber

Der jeweilige Status des PDCA-Zyklus im Verantwortungsbereich der ELGA-Systembetreiber (grün umrandete Bereiche in Abbildung 4) ist dabei wie folgt zu verstehen:

1. Plan-Status (ELGA-Systembetreiber)

   In diesem Status werden die inhaltlichen Themen der ELGA-Sicherheitskommission eingearbeitet und unter Berücksichtigung der Aktionen aus dem Act-Status im jeweiligen Verantwortungsbereich des ELGA-Systembetreibers weiterentwickelt. Das Ergebnis ist der Plan, der im Verantwortungsbereich der ELGA-Systembetreiber umzusetzen ist.

2. Do-Status (ELGA-Systembetreiber)

   In diesem Status wird der Plan umgesetzt.

3. Check-Status (ELGA-Systembetreiber)

   In diesem Status wird die Umsetzung gemessen und bewertet. Externe Faktoren, wie gesetzliche oder technische Änderungen und „Best Practices", fließen hier ein.

4. Act-Status (ELGA-Systembetreiber)

   In diesem Status werden für die jeweiligen Verantwortungsbereiche der ELGA-Systembetreiber auf Basis des Prüfberichtes aus dem Check-Status vorbeugende und korrigierende Maßnahmen gesetzt.

Die ELGA ISMS-Leitlinien legen Mindestanforderungen fest, die um zukünftige geeignete ELGA-Checklisten ergänzt werden (kontinuierlicher Verbesserungsprozess).

8. Relation zwischen Aufwand und Sicherheitszuwachs

Allen Beteiligten ist bewusst, dass eine absolute Sicherheit selbst mit erheblichem Aufwand nicht zu realisieren ist. Eine Grundabsicherung ist hingegen mit relativ geringem Aufwand möglich. Die zusätzlichen Kosten für einen Sicherheitszuwachs steigen progressiv, je höher das bereits erreichte Sicherheitsniveau ist.

Auf Basis dieser Betrachtungen ist das Sicherheitszielniveau in jenem Bereich anzusiedeln, in dem die zusätzlichen Kosten im Verhältnis zum zu erzielenden Sicherheitszuwachs zu rechtfertigen sind.

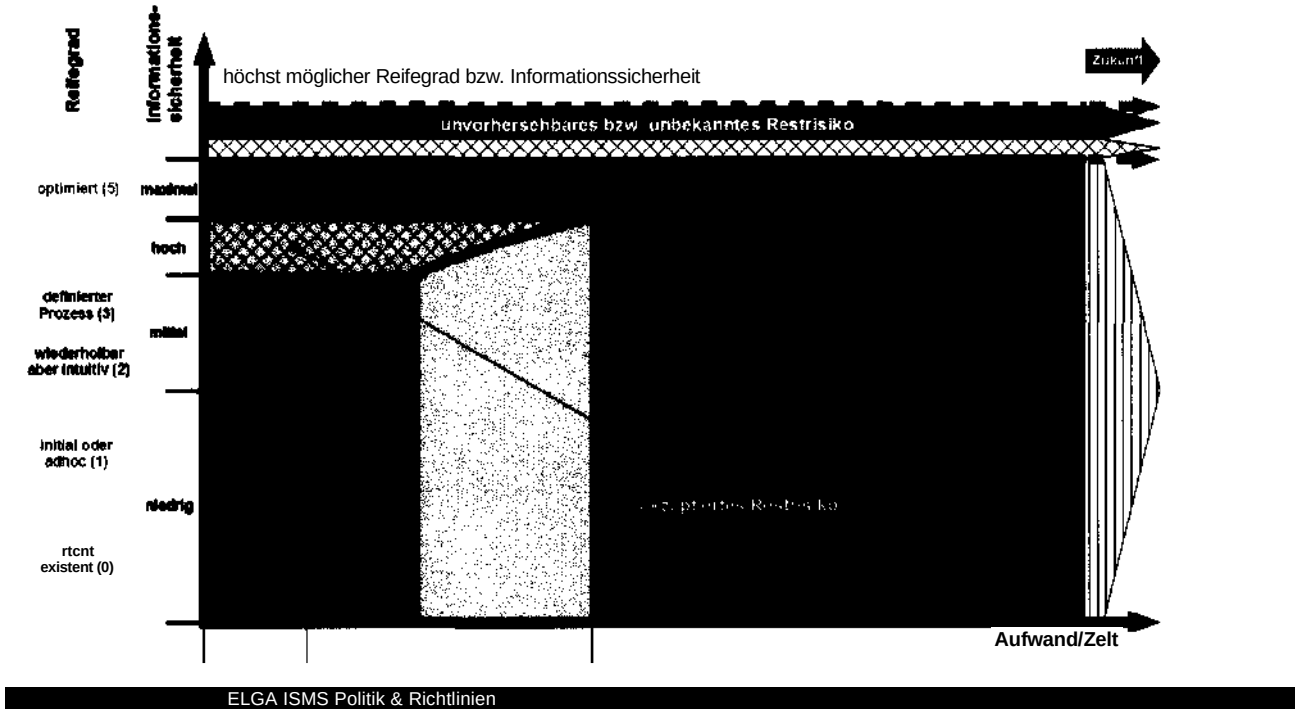

Abbildung 5: Zusammenhang Reifegrad und Aufwand

In Abbildung 5 wird das *Reifegradmodell* nach COBIT[2] *[2,* S.32] und das Modell *Sicherheitszugewinn nach Aufwand und Zeit* nach BSI[3] [3] zusammengeführt. Diese stellen die Basis für die Einführung, den Betrieb und die Optimierung eines ELGA ISMS dar.

Dieses kombinierte Modell ermöglicht, in Verbindung mit dem ELGA ISMS-Vorgehensmodell (Abbildung 4) im Zuge des Check-Status, die Bewertung des ELGA ISMS in seiner Gesamtheit oder seinen Teilen. In Verbindung mit der Aufwands-/Zeitachse wird ebenso die

Control Objectives for Information and related Technology
Bundesamt für Sicherheit in der Informationstechnik (Deutschland)

zeitliche Dimension (Phasen der Umsetzung des ELGA ISMS in den verschiedenen Verantwortungsebenen) dargestellt.

Der Reifegrad - und damit das akzeptierte Restrisiko - ermöglicht eine Bewertung des ELGA ISMS, welche auf unterschiedlichen Faktoren basieren kann. Beispielsweise wäre die Beurteilung des technischen Reifegrades eines oder mehrerer ELGA-Systembetreiber möglich. Welche Key Performance Indikatoren (KPI) für die Bewertung des ELGA ISMS angewendet werden, ist zwischen der ELGA GmbH und den ELGA-Systembetreibern noch zu definieren.

9. Leitlinien

Da es sich hierbei um langfristig orientierte Grundlagendokumente handelt, sind technische Details sowie Einzelheiten zu Informationssicherheitsmaßnahmen und deren Umsetzung nicht Bestandteil der ELGA-Informationssicherheitspolitik.

Zentrales Anliegen der Informationssicherheitspolitik ist es, den Betrieb und die Sicherheit von ELGA im Hinblick auf Vertraulichkeit, Integrität, Verfügbarkeit, Nachweisbarkeit (Nichtabstreitbarkeit) und Ordnungsmäßigkeit durch technische und/oder organisatorische Maßnahmen und unter Bereitstellung entsprechender Ressourcen, unter Wahrung der Effizienz, Effektivität und Qualität, zu gewährleisten und das existente Risiko auf ein beherrschbares Maß zu senken.

Der Fokus der Informationssicherheit in ELGA ist auf die Besonderheit der verteilten Aufgaben, Kompetenzen und Verantwortungen zu legen.

Bei der (elektronischen) Verarbeitung und Bereitstellung von persönlichen und gesundheitsbezogenen Daten ist besondere Rücksicht auf die Rechte des ELGA-Teilnehmers zu nehmen. Dabei ist die jeweils geltende Rechtslage zu berücksichtigen, insbesondere das Datenschutzgesetz, das Gesundheitstelematikgesetz und alle weiteren für ELGA geltenden Gesetze und Verordnungen sowie die Grundsätze der ordnungsgemäßen Datenverarbeitung.

Bei der Planung und Durchführung von organisatorischen und technischen Maßnahmen zur Erreichung der definierten Sicherheitsziele ist darauf Bedacht zu nehmen, dass die Aufmerksamkeit des medizinischen Personals primär dem Patienten gelten muss.

