Amt für Informatik und Organisation

KANTON solothurn

Ritterquai 23
4509 Solothurn
Telefon 032 627 22 41
Telefax 032 627 22 18
www.so.ch

ISDS Konzept

Klassifizierung *	intern
Status **	In Arbeit / In Prüfung / Abgeschlossen
Projektname	Elektronisches Grundbuch Kanton Solothurn - Capitastra
Projektabkürzung	Capitastra
Auftraggeber	Finanzdepartement Kanton Solothurn
Autor	Christian Hirschi, Ivan Schmitter
Initiale	CH, IS
Bearbeitende	Christian Hirschi, Ivan Schmitter
Prüfende	Departementssekretariat, Fachgruppenleiter GB, Beauftragte für Information und Datenschutz, ASI, AIO, AGI
Genehmigende	Finanzdepartement, RRB … vom …

* Nicht klassifiziert, Intern, Vertraulich
** In Arbeit, In Prüfung, Abgeschlossen

Änderungskontrolle, Prüfung, Genehmigung

Version	Datum	Beschreibung, Bemerkung	Name oder Rolle
0.1	05.05.2015	Initiale Erstellung	Ch. Hirschi
0.2	22.12.2015	Entwurf zur Vernehmlassung an Beauftragte für Information und Datenschutz	Ch. Hirschi A. Klüser
0.3	01.09.2016	in Arbeit	Ch. Hirschi
0.4	28.10.2016	Antworten der Vernehmlassung eingearbeitet	Ch. Hirschi
1.0		Genehmigung mittels RRB	Regierungsrat

Definitionen, Akronyme und Abkürzungen

Begriff / Abkürzung	Bedeutung
AD	Active Directory
AIO	Amt für Informatik und Organisation
AJAX	Asynchronous JavaScript and XML
AV	Amtliche Vermessung
AVGBS	Amtliche Vermessung-Grundbuch Schnittstelle
CSV	Dateiformat (Comma-separated values)
DMS	Dokumentenmanagement-System

eGRISDM	eGRISDM ist ein Datenmodell, mit dem die Daten des Grundbuches beschrieben werden.
GB	Grundbuch
GBDBS	Grundbuchschnittstelle
GBDBS-Auskunft	Grundbuchschnittstelle für die Auskunft/Datenbezug
GBDBS-eGVT	Grundbuchschnittstelle für den elektronischen Geschäftsverkehr
GBDBS-Dateitransfer	Grundbuchschnittstelle Langzeitarchivierung
HTML	Hypertext Markup Language
HTTP/HTTPS	Hypertext Transfer Protocol / Hypertext Transfer Protocol Secure
Intercapi	Web-Applikation Capitastra (Standardlösung für Auskunft Grundbuchdaten)
IKS	Internes Kontrollsystem
ISDS	Informationssicherheits- und Datenschutzkonzepte
ISOV	Informations-System für Öffentliche Verwaltungen
JDBC	Java Database Connectivity
KASO	Katasterschätzung Solothurn
OCI	Oracle Call Interface
BeKo	Betriebskonzept
OS/ECM	Ablagearchiv für eingescannte Grundbuchbelege und Loseblätter
PDF	Portable Document Format (Dateiformat)
TXT	Textdatei
ULC	Ultra Light Client
URL	Uniform Resource Locator (Internetadresse)
WebStart	Protokoll zum Starten einer Java-Applikation aus dem Internet

Referenzen

Erkennungszeichen	Titel, Quelle
[1]	Informationssicherheit und Datenschutz (ISDS) Konzept ISOV GB V6
[2]	Schutzbedarfsanalyse (Version 0.2)
[3]	Risikoanalyse (Version 0.2)
[4]	Rollen- und Berechtigungskonzept Capitastra
[5]	Benutzerhandbuch Capitastra (in der aktuellen Version)

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Allgemeines

Das ISDS-Konzept gilt als Hauptdokument der Informationssicherheit und des Datenschutzes im Betrieb von Capitastra im Kt. SO. Vorgängig wurde eine Schutzbedarfsanalyse [2] und danach aufgrund des Bedarfs die Risikoanalyse erstellt. Die aus der Risikoanalyse [3] ermittelten Ergebnisse bilden die Grundlage für das vorliegende ISDS-Konzept. Mit der Einführung von Capitastra wurde am 25.06.2013 ein erstes ISDS-Konzept genehmigt, welches sich in erster Linie auf die Themen der Realisierung bezog. Dessen Inhalt wurde soweit notwendig in das vorliegende Konzept integriert.

2. Zweck des Dokuments

Das vorliegende Sicherheitskonzept beschreibt die sicherheitsrelevanten Aspekte des Betriebs von Capitastra inkl. des Abfrage-Tools Intercapi und des Auskunftsportals Terravis. Der Schwerpunkt der Betrachtung liegt auf

- der sicherheitsrelevanten Systembeschreibung
- den möglichen Bedrohungen (Gefahren)
- den Schwachstellen mit Auswirkungen auf Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit
- den Risiken des Systems
- den Sicherheitsvorkehrungen.