Tabelle 1 listet in Anlehnung an das bewährte Vorgehensmodell der ISO 27000 Normserie und das im deutschsprachigen Raum weit verbreitete Prozessmodell des Grundschutzhandbuches des deutschen Bundesamtes für Informationssicherheit (BSI), die folgenden ELGA ISMS-Leitlinien auf:

ELGA ISMS-Leitlinien	
001	ELGA ISMS - Informationssicherheitspolitik
002	ELGA ISMS - Informationssicherheitsorganisation
003	ELGA ISMS - Risikomanagement
004	ELGA ISMS - Personelle Sicherheit
005	ELGA ISMS - Generelle Vorgaben für die physische und umgebungsbezogene Sicherheit
006	ELGA ISMS - Generelle Vorgaben für die Netzwerksicherheit und Rechnerverwaltung
007	ELGA ISMS - Systemzugriffsüberwachung und Zugriffskontrolle
008	ELGA ISMS - Beschaffung, Entwicklung und Wartung von ELGA-Komponenten und ELGA-Anwendungen
009	ELGA ISMS - Betriebliches Kontinuitätsmanagement
010	ELGA ISMS - Generelle Vorgaben für die Erfüllung der Verpflichtungen
011	ELGA ISMS - Datenschutz

Tabelle 1: Übersichtstabelle der ELGA ISMS-Leitlinien

10. Berücksichtigung der Datenschutzvorgaben

Die ELGA ISMS - Datenschutz-Leitlinie ist zu berücksichtigen und aktiv umzusetzen.

11. Weiterentwicklung

Die Inhalte der ELGA-Informationssicherheitspolitik unterliegen einer laufenden Beobachtung und Anpassung, insbesondere unter Beachtung der Entwicklung von Gesetzen und EU-Richtlinien sowie Aspekten der Wirtschaftlichkeit.

12. Einhaltung

Die Verantwortung für die Einhaltung der, in der ELGA-Informationssicherheitspolitik festgeschriebenen, ELGA ISMS-Leitlinien sowie die Erstellung der daraus notwendigen und erforderlichen Organisationskonzepte, obliegt den jeweiligen ELGA-Systembetreibern und der ELGA GmbH im Auftrag der ELGA-Systempartner.

Die ELGA-Informationssicherheitspolitik tritt mit sofortiger Wirkung in Kraft und ist allen Personen, die mit der Umsetzung von ELGA-Informationssicherheitsmaßnahmen betraut sind, zur Kenntnis zu bringen.

13. Abkürzungen und Begriffe

Abkürzungen und Begriffserklärungen befinden sich im ELGA ISMS - Leitlinien-Glossar.

14. Abbildungsverzeichnis

15. Tabellenverzeichnis

16. Literaturverzeichnis

[1] Österreichisches Normungsinstitut. ISO/IEC 27001:2005 - Informationstechnologie -Sicherheitstechnik: Informationssicherheits-Managementsysteme -Anforderungen. Wien, 2008.

[2] IT Governance Institute. COBIT 4.0, 2005. Available from: http://www.isaca.at/index.php?option=com_docman&task=doc_download&gid=36&Itemid=60 . Letzter Zugriff: Juli 2011.

[3] Bundesamt für Sicherheit in der Informationstechnik (Deutschland). BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, 2008. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002.pdf? _ blob=publicationFile. Letzter Zugriff: Juli 2011.

Meine elektronische
Gesundheitsakte

ELGA GmbH

ELGA ISMS -

Informationssicherheitsorganisation

Leitlinie 002

Datum: 28.09.2011

Version: 2.0

Inhaltsverzeichnis

Es wird ausdrücklich darauf hingewiesen, dass alle personenbezogenen Bezeichnungen jeweils als geschlechtsneutral formuliert zu verstehen sind.

1. Präambel

Die Leitlinie zur Informationssicherheitsorganisation beruht auf der ELGA-Informationssicherheitspolitik.

Diese Leitlinie nimmt beim Betrieb von ELGA Bedacht auf die Prinzipien der Ordnungsmäßigkeit, der Rechtmäßigkeit, der Wirtschaftlichkeit, der Sparsamkeit, der Zweckmäßigkeit und der Einheitlichkeit.

2. Grundsätze

Durch diese Leitlinie und den darauf basierenden nachgelagerten Leitlinien und ggf. daraus abgeleiteten Checklisten und Empfehlungen wird/werden:

1. ein hohes Sicherheitsbewusstsein geschaffen,
2. der Aufbau einer übergreifenden Informationssicherheitsorganisation (ISiOrg) festgelegt,
3. die jeweiligen Aufgaben und Verantwortlichkeiten mit den erforderlichen Kompetenzen zugewiesen,
4. die Basis für eine kontinuierliche Weiterentwicklung der Informationssicherheitsprozesse geschaffen und
5. gemeinsame Mindeststandards von Informationssicherheitsmaßnahmen nach einheitlichen Grundsätzen festgelegt.

3. Zielsetzung

Ziele dieser Leitlinie sind:

LL02_Z1 Die Ziele der gesamten ELGA mit all ihren Komponenten und Subsystemen, deren Organisation und Betriebsführung sind durch koordinierende Maßnahmen und Rahmenbedingungen als ganzheitliches System besser versteh- und steuerbar.

LL02_Z2 Die Sicherheit und der Schutz aller Daten von ELGA-Teilnehmern, ELGA-GDA und deren Systembetreibern und Mitarbeitern sind gewährleistet.

LL02_Z3 Die Leistungen, die mit Hilfe von ELGA erbracht werden können, sind patientengerecht, effizient und effektiv gestaltet.

LL02_Z4 Der Organisationsgrundsatz nach dem Prinzip einer klaren Zuteilung von Aufgaben, Kompetenzen und Verantwortlichkeiten ist realisiert.

LL02_Z5 Eine angemessene und überprüfbare Sicherheitskultur in ELGA, der die ELGA-Benutzer vertrauen können, ist vorhanden.

LL02_Z6 Ein Notfall- und Wiederanlaufprozess liegt vor, ist etabliert und wird regelmäßig geprüft.

4. Geltungsbereich

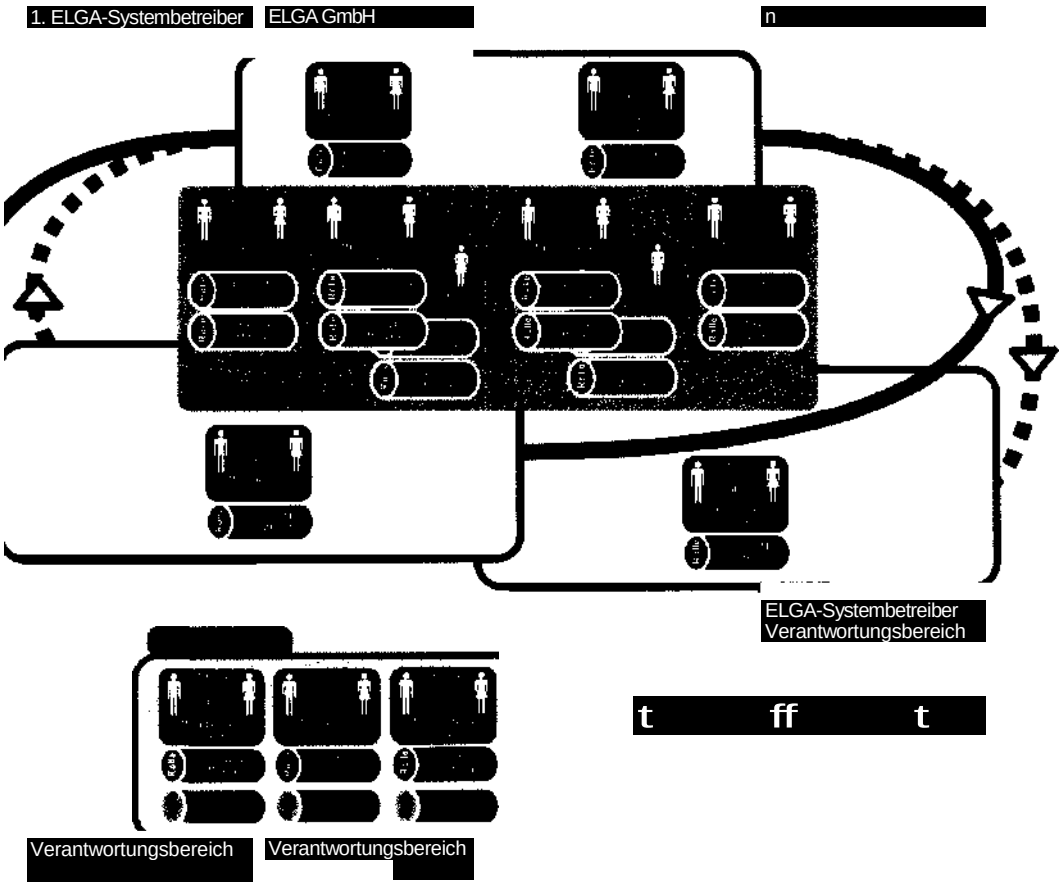

Abbildung 1: ELGA-Informationssicherheitsorganisation

^. Der Geltungsbereich dieser Leitlinie erstreckt sich auf die ELGA GmbH und alle ELGA-Systembetreiber.

2. Die Verantwortung für die Informationssicherheit in ELGA liegt bei der ELGA GmbH und den ELGA-Systembetreibern. Diese sind sich der damit verbundenen Verantwortung bewusst.

3. Jeder Mitarbeiter der ELGA GmbH und der ELGA-Systembetreiber muss daher hinsichtlich der Sicherheitsvorgaben und Sicherheitsmaßnahmen innerhalb seines Wirkungsbereichs in ELGA geschult sein und entsprechend danach handeln.
4. Im Falle einer Beauftragung von Leistungen an Dritte sind diese nachweislich zu verpflichten, die jeweils geltenden gesetzlichen und die ELGA-Sicherheitsvorgaben einzuhalten.
5. Den Leitern der ELGA GmbH und der ELGA-Systembetreiber obliegen in ihrem Verantwortungsbereich insbesondere folgende Aufgaben für ELGA:
    - Feststellung des Schutzbedarfs und des Informationssicherheitsniveaus,
    - Erlassung von Informationssicherheitskonzepten und Durchführungsbestimmungen,
    - Weiterentwicklung der Informationssicherheit und der dazugehörigen Prozesse,
    - Förderung des Sicherheitsbewusstseins der Mitarbeiter,
    - Berichtswesen an die jeweils übergeordnete Instanz.
6. Die ELGA-Systembetreiber können ihre Aufgaben im eigenen Wirkungsbereich wahrnehmen und gestalten. Sie können sich zur Vorbereitung und Unterstützung ihrer Aufgaben sowie zur Kontrolle und Steuerung der Informationssicherheitsprozesse, angepasst an die betrieblichen Erfordernisse, auch qualifizierter Dritter bedienen.
7. ELGA ist Teil einer kritischen Infrastruktur und daher speziell zu schützen (Critical Information Infrastructure Protection (CUP))[1]. Eine Abstimmung mit nationalen und internationalen Sicherheitsgremien und/oder Projekten wie z.B. epSOS[2] [2] oder STORK[3] [3] ist durchzuführen.

[1] siehe Masterplan zum Schutz kritischer Infrastruktur (ACIP) lt. Beschluss des Nationalen Sicherheitsrates (Österreich) [1]
[2] European Patients Smart Open Services
[3] Secure Identity Across Borders Linked

5. Aufbauorganisation

5.1. Organisation der Informationssicherheit

Betreiber von ELGA-Komponenten und definierter ELGA-Anwendungen müssen bereits bei Inbetriebnahme eine entsprechende Sicherheitsorganisation vorweisen können. Sie müssen unabhängig ihrer Größe und ihres Reifegrades einen Grundschutz gewährleisten, der mit der Teilnahme an ELGA bestätigt wird und bei dessen Ausfall von einer entsprechenden Haftung auszugehen ist. Geeignete Dienstleister können Informationssicherheitsaufgaben übernehmen, wenn sie über eine ausreichende Sicherheitsorganisation verfügen.

Die Organisation der Informationssicherheit setzt sich aus nachstehenden Rollen und den damit verbundenen Aufgaben zusammen:

- den von jedem ELGA-Systembetreiber und der ELGA GmbH zu bestellenden ISMS-Beauftragten
- dem ISMS-Koordinator der ELGA GmbH
- der ELGA-Sicherheitskommission

Eine Rolle kann von mehreren Personen wahrgenommen werden. Die Rollen ISMS-Koordinator und l SMS-Beauftragter der ELGA GmbH können nicht durch ein und dieselbe Person abgedeckt werden.

5.1.1. ISMS-Beauftragter

Dem l SMS-Beauftragten obliegt insbesondere:

1. die Beratung (Empfehlungen, Verbesserungsvorschläge) bezüglich informationssicherheitsrelevanten Frage- und Problemstellungen;
2. die Sicherstellung der Umsetzung informationssicherheitsrelevanter Vorgaben in Abstimmung mit dem jeweils organisatorisch Zuständigen bzw. den zuständigen Seh utzbeauftragten;
3. die Durchführung von entsprechenden Sensibilisierungsveranstaltungen, Schulungen, Arbeitskreisen, Vorträgen und dergleichen;
4. die Erstellung eines jährlichen Informationssicherheitsberichtes für seinen Wirkungsbereich;
5. die Mitwirkung an einem übergreifenden ELGA-Informationssicherheitsbericht;
6. in seinem Bereich das Risikomanagement für ELGA wahrzunehmen und zwar in Abstimmung mit dem ISMS-Koordinator;

7. im Rahmen seiner Kontrolltätigkeit die Untersuchung bzw. Mitwirkung an der Untersuchung von eventuell informationssicherheitsrelevanten Ereignissen in Zusammenarbeit mit den betroffenen Schutzbeauftragten;
8. die Erarbeitung von Umsetzungsvorschlägen zu konkreten Informationssicherheits maßnahmen in Abstimmung mit den ELGA-Systembetreibern;
9. die Gewährleistung der Dokumentation der gesetzten Informationssicherheits maßnahmen in seinem Bereich;
10. eine Nahtstellenfunktion zu den aufgrund der gesetzlichen und internen Vorgaben für spezielle Bereiche etablierten Schutzbeauftragten (z.B. Arbeitnehmerschutz, Brandschutz, Datenschutz, Gebäudeschutz, Strahlenschutz), soweit die Informationssicherheit davon betroffen ist.

5.1.2. ISMS-Koordinator

Dem ISMS-Koordinator obliegt insbesondere:

1. die Beratung der Geschäftsführung der ELGA GmbH und der ELGA-Sicherheitskommission in informationssicherheitsrelevanten Frage- und Problemstellungen;
2. die Erstellung des Informationssicherheitsberichtes für die ELGA-Sicherheitskommission;
3. die Kompetenz, die Informationssicherheitsberichte der ELGA-Systembetreiber verpflichtend einzufordern;
4. in regelmäßigen Abständen, aber mindestens jährlich, eine Abstimmung mit den Sicherheitsbeauftragten der ELGA-Systembetreiber durchzuführen und die Ergebnisse in seinen Bericht einzuarbeiten;
5. die Mitwirkung an der kontinuierlichen Weiterentwicklung des ELGA ISMS;
6. die Ausarbeitung und Umsetzung von Kontrollmaßnahmen in Abstimmung mit der ELGA-Sicherheitskommission.

5.1.3. ELGA-Sicherheitskommission

Die ELGA-Sicherheitskommission setzt sich zusammen aus:

- Geschäftsführung der ELGA GmbH (Vorsitz),
- ISMS-Koordinator und
- ISMS-Beauftragte der Betreiber zentraler und dezentraler ELGA-Komponenten,
- Auskunftspersonen/Sicherheitsexperten (optional).

Die ELGA-Sicherheitskommission hat sich eine Geschäftsordnung zu geben.

Der ELGA-Sicherheitskommission obliegt insbesondere:

1. Beratung und Beschlussfassung bezüglich ISMS hinsichtlich:
    - Umsetzung und Anpassung
    - Compliance,
    - Qualitätssicherung und Weiterentwicklung;
2. Beschluss des Sicherheitsberichtes.

5.1.4. CERT

Die ELGA GmbH und die ELGA-Systembetreiber haben beim Aufbau eines *Computer Emergency Response Teams* (E-Health CERT) mitzuwirken. Dieses ist in Abstimmung mit dem *CERTAustria [4]* zu realisieren und zu betreiben. Dabei sind die bestehenden Infrastrukturen zu nützen, damit Synergien entstehen und die Reaktionszeiten verbessert werden können.

Im Rahmen eines CERTs werden, anders als bei den vorhandenen Maßnahmen für Rechner- und Netzwerksicherheit, die Angriffe und (Sicherheits-)Vorfälle in den Fokus gerückt. Damit wird das Wissen über Vorfälle für unterschiedliche Zielgruppen nutzbar gemacht, um weitere Schäden zu begrenzen oder ganz abzuwehren. Angepasste Verfahren machen Vorfälle erkennbar, erlauben raschere Gegenmaßnahmen und tragen so ebenfalls wirksam zu dem globalen Ziel bei, die Zahl von Angriffen und Vorfällen, und damit Schäden für ELGA, zu minimieren.

6. Abläufe der ELGA-Informationssicherheit nach PDCA

Die Inhalte der Informationssicherheitspolitik unterliegen einer laufenden Beobachtung und Anpassung, insbesondere unter Beachtung der Entwicklung von Gesetzen und EU-Richtlinien sowie Aspekten der Wirtschaftlichkeit.