3. Zusammenfassung

Das vorliegende ISDS-Konzept konzentriert sich auf die Aspekte der Datensicherheit und des Datenschutzes, die im Kontext mit dem Betrieb von Capitastra im Kt. SO beachtet werden müssen. In Absprache mit dem AIO sind Sicherheitsbedürfnisse, die an ein Rechenzentrum gestellt werden, nicht Bestandteil des vorliegenden Sicherungskonzeptes. Die Standardlösung Capitastra für die Grundbuchführung ist vom Bund homologiert und wird in mehreren Kantonen (AG, BE, GE etc.) produktiv eingesetzt. Capitastra erfüllt demzufolge alle rechtlichen Anforderungen, welche an ein elektronisches Grundbuch gestellt werden. In der durchgeführten Risikoanalyse wurde deshalb insbesondere der organisatorische Risikobereich untersucht.

4. Sicherheitsrelevante Systembeschreibung

4.1. Ausgangslage, Vorleistungen

Im Rahmen des Erneuerungsprojektes ISOV GB 6 wurde im Jahr 2006 durch die IBM ein umfassendes ISDS-Konzept [1] erstellt.
Nach dem definitiven Scheitern des Projektes für eine Upgrade-Version von ISOV 5 nach ISOV 6 hat sich der Kanton Solothurn nach eingehender Analyse und Evaluation dafür entschieden, die Grundbuchführung mit ISOV durch die Standardlösung Capitastra 6 der Firma Bedag abzulösen. Die komplett erneuerte Version 6 von Capitastra ist heute erfolgreich in mehreren Kantonen produktiv im Einsatz.
Die alte Grundbuchlösung ISOV konnte Ende Oktober 2014 im Kt. Solothurn durch Capitastra abgelöst werden. Im Rahmen des Projektes wurde ein ISDS-Konzept für die Einführung von Capitastra erarbeitet. Dessen Inhalt wurde soweit notwendig und sinnvoll in das vorliegende Konzept integriert.
Mit dem neuen ISDS-Konzept werden alle Aspekte des Betriebes von Capitastra inkl. Intercapi und des Auskunftsportals Terravis berücksichtigt.
Voraussetzung für die Erstellung des vorliegenden ISDS-Konzeptes sind das Informations- und Datenschutzgesetz (vgl. Kapitel 11 [R3]) und die Informations- und Datenschutzverordnung (vgl. Kapitel 11 [R4]).

4.2. Homologierte Grundbuchanwendung Capitastra

Capitastra ist eine vom Bund homologierte Grundbuchanwendung und erfüllt alle rechtlichen Anforderungen für die Führung eines elektronischen Grundbuches:

- Grundbucheinträge, die mit Capitastra getätigt wurden, werden vom Verifikator nach erfolgreicher Prüfung des Geschäftes explizit als rechtlich verbindlich erklärt. Der Verifikator wird bei der Prüfung des Geschäfts durch Capitastra unterstützt. Mit den Geschäftsprüfungen werden die Vollständigkeit und die Korrektheit des Grundbucheintrags geprüft. Alle im Geschäft erledigten Eintragungen werden für die visuelle Verifikation auf einer Bildschirmmaske dargestellt.
- Sämtliche Eintragungen im Grundbuch werden protokolliert und sind nachvollziehbar. Von jeder Eintragung ist jederzeit feststellbar, welcher Benutzer sie zu welchem Zeitpunkt mit welchem Geschäft erstellt hat. Die Eintragungen werden historisiert.
- Durch die umfangreiche Berechtigungsverwaltung kann der Datenzugriff in Capitastra und Intercapi differenziert festgelegt werden. Sämtliche Abfragen über Intercapi werden protokolliert. Anhand dieses Zugriffsprotokolls kann festgestellt werden, ob sich ein Intercapi-Benutzer an die Nutzungsvereinbarungen hält oder nicht.

4.3. Systembeschrieb

Die nachfolgende Darstellung zeigt eine Übersicht des Gesamtsystems GBSO mit den wesentlichen Komponenten inklusive den internen und externen Schnittstellen. Jede Komponente und Schnittstelle ist mit einem eindeutigen Namen versehen. Die einzelnen Komponenten und Schnittstellen werden in den nachfolgenden beiden Kapiteln 4.3.1.1 und 4.3.1.2 ausführlich behandelt.