In strenger Anlehnung an die ISO 27000 Normserie [5, 6] wird zur Umsetzung und Sicherstellung der Qualität des ELGA ISMS das in der Leitlinie „ELGA ISMS -Informationssicherheitspolitik" vorgestellte Plan-Do-Check-Act-Modell (PDCA) angewandt.

6.1. Plan-Do-Check-Act-Modell: „Planen"

1. Einrichten einer Informationssicherheitspolitik sowie von Zielen, Prozessen und Verfahren, die für das Risikomanagement und die Verbesserung der Informationssicherheit notwendig sind, um Ergebnisse im Einklang mit den übergeordneten Grundsätzen, Zielen und Strategien der ELGA, der ELGA GmbH, der ELGA-Systempartner sowie der ELGA-Systembetreiber zu erreichen.
2. Formulierung eines Risikobehandlungsplans durch die ELGA GmbH und ELGA-Systembetreiber, der die geeigneten Aktionen des Managements, Ressourcen, Verantwortlichkeiten und Prioritäten für das Management von Informationssicherheitsrisiken identifiziert;
3. Informationen und Daten müssen durch Festlegung eines angemessenen Sicherheits und Kontrollumfangs durch die ELGA GmbH und die ELGA-Systembetreiber geschützt werden. Dabei ist zu berücksichtigen, dass
   - der festgelegte Schutz der Daten und Informationen ihrer geschäftlichen/betrieblichen Relevanz entspricht,
   - die erforderlichen Daten und Informationen für die jeweiligen Geschäftsanforderungen zugänglich sind,
   - die festgelegten Aufbewahrungs-, Weitergabe- und Qualitätsvorschriften, sowie die mit den Daten und Informationen verbundenen gesetzlichen, vertraglichen und aufsichtsrechtlichen Verpflichtungen erfüllt werden.
4. Als Ergebnis liegt ein entsprechender Prüfplan vor.

6.2. Plan-Do-Check-Act-Modell: „Durchführen"

Umsetzen und Durchführen der Informationssicherheitspolitik, Maßnahmen, Prozesse und Verfahren.

1. Umsetzung des Risikobehandlungsplans durch die ELGA GmbH und die ELGA-Systembetreiber, um die identifizierten Maßnahmenziele zu erreichen, einschließlich der Berücksichtigung der Finanzierung und der Zuweisung von Rollen und Verantwortlichkeiten;
2. Umsetzung von Programmen für Schulung und Bewusstseinsbildung durch die ELGA GmbH und die ELGA-Systembetreiber.
3. Verwaltung des Betriebs des ISMS durch die ELGA GmbH und die ELGA-Systembetreiber;
4. Verwaltung der Ressourcen für das ISMS durch die ELGA GmbH und die ELGA-Systembetreiber;
5. Umsetzung von Verfahren und anderen Maßnahmen, die eine sofortige Erkennung von Sicherheitsereignissen und eine Reaktion auf Sicherheitsvorfälle ermöglichen durch die ELGA GmbH und die ELGA-Systembetreiber.

6.3. Plan-Do-Check-Act-Modell: „Prüfen"

1. Bewerten und gegebenenfalls Messen der Prozessleistung an der Informationssicherheitspolitik, den ISMS Zielen und den praktischen Erfahrungen; Berichten der Ergebnisse an das eigene Management und an die ELGA-Sicherheitskommission zur Überprüfung.
2. Die Überprüfung der Effizienz und Effektivität der gesetzten Sicherheitsmaßnahmen ist durch die ELGA GmbH und die ELGA-Systembetreiber sicherzustellen. Im Rahmen dieser Prüfung ist das Funktionieren von Sicherheitsabläufen regelmäßig zu kontrollieren und die Prüfergebnisse sind zu dokumentieren.
3. Darüber hinaus können Prüfungen aus besonderem Anlass von der ELGA GmbH und den ELGA-Systembetreibern im festgelegten Wirkungsbereich beauftragt werden.
4. Ein Prüfungsergebnis hat jedenfalls den Reifegrad der Sicherheit des ISMS zum Ausdruck zu bringen, welcher nach dem COBIT-Schema [7, S.21 ff] festzustellen ist. In Abhängigkeit vom erreichten Reifegrad sind unterschiedliche Auditintervalle vorzusehen.

Reifegradschema nach COBIT

0 - nicht existent	Es wurde noch kein Prozess umgesetzt.
1 - initial oder adhoc	Die Notwendigkeit für die Einführung eines Prozesses wurde erkannt. Es gibt allerdings zum derzeitigen Zeitpunkt keine standardisierten Prozesse, sondern adhoc-Ansätze auf individueller Basis, deren Umsetzung von Fall zu Fall verschieden sein kann.
2 - ist wiederholbar aber intuitiv	Es wurde begonnen einen Prozess zu definieren, der bereits von unterschiedlichen Personen eingehalten wird. Dieser Prozess wurde allerdings noch nicht kommuniziert und geschult.
3 - definierter Prozess	Die Prozessabläufe wurden standardisiert, dokumentiert und geschult. Die Anwendung der Prozesse bleibt aber auf dieser Ebene immer noch den einzelnen Personen überlassen.
4 - geführt und messbar	Auf dieser Ebene findet eine regelmäßige Überwachung der Prozesse statt. Wenn erkannt wird, dass ein Prozess nicht effektiv ist, so wird dieser kontinuierlich überarbeitet und verbessert.
5 - optimiert	In diesem Zustand wurden Prozesse so weit verbessert, dass sie als „best practice" angesehen werden können. Es findet eine regelmäßige Überwachung und Verbesserung statt.

6.4. Plan-Do-Check-Act-Modell: „Handeln"

1. Ergreifen von Korrektur- und Vorbeugungsmaßnahmen, basierend auf den Ergebnissen interner ISMS Audits und Management-Überprüfungen oder anderen wesentlichen Informationen, um eine ständige Verbesserung des ISMS zu erreichen.
2. Melden von sicherheitsrelevanten Vorkommnissen an das E-Health GERT, nach dessen Meldepflichten.
3. Mitteilung der Maßnahmen und Verbesserungen an alle beteiligten Parteien in einem den Umständen angemessenen Detaillierungsgrad und gegebenenfalls Abstimmung des weiteren Vorgehens durch die ELGA GmbH und die ELGA-Systembetreiber.
4. Sicherstellung, dass die Verbesserungen die beabsichtigten Ziele erreichen.

7. Berichtswesen

1. Über den Zeitraum jedes Kalenderjahres ist für die einzelnen ELGA-Systembetreiber ein Informationssicherheitsbericht durch deren ISMS-Beauftragten zu erstellen und dem ISMS-Koordinator zu übermitteln.
2. Der ISMS-Koordinator fasst die Berichte zusammen und bringt sie in die ELGA-Sicherheitskommission ein.
3. Die ELGA GmbH berichtet jährlich nach Beschlussfassung durch die ELGA-Sicherheitskommission eine entsprechende Zusammenfassung an ihre Gremien.
4. Die ELGA GmbH publiziert mindestens alle zwei Jahre einen ELGA-Sicherheitsbericht nach Freigabe durch die Gremien.
5. Alle Berichte haben jedenfalls folgende Punkte zu enthalten:
   - Darstellung der Ist-Situation,
   - Bericht über Sicherheitsaktivitäten,
   - Rückblick und Mittelfristplanung,
   - Tätigkeitsbericht über die in dem betreffenden Jahr gesetzten sicherheitsrelevanten Maßnahmen, sowie
   - empfohlene Maßnahmen und deren Umsetzungsstand,
   - Kennzahlen zur Informationssicherheit wie Reifegrad, Verfügbarkeit, etc.

8. Maßnahmen

8.1. Change Management

LL02_M1 Mit der Einführung bzw. der Optimierung des Change Managements wird sichergestellt, dass Änderungen an ELGA:

- jederzeit nachvollziehbar,
- in geordneter,
- effizienter Weise,
- bei auftretenden Problemen ganz oder teilweise umkehrbar und
- qualitätsgesichert

implementiert werden.

LL02_M2 Die Aufgabe des Change Managements basierend auf ITIL[4] Best Practice ist es, sicherzustellen, dass standardisierte Methoden und Verfahren zur effizienten Durchführung von Änderungen (Changes) existieren, um Auswirkungen von änderungsbedingten Störungen auf die IT-Services der ELGA zu minimieren.

LL02_M3 Aufgrund der Vernetzung von ELGA, des Zusammenwirkens aller Subsysteme und notwendiger Dokumentationen, wie zum Beispiel der Notfallplanungen, müssen Changes sorgsam geplant und insbesondere mögliche Auswirkungen von Änderungen über Systemgrenzen der ELGA-Systembetreiber hinweg im Vorfeld beurteilt werden.

8.2. Maßnahmenkataloge Informationssicherheit

LL02_M4 Um einen ausreichenden Schutz der ELGA zu erreichen, sind geeignete Maßnahmen zu treffen, die auf standardisierten Katalogen aufsetzen (z.B. BSI[5] Grundschutz, österreichisches Sicherheitshandbuch).

LL02_M5 Anpassungen sind gemäß den betrieblichen Erfordernissen in Abstimmung mit den ISMS-Beauftragten und dem ISMS-Koordinator zulässig.

[4] Information Technology *Infrastructure Library (ITIL)*
[5] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Deutschland)

8.3. Abstimmung mit verwandten Bereichen

LL02_M6 Da andere Bereiche wie Datenschutz, medizinische Register, Medizinprodukte, physikalischer Schutz usw. Einfluss auf die Informationssicherheit haben, sind die entsprechenden Nahtstellen zu identifizieren und in die Informationssicherheitsorganisation des eigenen Wirkungsbereiches einzubinden.

LL02_M7 Die Abstimmung mit diesen Bereichen obliegt dem l SMS-Beauftragten im jeweiligen Wirkungsbereich.

8.4. Notfallpläne und Wiederanlaufverfahren

LL02_M8 Notfallpläne müssen erstellt, erprobt und aktuell gehalten werden.

LL02_M9 Wiederanlaufverfahren und die Nichtverfügbarkeit von ELGA-Komponenten und definierten ELGA-Anwendungen sind zu üben.

LL02_M10 Die betroffenen und beteiligten Personen der ELGA GmbH und der ELGA-Systembetreiber sind diesbezüglich zu schulen.

9. Abkürzungen und Begriffe

Abkürzungen und Begriffserklärungen befinden sich im ELGA ISMS - Leitlinien-Glossar.

10. Abbildungsverzeichnis

11. Literaturverzeichnis

[1] KIRAS Sicherheitsforschung. *MASTERPLAN Österreichisches Programm zum Schutz Kritischer Infrastruktur (APCIP).* Available from: http://www.kiras.at/uploads/media/MRV_APCIP_Beilage_Masterplan_FINAL.pdf. Letzter Zugriff: Juli 2011

[2] European Commission. Smart *Open Services for European Patients - epSOS.* Available from: http://www.epsos.eu. Letzter Zugriff: Juli 2011

[3] European Commission. *Secure Identity Across Borders Linked - STORK.* Available from: https://www.eid-stork.eu/. Letzter Zugriff: Juli 2011.

[4] Computer Emergency Response Team Austria. *CERT.AT.* Available from http://www.cert.at/. Letzter Zugriff: Juli 2011.

[5] Österreichisches Normungsinstitut. *ISO/IEC 27001:2005 - Informationstechnologie -Sicherheitstechnik: Informationssicherheits-Managementsysteme - Anforderungen.* Wien, 2008.

[6] ON Österreichisches Normungsinstitut. *ISO/IEC 27002:2005 - Informationstechnologie — Sicherheitstechnik — Leitfaden für das Management der Informationssicherheit.* Wien, 2008.

[7] IT Governance Institute. *COBIT4.0,* 2005. Available from: http://www.isaca.at/index.php?option=com_docman&task=doc_download&gid=36&ltemid=60. Letzter Zugriff: Juli 2011.

Meine elektronische
Gesundheitsakte

ELGA GmbH

ELGA ISMS -

Generelle Vorgaben für die Netzwerk-sicherheit und Rechnerverwaltung

Leitlinie 006

Datum: 28.09.2011

Version: 2.0

Inhaltsverzeichnis

Es wird ausdrücklich darauf hingewiesen, dass alle personenbezogenen Bezeichnungen jeweils als geschlechtsneutral formuliert zu verstehen sind.

1. Präambel

Mit der fortschreitenden Vernetzung von ELGA steigen die Anforderungen an die Informationssicherheit. Diese Leitlinie umfasst alle Maßnahmen zur Planung, Durchführung, Überwachung der Rechner- und Netzwerkverwaltung, zur Abwehr von Angriffen und Wiederherstellung der Sicherheit.

Die Leitlinie für die Netzwerksicherheit und Rechnerverwaltung beinhaltet daher Vorgaben für technische und organisatorische Maßnahmen für ELGA [1].

2. Zielsetzung

Ziele dieser Leitlinie sind:

LL006_Z1 Der korrekte und sichere Betrieb von Rechner- und Netzwerkeinrichtungen ohne Beeinträchtigung durch Schadsoftware ist bei einer der Ausbaustufe und Nutzungsfrequenz von ELGA entsprechenden Verfügbarkeit gewährleistet.

LL006_Z2 Alle Systemänderungen unterliegen einem Change Management. Sie sind getestet, geprüft und dokumentiert und nur durch autorisierte Personen durchführbar.

LL006_Z3 Das Risiko von Systemfehlern und Systemausfällen ist durch Vorausplanung der notwendigen Kapazitäten auf ein Minimum reduziert.

LL006_Z4 Es stehen Backup- und Wiederanlaufverfahren bzw. andere geeignete Verfahren zur Verfügung, um allenfalls die Rechner- und Netzwerkfunktionalität wiederherzustellen.

LL006_Z5 Die Integrität und die Verfügbarkeit von Informationen und informationsverarbeitenden Einrichtungen sind sichergestellt.

LL006_Z6 Die Informationen sind vor missbräuchlicher Verwendung im Netzwerk geschützt und werden überwacht.

LL006_Z7 Die Sicherheit und die sichere Nutzung von ELGA sind gewährleistet.

LL006_Z8 Sicherheitsvorfälle werden erkannt, gemeldet, bearbeitet und behoben.

3. Geltungsbereiche

Diese Leitlinie dient der Sicherstellung des Betriebs von ELGA zur dauerhaften und nachhaltigen Unterstützung aller ELGA-Systembetreiber. Dies schließt die damit verbundene und eingesetzte Hardware, Software und Netzwerke ein.

Diese Leitlinie gilt für alle ELGA-Systembetreiber und deren Dienstleister.

Die Verantwortung für die Informationssicherheit verbleibt unbenommen der Regelungen dieser Leitlinie beim jeweiligen ELGA-Systembetreiber für die von ihm zu verantwortenden ELGA-Komponenten und ELGA-Anwendungen.

4. Maßnahmen

4.1. ELGA-Systembetreiber

LL006_M1 Der ELGA-Systembetreiber hat in seinem Wirkungsbereich auf mehreren Ebenen Maßnahmen zum Schutz vor Schadprogrammen und ähnlichen Bedrohungen wie z.B. Spam zu setzen oder setzen zu lassen.

LL006_M2 Für ELGA-Komponenten und ELGA-Anwendungen ist ein Sicherheitsmanagement für Netzwerke zu implementieren.

LL006_M3 Für ELGA-Komponenten und ELGA-Anwendungen sind die Betriebsverfahren zu dokumentieren.

LL006_M4 Änderungen an ELGA-Komponenten und ELGA-Anwendungen unterliegen Änderungskontrollverfahren.

LL006_M5 Aufgaben und Verantwortungsbereiche sind gemäß dem 4-Augen-Prinzip zu organisieren.

LL006_M6 Entwicklungs-, Test- und Produktivumgebungen sind zu trennen.

LL006_M7 ELGA-Systembetreiber haben die Umsetzung von Dienstleistungen durch Dritte zu überprüfen, die Einhaltungen der Vereinbarungen zu überwachen und Änderungen zu verwalten.

LL006_M8 Es sind Vorausplanungen und Vorbereitungen erforderlich, um die Verfügbarkeit adäquater Kapazitäten und Ressourcen für die Bereitstellung der geforderten Systemleistung sicherzustellen.

LL006_M9 Für neue ELGA-Komponenten oder ELGA-Anwendungen, Upgrades und neue Versionen sind Abnahmekriterien festzulegen. Während der Entwicklung und vor der Abnahme sind angemessene Systemtests durchzuführen.

LL006_M10 Zur Aufrechterhaltung der Integrität und Verfügbarkeit der ELGA sind Backupverfahren einzuführen, um Sicherungskopien von Daten zu erstellen bzw. eine Wiederherstellung des Systems zu ermöglichen.

LL006_M11 Datenströme über Netzwerke, die ELGA-Komponenten und ELGA-Anwendungen betreffen, sind einer sorgfältigen Überwachung zu unterziehen.

LL006_M12 Speziell zum Schutz von ELGA-Komponenten und ELGA-Anwendungen sind für die Nahtstellen oder Netzwerkübergänge entsprechende Verfahren zur Berechtigungs- und Zugriffskontrolle zu implementieren.