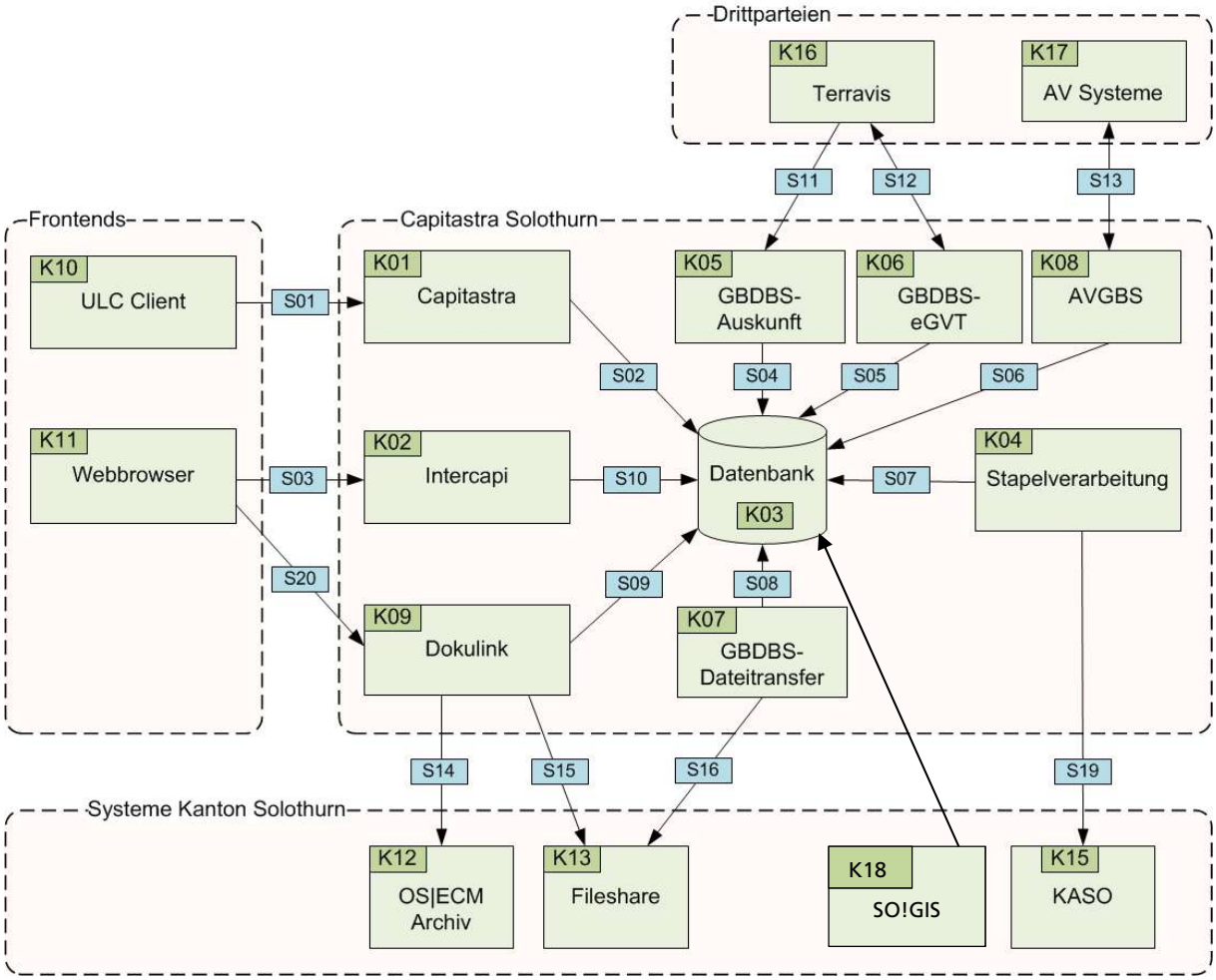

Abbildung 1: Systemübersicht

4.3.1.1. Komponenten

K01 Capitastra
Die Komponente K01 ist der Serverteil der Capitastra Grundbuchlösung. Über diese Komponente können Aufträge und Geschäfte erfasst und abgewickelt werden. Zudem können über diese Komponente Grundbuchabfragen durchgeführt werden.

K02 Intercapi
Intercapi ist das Internet-Auskunftssystem für Grundbuchdaten. Über Intercapi können rechtsgültige Daten inkl. Historie abgefragt und angezeigt werden. Intercapi generiert dabei HTML Seiten, welche von Webbrowsern angezeigt werden können.

K03 Capitastra Datenbank
Die Capitastra Datenbank speichert die Grundbuchdaten historisiert und revisionssicher ab. Die technischen Datenmodelle sind an das eGRISDM und AVGBS angelehnt. Zudem wurde das GBDBS Datenmodell berücksichtigt. Als Datenbankprodukt wird Oracle verwendet. In der Capitastra Datenbank werden die Grundbuchdaten revisionssicher und konsistent abgelegt. Jeder Zugriff auf Grundbuchdaten erfolgt im Rahmen einer Transaktion, welche entweder komplett festgeschrieben oder zurückgefahren (Prinzip ACID[1]) wird. Die Kombination aus transaktionsbasierten Datenzugriff in Verbindung mit der Oracle Datenbank, welche die Integrität des Datenmodells überwacht und sicherstellt, sorgt für den sicheren, langfristigen Betrieb der Grundbuchlösung.
Mutationen von Grundbuchdaten erfolgen im Capitastra Datenmodell immer im Kontext von Geschäften. Das Capitastra Datenmodell ist historisiert. Rechtsgültige Daten werden nie verändert, sondern im Kontext eines Geschäfts durch neuere Versionen ersetzt. Dabei wird nicht nur das aktuelle Geschäft für das Audit Logging verwendet, sondern auch der aktuell angemeldete Benutzer. Der Zugriff auf die historischen Daten ist über die Capitastra Frontends K10 und K11 jederzeit möglich.

K04 Stapelverarbeitung
Capitastra kann div. Auswertungen und Statistiken generieren. Zudem laufen mehrere Stapelverarbeitungen, wie z.B. die Schnittstellen S10 und S12. Da gerade Auswertungen sehr rechenintensiv sein können, werden diese in getrennten Prozessen gestartet. Dies ermöglicht die Entkopplung von Online- und Offlineverarbeitungen. Als Offlineverarbeitung zählt auch der In- oder Export von CSV oder TXT Dateien. Üblicherweise werden die Textdateien durch Benutzerinteraktion mit dem ULC Frontend der Stapelverarbeitung bekannt gemacht. Die eigentliche Verarbeitung erfolgt asynchron. Im Anschluss an die Verarbeitung wird ein Fehlerprotokoll ausgegeben.

K05 GBDBS-Auskunft
Über diese Schnittstelle werden Grundbuchdaten gemäss Vorgabe GBDBS zur Verfügung gestellt.

K06 GBDBS-eGVT
Die Schnittstelle dient für den elektronischen Geschäftsverkehr mit der Anwendung Terravis der Firma Six Group.

K07 GBDBS-Dateitransfer
Die Schnittstelle wird benötigt für den Export der Grundbuchdaten zur Langzeitarchivierung beim Bund.

K08 AVGBS
Diese Komponente stellt die Amtliche Vermessung-Grundbuch Schnittstelle zur Verfügung.

K09 Dokulink
Dokulink ist die Schnittstelle zwischen Capitastra und einem Dokumentenablagesystem, z. B. ein

[1] http://de.wikipedia.org/wiki/ACID

DMS oder ein einfaches Fileshare. Da Belege für rechtsgültige Daten auch über Intercapi angezeigt werden können, stellt Dokulink zusätzlichen Zugriffsschutz zur Verfügung. Dies verhindert, dass eine Dokumentenablage z. B. direkt aus dem Internet zugreifbar ist. Dokulink verhält sich ähnlich wie ein Proxy Server.[2]

K10 ULC Client
Der ULC Client ist der Client Teil der Capitastra Fachanwendung. Er wird via Java WebStart[3] auf die Client Arbeitsstationen oder Citrix Sessions verteilt und zeigt dort die Benutzerschnittstelle an. Der ULC Client ist ein Thin Client, er beinhaltet keine Geschäftslogik. Die Capitastra Gechäftslogik bleibt auf dem Applikationsserver, siehe Komponente K01. Der Capitastra ULC Client interagiert mit dem Microsoft Office Paket, um z. B. Grundbuchauszüge zu erstellen. Capitastra steuert Drucker nicht direkt an, sondern druckt Dokumente über Microsoft Word.

K11 Webbrowser
Ein Webbrowser dient zur Anzeige von HTML Seiten. Intercapi unterstützt als Browser Internet Explorer sowie Mozilla Firefox.

K12 Archiv / OS|ECM
Grundbuchdokumente werden manuell mit einem Multifunktionsprinter eingescannt und via Webtransfer in einem externen Dokumenten-Archiv als PDF Dateien abgelegt. Der Kanton Solothurn hosted sein Archiv bei Tessi document solutions GmbH (Produkt OS|ECM).

K13 Fileshare
Auf dem Fileshare werden Arbeitsdokumente zwischengespeichert, bevor diese in das Archiv übernommen werden.

K15 KASO
KASO steht für Katasterschätzung Solothurn. Von der KASO werden den Grundbuchämtern Gebäudeinformationen und Steuerwerte übermittelt.

K16 Terravis
Im Zuge des eGRIS Projektes wurde von der Firma SIX Group das System Terravis entwickelt. Terravis greift über die GBDBS Schnittstelle direkt auf die kantonalen Grundbuchsysteme zu. Terravis führt dabei entweder Abfragen durch (Teil GBDBS Auskunft) oder übermittelt Anmeldungen oder Aufträge (Teil elektronischer Geschäftsverkehr).

K17 AV Systeme
Bei den AV Systemen handelt es sich um Systeme der Geometer, welche sie bei der Durchführung der Vermessung unterstützen. Die AV Systeme kommunizieren über die AVGBS mit dem Grundbuch.

K18 SO!GIS
Amt für Geoinformation greift per View auf ausgewählte Grundbuchdaten (BFS, Nummer, Kreisnummer, Gemeindename, Grundstückart, Grundstück-Nr., Grundstück-Nr.-Zusatz, Grundstück-Nr.-3, Führungsart, Fläche, EGRID) zu. Die Daten werden benötigt für die Qualitätssicherung. Grundstücksdaten der amtlichen Vermessung und Grundbuch müssen identisch sein.