LL006_M13 Die Betreiber von ELGA-Komponenten und ELGA-Anwendungen haben geeignete Maßnahmen dahingehend zu ergreifen, dass der direkte Zugriff nur auf solche Daten ermöglicht wird, für deren Nutzung eine ausdrückliche Berechtigung besteht.

LL006_M14 ELGA-Komponenten und ELGA-Anwendungen sind durch definierte Sicherheitsgrenzen (z.B. Firewall) zu schützen. Zu diesen Maßnahmen gehören z.B. Verfahren für die Nutzung von Netzdiensten in Form von Einschränkung des Zugangs, Verfahren für das Management von Geräten für die Fernwartung, Netzwerkverbindungsregeln und Sicherheitslösungen für ein angemessenes Protokollierungs- und Überwachungsverfahren zur Meldung von unberechtigten Eindringversuchen bzw. für die Aufzeichnung von sicherheitsrelevanten Aktionen.

LL006_M15 Der ELGA-Systembetreiber hat im Interesse der Informationssicherheit die Wahrnehmung eines Vorfalls, welcher sich negativ auf die Funktionalität der gesamten ELGA auswirken kann, und seine Reaktion darauf, an den Sicherheitsbeauftragten zu melden. Dies hat zum Ziel, dass nachhaltige Auswirkungen von Fehlern auf ELGA minimiert bzw. verhindert werden.

LL006_M16 Der ELGA-Systembetreiber hat Datenträger (z.B. Bänder, Festplatten) sowie Systemdokumentationen vor unberechtigter Weitergabe, Änderung, Entfernung und Vernichtung zu schützen.

4.2. ELGA-Teilnehmer

LL006_M17 Die ELGA-Teilnehmer sind über Sicherheitsmethoden, die einen sicheren Umgang mit ELGA gewährleisten, aufzuklären.

5. Abkürzungen und Begriffe

Abkürzungen und Begriffserklärungen befinden sich im ELGA ISMS - Leitlinien-Glossar.

6. Literatur

[1] Österreichisches Normungsinstitut. ISO/IEC 27001:2005 - Informationstechnologie -Sicherheitstechnik: Informationssicherheits-Managementsysteme - Anforderungen. Wien, 2008.

Meine elektronische
Gesundheitsakte

ELGA GmbH

ELGA ISMS -

Systemzugriffsüberwachung und Zugriffskontrolle

Leitlinie 007

Datum: 28.09.2011

Version: 2.0

Inhaltsverzeichnis

Es wird ausdrücklich darauf hingewiesen, dass alle personenbezogenen Bezeichnungen jeweils als geschlechtsneutral formuliert zu verstehen sind.

1. Präambel

Diese Leitlinie dient der Festschreibung und Weiterentwicklung der allgemeinen Grundsätze und Aufgaben der ELGA-Systemzugriffsüberwachung und Zugriffskontrolle bei systemübergreifenden Tätigkeiten. Dies betrifft alle Komponenten auf denen ELGA betrieben wird. Diese Komponenten (Router, Switch, Gateway, DB-Rechner, Web-Rechner usw.) sowie die ELGA-Anwendungen müssen überwacht werden.

Die Vereinheitlichung der Vorgangsweise und Klarstellung der Aufgabenverteilung und Zuständigkeiten zwischen den ELGA-Systembetreibern werden geregelt.

2. Grundsätze

„Eine der wichtigsten Grundlagen der Informationssicherheit ist die Art und Weise, wie auf Ressourcen zugegriffen werden kann und wie diese Ressourcen durch die Zugriffsmechanismen geschützt werden." [3] Dabei spielen sowohl technische als auch organisatorische Maßnahmen eine entscheidende Rolle.

Die ELGA-Systemzugriffsüberwachung protokolliert alle Zugriffe auf Ressourcen von ELGA.

Die Zugriffskontrolle entscheidet, ob der Zugang zu einer bestimmten Ressource gewährt oder verwehrt wird. Das Ziel der Zugriffskontrolle ist die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Informationen unter dem Aspekt der Nachvollziehbarkeit.

3. Zielsetzung

LL007_Z1 Die Überwachung der Nutzung von ELGA ist gewährleistet.

LL007_Z2 Die Protokolle zur Systemzugriffsüberwachung und die Zugriffsprotokolle der ELGA-Anwendungen sind verlustfrei, unveränderbar und vor unbefugtem Zugriff geschützt vorhanden.

LL007_Z3 Die Protokollierung in ELGA ist zeitlich und über Organisationsgrenzen hinweg synchronisiert.

LL007_Z4 Die Protokollierung in ELGA ist über Organisationsgrenzen hinweg geregelt und kann Zugriffe zwischen ELGA-Systembetreibern aus verschiedenen Log-Dateien eindeutig zuordnen.

LL007_Z5 In ELGA sind Protokollierungen über Administrator- und Operatortätigkeiten eingerichtet und regelmäßig geprüft.

LL007_Z6 Ein ELGA-Teilnehmer kann alle ELGA-Zugriffe auf ihn betreffende Daten, organisationsübergreifend in geeigneter, transparenter Art abrufen.

LL007_Z7 Die Revisionsmöglichkeit der Protokollierung ist durch die ELGA ISMS-Organisation gegeben.

LL007_Z8 Die Systemzugriffsüberwachung und die Zugriffskontrolle sind durch Anweisungen und Standards hinsichtlich Protokollierung konkretisiert.

4. Geltungsbereich

Diese Leitlinie gilt für alle Organisationsbereiche von ELGA für Steuerung und Betrieb.

5. Maßnahmen

LL007_M1 Es sind Verfahren zur Überwachung der Nutzung von ELGA einzurichten. Daraus resultierende Protokolle und sonstige Ergebnisse der Überwachungen sind regelmäßig zu überprüfen.

LL007_M2 Es müssen gut strukturierte Ereignisprotokolle erstellt werden, in denen Benutzeraktivitäten, ungewöhnliche Ereignisse und Informationssicherheitsvorfälle festgehalten werden. Sie müssen für denselben Zeitraum wie Protokolldaten verwahrt werden, um bei zukünftigen Untersuchungen und Überwachungen der Zugriffskontrolle behilflich zu sein. Die automatische Auswertbarkeit muss zumindest 18 Monate gewährleistet sein.

LL007_M3 Beginn und Ende von Zugriffen (Verbindungsdaten) von personalisierten Systemadministratoren und Systemoperatoren auf ELGA sind zu protokollieren.

LL007_M4 Fehler sind zu protokollieren und zu analysieren und es sind entsprechende Maßnahmen zu ergreifen

LL007_M5 Protokollinformationen sind durch geeignete technische und organisatorische Verfahren vor unerlaubtem Zugriff, Verlust und Änderung zu schützen.

LL007_M6 Durch Vergabe einer eindeutigen, über die Organisationsgrenze hinaus geltenden Zugriffs-ID (z.B. Transaktionsnummer), können alle Zugriffe von

ELGA-Benutzern in den verschiedenen Log-Dateien der ELGA-Systembetreiber miteinander abgeglichen werden.

LL007_M7 Die Systemzeit in ELGA ist auf eine vereinbarte Referenzzeit zu synchronisieren.

LL007_M8 Der ISMS-Beauftragte hat in seinem Wirkungsbereich technisch oder organisatorisch sicherzustellen, dass die Systemzugriffsüberwachung korrekt durchgeführt wird.

LL007_M9 Regelmäßige Integrationstests stellen sicher, dass die Systemzugriffsprotokollierung standardkonform erfolgt und nicht deaktiviert wird. Speziell ist darauf im Rahmen des Change Management Prozesses Rücksicht zu nehmen.

6. Abkürzungen und Begriffe

Abkürzungen und Begriffserklärungen befinden sich im ELGA ISMS - Leitlinien-Glossar.

7. Literaturverzeichnis

[1] Österreichisches Normungsinstitut. ISO/IEC 27001:2005 - Informationstechnologie -Sicherheitstechnik: Informationssicherheits-Managementsysteme - Anforderungen. Wien, 2008.

[2] österreichisches Normungsinstitut. ISO/IEC 27002:2005 - Informationstechnologie — Sicherheitstechnik — Leitfaden für das Management der Informationssicherheit. Wien, 2008.

[3] Wikipedia, Stichwort "Zugriffskontrolle", Version vom 23. Juli 2011, Available from: http://de.wikipedia.org/w/index.php?title=Zugriffskontrolle&oldid=91592646. Letzter Zugriff: August 2011.