4.3.1.2. Schnittstellen

S01 Capitastra <-> ULC Client
Diese Schnittstelle basiert auf dem ULC Protokoll[4] und dient der Kommunikation zwischen Capitastra ULC Thin Client und dem Capitastra Applikationsserver. Neben dem ULC Protokoll wird zusätzlich das Java WebStart Protokoll für das Verteilen des Thin Clients eingesetzt. Beide Proto-

2 http://de.wikipedia.org/wiki/Proxy_(Rechnernetz)

3 http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136112.html

4 http://ulc.canoo.com/developerzone/technicalconcept.html

kolle basieren auf HTTP/HTTPS.

S02 Capitastra <-> Capitastra Datenbank
Für die Verbindung von Capitastra zur Capitastra Oracle Datenbank wird JDBC (Java Database Connectivity) eingesetzt, es wird der von Oracle zur Verfügung gestellte JDBC Typ 4 Treiber verwendet. Der JDBC Treiber selber baut über das OCI (Oracle Call Interface)[5] eine Netzwerkverbindung zur Datenbank auf.

S03 Webbrowser <-> Intercapi
Die Verbindung zwischen Webbrowser und Intercapi erfolgt über das HTTP Protokoll. Intercapi verwendet AJAX Requests, um die Geschwindigkeit des Seitenaufbaus zu erhöhen und die Benutzerfreundlichkeit zu Verbessern. Es wird kein WebSocket verwendet.

S04 GBDBS-Auskunft <-> Capitastra-DB
Diese Schnittstelle entspricht inhaltlich der Schnittstelle S02.

S05 GBDBS-eGVT <-> Capitastra-DB
Diese Schnittstelle entspricht inhaltlich der Schnittstelle S02.

S06 GBDBS-AVGBS <-> Capitastra-DB
Diese Schnittstelle entspricht inhaltlich der Schnittstelle S02.

S07 Stapelverarbeitung <-> Capitastra-DB
Diese Schnittstelle entspricht inhaltlich der Schnittstelle S02.

S08 GBDBS-Dateitransfer <-> Capitastra-DB
Diese Schnittstelle entspricht inhaltlich der Schnittstelle S02.

S09 DokuLink <-> Capitastra-DB
Diese Schnittstelle entspricht inhaltlich der Schnittstelle S02.

S10 Intercapi <-> Capitastra DB
Diese Schnittstelle entspricht inhaltlich der Schnittstelle S02.

S11 GBDBS-Auskunft <-> Terravis
Die Verbindung zwischen GBDBS und Terravis erfolgt für die Auskunft via WebServices. Die Kommunikation zwischen Terravis und Capitastra erfolgt über HTTPS in Verbindung mit Two-Way SSL[6].

S12 GBDBS-eGVT <-> Terravis
Die Verbindung zwischen GBDBS und Terravis erfolgt für den elektronischen Geschäftsverkehr via WebServices. Für den elektronischen Geschäftsverkehr wird ein WebService von Capitastra aufgerufen, um eine Anmeldung oder einen Auftrag zu übermitteln; zusätzlich ruft Capitastra WebServices auf Seite Terravis bei bestimmten Zustandsübergängen des jeweiligen Grundbuchgeschäfts auf. Die Kommunikation zwischen Terravis und Capitastra erfolgt über HTTPS in Verbindung mit Two-Way SSL.
Anmeldungen, welche via elektronischen Geschäftsverkehr übermittelt werden, können Dokumente als Anhang beinhalten, welche elektronisch mit einer vollqualifizierten Signatur versehen worden sind. Capitastra kann diese Signaturen mittels dem sog. Diskreten Validator[7] der Open eGov Plattform überprüfen. Der Einsatz des diskreten Validators ermöglicht es, dass keine vertraulichen Dokumente an Dritte übertragen werden.

S13 AVGBS <-> AV Systeme

5 http://www.oracle.com/technetwork/database/features/oci/index.html

6 http://publib.boulder.ibm.com/infocenter/tivihelp/v5r1/index.jsp?topic=%2Fcom.ibm.itim.infocenter.doc%2Fcpt%2Fcpt_ic_security_ssl_authent2way.html

7 https://www.e-service.admin.ch/wiki/display/openegovtopde/Diskreter+Validator

Die Nachführung von AV-Daten erfolgt durch den Austausch von XML-Daten über einen manuellen Webtransfer.

S14 Dokulink <-> OS/ECM Archiv
Der Zugriff von Dokulink auf Archivdaten erfolgt durch Aufruf einer URL. Zusätzlich werden noch Benutzername und Passwort des aktuell angemeldeten Benutzers mitgegeben.

S15 Dokulink <-> Fileshare
Dokulink könnte auch Dokumente zur Verfügung stellen, welche nicht im Archiv, sondern in einem anderen Ablageort liegen, z. B. ein Fileshare oder auch ein anderes Dokumentenmanagementsystem / externe Geschäftsverwaltung. Diese Schnittstelle ist noch nicht implementiert. Als mögliche Protokolle kann z. B. CMIS[8] für den Zugriff auf ein DMS oder ein einfacher Zugriff auf das lokale Dateisystem gewählt werden. CMIS basiert grundsätzlich auf WebServices und verwendet HTTP(S).