Meine elektronische
Gesundheitsakte

ELGA GmbH

ELGA ISMS -

Beschaffung, Entwicklung und Wartung von ELGA-Komponenten und ELGA-Anwendungen Leitlinie 008

Datum: 28.09.2011

Version: 2.0

Inhaltsverzeichnis

Es wird ausdrücklich darauf hingewiesen, dass alle personenbezogenen Bezeichnungen jeweils als geschlechtsneutral formuliert zu verstehen sind.

1. Präambel

Diese Leitlinie dient der Festschreibung und Weiterentwicklung der allgemeinen Grundsätze, Aufgaben und Ziele der Beschaffung, Entwicklung und Wartung von ELGA-Komponenten und ELGA-Anwendungen im systematischen Gesamtzusammenhang sowie der Vereinheitlichung der Vorgangsweise und Klarstellung der Aufgabenverteilung, Zuständigkeiten und Abläufe zwischen den kommunizierenden ELGA-Systembetreibern.

2. Grundsätze

Durch diese Leitlinie werden Vorgaben betreffend Beschaffung, Entwicklung und Wartung von ELGA-Komponenten und ELGA-Anwendungen festgelegt, die einerseits die Informationssicherheit erhöhen und andererseits gewährleisten, dass die Sicherheit der gesamten ELGA nicht gefährdet wird [1,2].

3. Zielsetzung

LL008_Z1 Die Sicherheit im Software-Entwicklungsprozess ist durch eine saubere Trennung von Entwicklungs-, Test- und Produktivumgebung gegeben. Weiters liegen dokumentierte Übergabeprozeduren vor.

LL008_Z2 Alle Sicherheitsanforderungen an ELGA-Komponenten und ELGA-Anwendungen sind vor deren Beschaffung, Entwicklung oder Implementierung identifiziert und nachweislich vereinbart.

LL008_Z3 Der Zugriff auf den Programm-Quellcode und auf Systemdateien ist nur Berechtigten möglich. Supportaktivitäten werden auf sichere Art und Weise durchgeführt.

LL008_Z4 Sensible Daten in Testumgebungen sind besonders geschützt.

4. Geltungsbereich

Diese Leitlinie gilt für alle ELGA-Systembetreiber.

5. Maßnahmen

LL008_M1 Im Zuge der Beschaffung bzw. Entwicklung neuer ELGA-Komponenten oder ELGA-Anwendungen oder deren Erweiterung sind Anforderungen an Sicherheitsmaßnahmen zu spezifizieren.

LL008_M2 Verarbeitungsfehler, die letztlich zu einem Integritätsverlust führen, sind durch Überprüfung des Designs und der Implementierung im Zuge eines dokumentierten Abnahmeverfahrens zu reduzieren.

LL008_M3 Daten, die in ELGA-Komponenten oder ELGA-Anwendungen eingegeben bzw. von diesen ausgegeben werden, sind zu validieren, um sicherzustellen, dass die Eingaben korrekt und passend sind sowie die Verarbeitung der gespeicherten Informationen korrekt erfolgt (Plausibilitätsprüfung).

LL008_M4 Test- und Systemtestdaten sind sorgfältig auszuwählen. Personenbezogene bzw. sensible Inhalte sind vor deren Verwendung möglichst zu entfernen oder unkenntlich zu machen.

LL008_M5 Testsysteme, die eine Verwendung personenbezogener oder anderer sensibler Informationen erforderlich machen, unterliegen den Sicherheitsrichtlinien des Produktivsystems mit Ausnahme der Vorgaben zu Integrität, Verfügbarkeit und Konsistenz.

LL008_M6 Der kompilierbare Programmquellcode der ELGA-Komponenten und ELGA-Anwendungen ist vom Produktivsystem getrennt zu halten. Zugriffsberechtigungen auf diesen sind strikt zu beschränken. Änderungen des Programmquellcodes der ELGA-Komponenten und ELGA-Anwendungen sind zu protokollieren, um missbräuchliche Veränderungen auszuschließen.

LL008_M7 Die Wartung und das Kopieren von Programmquellcode sind strengen Kontrollverfahren zu unterziehen und zu dokumentieren.

LL008_M8 Die Umsetzung von Änderungen hat mittels eines formalen Change Management Prozesses durchgeführt zu werden.

6. Abkürzungen und Begriffe

Abkürzungen und Begriffserklärungen befinden sich im ELGA ISMS - Leitlinien-Glossar.

7. Literaturverzeichnis

[1] Österreichisches Normungsinstitut. ISO/IEC 27001:2005 - Informationstechnologie -Sicherheitstechnik: Informationssicherheits-Managementsysteme - Anforderungen. Wien, 2008.

[2] Österreichisches Normungsinstitut. ISO/IEC 27002:2005 - Informationstechnologie — Sicherheitstechnik — Leitfaden für das Management der Informationssicherheit. Wien, 2008.

Meine elektronische
Gesundheitsakte

ELGA GmbH

ELGA ISMS

Leitlinien-Glossar

Datum: 28.09.20111

Version: 2.0

Inhaltsverzeichnis

Es wird ausdrücklich darauf hingewiesen, dass alle personenbezogenen Bezeichnungen jeweils als geschlechtsneutral formuliert zu verstehen sind.

1. Abkürzungen und Begriffe

Folgende Abkürzungen und Begriffe gelten für alle ELGA ISMS-Leitlinien.

Austrian Programme for Critical Infrastructure Protection	APCIP	Austrian Programme for Critical Infrastructure Protection. „Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden" [APCIP].
Betriebliches Kontinuitätsmanagement	BKM	ist ein krisensicheres IT-Konzept, das die Aufrechterhaltung aller Geschäftsaktivitäten im Ausnahmefall gewährleistet. Dazu gehört die IT-Sicherheit, die Informationssicherheit, das Risikomanagement, die Archivierung und das Disaster Recovery.
Bundesamt für Sicherheit in der Informationstechnik	BSI	Das BSI ist als zentraler II-Sicherheitsdienstleister des Bundes für die IT-Sicherheit in Deutschland verantwortlich [BSI].
Computer Emergency Response Team Austria	CERT.at	österreichisches nationales CERT. Ansprechpartnerfür IT-Sicherheit im nationalen Umfeld; vernetzt andere CERTs und CSIRTs (Computer Security Incident Response Teams) aus den Bereichen kritische Infrastruktur, Informations- und Kommunikationstechnik und gibt Warnungen und Tipps für kleine und mittlere Unternehmen heraus [CERT].
Control Objectives for Information and related Technology	COBIT	International anerkanntes Framework zur IT-Governance [COB].

Critical Information Infrastructure Protection	CUP	Bezeichnet den Schutz der Kritischen Informationsinfrastrukturen des Informations- und Kommunikationstechnologie-Sektors (IKT) und IKT-basierten Infrastrukturen anderer Sektoren.
Daten		sind Angaben über Betroffene im Sinne §4 Z.1 DSG, die elektronisch, schriftlich, bildlich oder akustisch zur Verfügung stehen. Sie werden in alphanumerische Daten, Biosignale, Bild- und Tonaufzeichnungen usw. unterschieden und können ermittelt, verarbeitet und überlassen werden.
Datenklassifikation		ist die Einstufung von Daten in Gruppen entsprechend ihrer Bedeutung und Vertraulichkeitsstufe. Anhand der Datenklassifikationen wird grundsätzlich der Schutzbedarf der einzelnen Daten und Informationen festgelegt. Die Klassifikationsstufen sind: a) frei zugängliche Daten; b) Daten, deren Missbrauch keine besondere Beeinträchtigung erwarten lässt; c) Daten, deren Missbrauch den Betroffenen in dessen gesellschaftlicher/wirtschaftlicher Stellung beeinträchtigen kann; d) Daten, deren Missbrauch Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen kann. Patientendaten sind zumindest der Stufe (c) zuzurechnen.
Disaster Recovery Plan	DRP	IT-Notfallplanung im Rahmen des betrieblichen Kontinuitätsmanagements
Document Producer		ELGA-Benutzer, der Daten in ELGA verfügbar

		macht.
Document Registry		Auflistung der Verweise auf Daten, die in ELGA abrufbar sind.
Elektronische Gesundheitsakte (in Österreich)	ELGA	ist ein Informationssystem, das sektorenübergreifend allen berechtigten ELGA-Gesundheitsdiensteanbietern und ELGA-Teilnehmern ELGA-Gesundheitsdaten im Sinne des §2 Z. 9 und 10 [ELGA-Gesetz] in elektronischer Form orts- und zeitunabhängig zur Verfügung stellt.
ELGA ISMS-Organisation		Gesamtheit der ELGA-Sicherheitskommission und der ELGA-Systembetreiber
ELGA-Sicherheitskommission		Beratung und Beschlussfassung bezüglich ISMS, Beschluss des Sicherheitsberichtes; die Kommission besteht aus: 1. Geschäftsführung der ELGA GmbH (Vorsitz) 2. ISMS-Koordinator 3. ISMS-Beauftragte der Betreiber zentraler und dezentraler ELGA-Komponenten 4. Auskunftspersonen/Sicherheitsexperten (optional)
ELGA-Systembetreiber		spezialisierter Provider für ELGA-Systemkomponenten, der im Sinne der Begriffsdefinition Betreiber lt. DSG § 50 ist.
ELGA-Anwendung	EANW	ist eine EDV-Anwendung aus dem eHealth-Bereich, die auf Daten, die über die ELGA verfügbar sind, zugreift oder Daten in ELGA bereitstellt. Beispiele: e-Medikation in der Österreichversion, Patientenverfügung.
ELGA-Benutzer		bezeichnet gesamthaft die verschiedenen Akteure wie ELGA-Teilnehmer, d.h. Bürger bzw.