S16 GBDBS-Dateitransfer <-> Fileshare
Die Export-Datei mit den Daten für die Langzeitarchivierung wird auf einem Fileshare abgelegt.

S19 Stapelverarbeitung <-> KASO
Die Schnittstelle zwischen KASO und der Capitastra Stapelverarbeitung dient dem Importieren von KASO Daten in Capitastra. Die KASO Daten stehen in Form von Dateien auf dem lokalen Dateisystem zur Verfügung. Diese Dateien werden dann von der Stapelverarbeitung zu definierten Zeitpunkten in die Capitastra Datenbank importiert. Es erfolgt keine Rückmeldung an KASO.

S20 Webbrowser <-> Capitastra Dokulink
Intercapi generiert für den Zugriff auf Dokumente einen HTML Link zu einer URL, welche auf den Capitastra Dokulink Server zeigt. Neben der URL wird zusätzlich noch ein einmaliges Security Token mitgegeben. Anhand des Security Tokens kann der Dokulink Server feststellen, ob der Zugriff auf ein Dokument erlaubt ist. Der Zugriff des Webbrowsers auf Dokulink erfolgt ebenfalls via HTTPS.

4.4. Benutzer, Rollen und Rechte

In Capitastra werden Berechtigungen in Form von Rollen verwaltet. Eine Rolle kann individuell aus ca. 200 einzelnen, vordefinierten Rechten zusammengestellt werden. Einem Benutzer werden eine oder mehrere Rollen zugeteilt. Die Rechte des Benutzers ergeben sich aus der Summe aller Rechte aller Rollen, welche er innehat. Optional können Rollen auf organisatorische Einheiten eingeschränkt werden. Dadurch kann ein Benutzer pro Amt unterschiedliche Rollen einnehmen.
Capitastra kennt zwei Arten von Rollen: Capitastra-Rollen und Intercapi-Rollen. Da es sich bei den Benutzern von Capitastra bzw. Intercapi um einen anderen Benutzerkreis handelt, sind die verfügbaren Rechte differenziert aufgebaut.

Ferner kann über eine Zuordnung von organisatorischen Einheiten zu Rollen die Zugriffsberechtigung auf ein oder mehrere Grundbuchämter eingeschränkt werden. Zum Beispiel kann ein Benutzer auf zwei Ämtern Tagebucheinträge erstellen aber nur auf einem Amt Hauptbuchbearbeitungen durchführen. Im Intercapi besteht die Möglichkeit einer Einschränkung auf eine Region. Damit können nur Grundstücke innerhalb dieser Region aufgerufen werden.

Weitere Details sind im Benutzerhandbuch [5] von Capitastra enthalten.

4.5. Abgrenzung

Das vorliegende ISDS-Konzept beschränkt sich auf den Betrieb von Capitastra beinhaltend die Zugriffsberechtigungen von Personen mittels Capitastra und von Dritten via Intercapi oder Terravis auf die Grundbuchdaten sowie der Schnittstellen zu Umsystemen.
Die technische Wartung und der Support der Anwendung im AIO ist nicht Bestandteil des Konzepts. Die Datensicherheit und der Datenschutz innerhalb des AIO werden in einem eigenen

[8] http://en.wikipedia.org/wiki/Content_Management_Interoperability_ServiceS

Konzept dargestellt und erläutert. Die Sicherheitsbedürfnisse, welche in diesem Dokument nicht festgehalten werden, beziehen sich auf Teile der Schnittstelle GBDBS. Diese Bestandteile sind Gegenstand von späteren Einführungsprojekten. Folgende Komponenten sind demzufolge nicht Bestandteil des vorliegenden Sicherheitskonzeptes:

- K06 GBDBS-eGVT (elektronischer Geschäftsverkehr)
- K08 AVGBS
- K17 AV-Systeme

4.6. Ansprechpartner / Verantwortlichkeiten

Rolle	Name	OE, Firma	Hinweise
Inhaber der Datensammlung		Finanzdepartement	Datensammlung in den Umgebungen Produktion und Benutzertestumgebung
Systembetreiber		Amt für Informatik und Organisation	
Fachbereichsverantwortliche	C. Hirschi	Amtschreibereien	Leiter Amtschreibereien, Departementscontroller FD
Grundbuchaufsicht	Ph. Adam	Amtschreiberei-Inspektorat	Fachliche Aufsicht über das Grundbuch
Applikationsverantwortlicher	W. Stuppan D. Di Carlo	Amtschreibereien	Administratoren Capitastra / Intercapi
ISDS-Verantwortlicher	Ch. Kaiser	Betriebswirtschaftliche Dienste FD	Leiter BWD FD

Tabelle 1: Ansprechpartner / Verantwortlichkeiten

4.7. Datenschutz

4.7.1. Personendaten

Mit der Anwendung Capitastra kann für folgende Zwecke auf Personendaten zugegriffen werden:

- Aufruf von Eigentümerinformationen, Informationen von Berechtigten aus Dienstbarkeiten und Grundlasten, Vormerkungen, Anmerkungen, Informationen von Pfandrechtsgläubigern aus dem elektronischen Grundbuch.
- Erstellung von Verknüpfungen mit Stammpersonen aus der Personenverwaltung in Capitastra in verschiedenen Rollen (z.B. Veräusserer, Erwerber usw.) zum Auftragsmodul und als Anmelder zum Tagebucheintrag.
- Erstellen und Verknüpfen einer Stammperson aus der Personenverwaltung in Capitastra als Kontaktperson zu einem Grundstück (z.B. Verwalter einer Stockwerkeigentümergenossenschaft).

4.7.2. Benutzerkreis

Auf den Client von Capitastra hat nur ein sehr beschränkter Benutzerkreis Zugriff. Es sind dies fast ausschliesslich Benutzer aus den Amtschreibereien und dem Amtschreiberei-Inspektorat.

Zusätzlich haben Benutzer aus der kantonalen Verwaltung, von Gemeinden und Geometern mit Intercapi Zugriff auf die Grundbuchdaten für die Verwendung im Rahmen ihrer amtlichen Aufgaben.

Im Weiteren steht mit der alternativen Auskunftsplattform von Terravis externen Anspruchsgruppen wie Banken und Pensionskassen die Möglichkeit eines Grundbuchzugriffs zur Verfügung. In allen Fällen entscheidet das Finanzdepartement welchen Anspruchsgruppen ein Zugriff gewährt wird.

Benutzerkreis	Clienttyp	Authentisierungsangaben	Benutzerverzeichnis
Amtschreibereien	Capitastra-Client (für die Bearbeitung	BenutzerID und Passwort	AD Benutzerverwaltung

	der Grundbuchgeschäfte)		Capitastra (Rollen Capitastra)
Amtschreiberei-Inspektorat	Capitastra-Client (für das Abfragen von Grundbuch- und Geschäftsdaten)	BenutzerID und Passwort	AD Benutzerverwaltung Capitastra (Rollen Capitastra)
Gemeinden Kantonale Behörden	Intercapi (für Auskunft und Abfrage von Grundbuchdaten)	BenutzerID und Passwort	AD Benutzerverwaltung Capitastra (Rollen Intercapi)
Banken Rechtsanwälte Versicherungen Pensionskassen Bund	Terravis Auskunftsplattform	BenutzerID und Passwort	Vereinbarung über den Zugriff zwischen SIX Terravis AG und Berechtigten gestützt auf Benutzerrollen Terravis

Tabelle 2: Benutzerkreis und Client

4.8. Rechtsgrundlagen

Stufe	Titel
Strategie	ISB - IKT-Strategie der Bundesverwaltung 2012-2015
Leitbild	ISB - IKT-Sicherheitsleitbild der Bundesverwaltung
Verordnung	ISB - Bundesinformatikverordnung
Weisung	ISB - Weisungen des Bundesrates über die Informatiksicherheit in der Bundesverwaltung WIsB
Verordnung	SR 510.411 Informationsschutzverordnung (ISchV), Intranet
Gesetz	SR 235.1 Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG)
Verordnung	SR 235.11 Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG)
	SR 172.010.442 Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen
Gesetz	SR 152.1 Bundesgesetz vom 26. Juni 1998 über die Archivierung (Archivierungsgesetz, BGA)
Gesetz	SR 210 Schweizerisches Zivilgesetzbuch (ZGB)
Verordnung	SR 211.432.1 Grundbuchverordnung (GBV)
	SR 211.432.11 Technische Verordnung des EJPD und des VBS über das Grundbuch (TGBV)

Tabelle 3: Rechtsgrundlagen Bund

Stufe	Titel
Gesetz	BGS 114.1 Informations- und Datenschutzgesetz (InfoDG)
	BGS 211.1 Gesetz über die Einführung des Schweizerischen Zivilgesetzbuches (EG ZGB)
Verordnung	BGS 212.472 Kantonale Verordnung über die Führung des Grundbuches

Tabelle 4: Rechtsgrundlagen Kanton

Die amtliche Tätigkeit der Grundbuchämter und Vermessungsbüros ist im schweizerischen Zivilgesetzbuch Art. 942 ff ZGB umfassend geregelt. Die Verordnung betreffend dem Grundbuch (GBV) (SR 211.432.1) regelt im Detail, welche Daten erfasst und bearbeitet werden müssen und liefert die Grundlage für die alternative Datenplattform Terravis.
In der Verordnung des EJPD und des VBS (TGBV) (SR 211.432.11) sind die technische Anforderungen bezüglich den eidgenössisch standardisierten Schnittstellen und Datenmodellen z.B. GBDBS, etc. geregelt.

Weiter gelten die Regelungen im Einführungsgesetz zum schweizerischen Zivilgesetzbuch (EG ZGB) und die kantonale Verordnung über die Führung des Grundbuches (BGS 212.472).