		dessen Bevollmächtige und gesetzliche Vertreter, ELGA-Service-Mitarbeiter und ELGA-GDA als Person oder Organisation.
ELGA-Gesundheitsdienstea nbieter	ELGA-GDA	ELGA-Gesundheitsdiensteanbieter laut § 2 Z. 10 [ELGA-Gesetz] i.d.g.F., die in die Behandlung oder Betreuung eines ELGA-Teilnehmers eingebunden sind und die Voraussetzungen für die Teilnahme an ELGA erfüllen.
ELGA-Komponenten		Sind jene Komponenten und Services, aus denen sich ELGA zusammensetzt. Sie werden eingeteilt in „logisch" Zentrale Komponenten (Z-Pl, GDA-I, Berechtigungssystem, Protokollierung, Portal, Grundversorgungs-bereich) und dezentral zur Verfügung zu stellende Komponenten (ELGA-Bereiche mit ihren Gateways, ihrer Einbindung ins Berechtigungssystem und die Protokollierung, L-PI, Register, Repositories).
ELGA-Systempartner		umfasst Bund, Länder sowie den Hauptverband der österreichischen Sozialversicherungsträger (§2 Z. 11 [ELGA-Gesetz]).
ELGA-Teilnehmer		sind natürliche Personen laut §2 Z. 12 [ELGA-Gesetz] i.d.g.F., die die Teilnahmevoraussetzungen des § 15 erfüllen und für die daher elektronische Verweise auf sie betreffende ELGA-Gesundheitsdaten aufgenommen werden dürfen.
Gesundheitsdiensteanbieter	GDA	Anbieter von Gesundheitsdiensten im österreichischen Gesundheitssystem im Sinne der Begriffsdefinition lt. § 2 Z.2 ELGA-Gesetz i.d.g.F.

Information		Wissenszuwachs, der auf vielfältigem Wege gewonnen werden kann. Informationen sind vielfach aus Daten ableitbar.
Information Technology Infrastructure Library	ITIL	Sammlung von Best Practices, die eine mögliche Umsetzung eines IT-Service-Managements beschreiben [ITIL].
Informationssicherheits-Managementsystem	ISMS	Verfahren und Regeln innerhalb eines Unternehmens, mit dem Zweck, Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrecht zu erhalten und fortlaufend zu verbessern. ISO/IEC 27001 definiert ein ISMS.
International Standard Organisation	ISO	Internationale Vereinigung von Normungsorganisationen [ISO].
Key Performance Indikator	KPI	bezeichnet eine Messgrösse die im Vergleich zu Zielwerten den Grad der erwarteten Leistung anzeigt.
Plan-Do-Check-Act-Kreislauf	PDCA	Demingkreis nach Deming E.W. bzw. Shewhart W. A [PCDA].
Schutzbeauftragte		Die gemäß den gesetzlichen Vorgaben oder innerorganisatorisch ernannten Schutzbeauftragten (Arbeitnehmerschutz, Datenschutz, Gebäudeschutz usw.) unterstützen den GDA bzw. ernannte Sicherheitsbeauftragte bei der Bewältigung von fachspezifischen informationssicherheitsrelevanten Frage- und Problemstellungen.
Schützenswerte Informationen		sind Informationen, deren Missbrauch die Menschenwürde, die persönliche Integrität und Sicherheit sowie das Vermögen der Patienten,

		der Mitarbeiter, Vertragspartner und sonstiger Dritter, das Vermögen der ELGA GmbH, des Bundes und der Länder und die Wahrung von Geschäfts- und Betriebsgeheimnissen gefährdet.
Secure Identity Across Borders Linked	STORK	EU-Projekt, das es Bürgerinnen ermöglicht, mittels ihrer jeweiligen elektronischen Identität (z.B. der Bürgerkarte) Behördenerledigungen Online auch auf ausländischen Portalen zu tätigen [STORK].
Sicherheit		Bezeichnet die Verringerung oder weitestgehende Ausschaltung von Risiken und Gefahren. Die Sicherheit umfasst insbesondere die physische Sicherheit, die Datensicherheit, die Kommunikationssicherheit und die operationale Sicherheit.
Sicherheitsbewusstsein		ist das Erkennen, dass effektive Sicherheit ein kritisches und wesentliches Element der Unternehmensphilosophie ist.
Sicherheitsmanagement		ist die Gesamtheit aller zur Gewährleistung der Sicherheit eingerichteten organisatorischen Strukturen (Aufbau- und Ablauforganisation) und präventiven Maßnahmen. Präventive Maßnahmen gliedern sich in Maßnahmen für die Bereiche organisatorische Sicherheit, Zutrittssicherheit, IT-Sicherheit (Zugriff, Integrität, Betrieb), Katastrophenschutz, personellen Schutz sowie Kontinuitätsplanung und Ausfallschutz.
Sicherheitsrisiken		resultieren vor allem aus höherer Gewalt, organisatorischen Mängeln, menschlichen Fehlhandlungen (fahrlässig wie vorsätzlich) und/oder technischem Versagen. Sie können

		durch den Einsatz homogener Abläufe und Systeme entscheidend reduziert werden.
Sicherheitsrisikoanalyse		Sie bestimmt die wesentlichen Sicherheitsrisiken im Unternehmen bzw. in Projekten, definiert das zulässige Restrisiko und ist fester Bestandteil bei der Entwicklung und Einführung von Informationssystemen. Das Ergebnis liefert den erforderlichen Schutzbedarf.
Smart Open Services for European Patients	epSOS	EU-Projekt mit dem Ziel den Austausch grundlegender Patientendaten und elektronischer Verschreibungen zwischen Europäischen Gesundheitssystemen zu ermöglichen [EPS].
Standard-Sicherheitsmaßnahmen		Diese dienen der Grundsicherheit von Daten und Informationen. Zu ihrer effizienten Umsetzung sind für gleichartige organisatorische und/oder technische sicherheitsrelevante Problemstellungen zur Schaffung eines einheitlichen Sicherheitsniveaus einheitliche Mindeststandards erforderlich.

2. Literaturverzeichnis

[APCIP] Bundesamt für Sicherheit in der Informationstechnik (Deutschland). Definition Kritische Infrastrukturen, 2008. Available from: https://www.bsi.bund.de/DE/Themen/KritischeInfrastrukturen/EinfuehrungundUeberblick/KRITISDefinitionen/kritisdefinitionen_node.html. Letzter Zugriff: August 2011

[BSI] Bundesamt für Sicherheit in der Informationstechnik, 2011. Available from: https://www.bsi.bund.de/. Letzter Zugriff: August 2011.

[GERT] cert.at. Computer Emergency Response Team Austria, 2011. Available from: http://www.cert.at/. Letzter Zugriff: August 2011.

[COB] COBIT Framework for IT Governance and Control, 2011. Available from: http://www.isaca.org/. Letzter Zugriff: August 2011.

[EPS] European Commission. Smart Open Services for European Patients - epSOS. Available from: http://www.epsos.eu. Letzter Zugriff: Juli 2011

[ISO] International Organization for Standardization. Available from: http://www.iso.org/. Letzter Zugriff: August 2011

[ITIL] Information Technology Infrastructure Library. Available from: http://www.itil.org/. Letzter Zugriff: August 2011

[PCDA] Österreichisches Normungsinstitut. ISO/IEC 27001:2005 - Informationstechnologie -Sicherheitstechnik: Informationssicherheits-Managementsysteme -Anforderungen. Wien, 2008.

[STORK] European Commission. Secure Identity Across Borders Linked - STORK. Available from: https://www.eid-stork.eu/. Letzter Zugriff: Juli 2011.

[CUP] Bundesamt für Sicherheit in der Informationstechnik. Critical Information Infrastructure Protection, 2011. Available from: https://www.bsi.bund.de/ContentBSI/Themen/Kritis/Einfuehrung/KritisDefinitionen/definitionen.html. Letzter Zugriff: August 2011.