4.9. Aufsicht und Controlling

Nach Art. 956 ZGB unterliegt die Geschäftsführung der Grundbuchämter der administrativen Aufsicht der Kantone und der Bund übt die Oberaufsicht aus. Die fachliche Aufsicht über die Grundbuchführung im Kanton Solothurn obliegt dem Amtschreiberei-Inspektorat, welches sich damit auch für die Aufsicht der SIX Terravis AG und deren Betreiben des Auskunftsportals Terravis verantwortlich zeichnet. Dazu wurde zusammen mit anderen Kantonen der Verein TerrAudit gegründet, welcher die interkantonale Koordination und Durchführung von Audits bei der SIX Terravis AG bezweckt. Der Verein beauftragt in der Regel eine nach Revisionsaufsichtsgesetz zugelassene Gesellschaft mit der Durchführung der Audits.
In Terravis können die getätigten Abfragen auch durch berechtigte Personen des Kantons Solothurn (Betriebswirtschaftliche Dienste FD und Amtschreiberei-Inspektorat) überwacht und geprüft werden.

4.10. Datenarchivierung und -vernichtung

Die Daten des Grundbuches müssen dauernd aufbewahrt werden. Grundsätzlich dürfen keine Grundbuchdaten physisch gelöscht und archiviert werden. Sind aufgrund von technischen Anforderungen Anpassungen an den Dateninhalten notwendig, liegt die Verantwortung beim Datenherrn, bzw. beim Auftraggeber der Mutationen. Solche Aufträge dürfen nur vom Applikationsverantwortlichen erteilt werden. Die Daten können aufgrund der dauernden Aufbewahrungspflicht höchstens verdichtet werden, müssen aber immer online während den Bürozeiten (Art. 14 GBV) zugreifbar sein. In Capitastra stehen die Grundbuchdaten grundsätzlich in nicht komprimierter Form online zur Verfügung. Mit der Schnittstelle GBDBS – Langzeitarchivierung werden die Daten periodisch einmal im Jahr an den Bund zur Aufbewahrung übermittelt.

4.11. Auskunft von Grundbuchdaten

Der öffentliche Zugang von Grundstückdaten an weitere Benutzerkreise (wie Gemeinden und Ämter) erfolgt grundsätzlich nur über das Auskunftssystem Intercapi bzw. über das Auskunftsportal Terravis der Firma Six Group (z.B. für Banken und Rechtsanwälte).

4.12. Berechtigungskonzept

Das Gesamtsystem Capitastra verfügt über ein Rollen- und Berechtigungskonzept [4], in dem sämtliche Zugriffsberechtigungen für Capitastra und Intercapi festgelegt sind. Ergänzt wird dieses Dokument mit den Rollen für Capitastra und Intercapi sowie je einer Zugriffsmatrix.
Das Finanzdepartement bewilligt im Einzelnen den Zugriff auf die Daten des informatisierten Grundbuchs im elektronischen Abrufverfahren und schliesst mit den Zugriffsberechtigten eine Vereinbarung ab (Art. 29 GBV; Art. 27 Verordnung über die Führung des Grundbuches).

4.13. Betriebskonzept

Das Betriebskonzept GBSO beschreibt die Integration des Gesamtsystems Capitastra in die Betriebsorganisation mit der Aufbauorganisation, den Betriebsprozessen sowie die organisatorischen Schnittstellen.

4.14. Einstufung

Die Angaben wurden aus der vorgenommenen Schutzbedarfsanalyse [2] entnommen.

Sicherheitsaspekt	Erhöhter Bedarf	Beschreibung
Vertraulichkeit nicht DSG/ISchV	Ja	Die amtliche Tätigkeit der Grundbuchämter ist im schweizerischen Zivilgesetzbuch Art. 942 ff ZGB umfassend geregelt. Die

Sicherheitsaspekt	Erhöhter Bedarf	Beschreibung
		Verordnung betreffend das Grundbuch (GBV, SR 211.432.1) regelt im Detail, welche Daten erfasst und bearbeitet werden müssen.
Vertraulichkeit nach DSG	Ja	Grundbuchpersonendaten (Eigentümer, Grundpfandgläubiger, Berechtigte aus Dienstbarkeiten / Grundlasten / Vormerkungen / Anmerkungen, Stammpersonen, Anmelder). Folgende Daten können öffentlich zugänglich gemacht werden (Art. 26, Abs. 1, Bst. a): Grundstücksbezeichnung und –beschreibung, Eigentümer, Eigentumsform und Erwerbsdatum.
Vertraulichkeit nach ISchV	Ja	Klassifikation INTERN. Daten/Informationen dürfen von unberechtigten Personen weder eingesehen noch verändert werden können. Folgende Daten können öffentlich zugänglich gemacht werden (Art. 26, Abs. 1 Bst. a GBV): Grundstücksbezeichnung und –beschreibung, Eigentümer, Eigentumsform und Erwerbsdatum.
Verfügbarkeit Betriebszeiten	Ja	Das System muss während den Bürozeiten online verfügbar sein.
Verfügbarkeit KaVor	Ja	An die Datensicherheit werden hohe Anforderungen gestellt (Art. 35 GBV). Das bestehende Notfallkonzept im AIO bildet die Grundlage für den sicheren Betrieb des Systems.
Integrität	Ja	Die Integrität und Authentizität der Grundbuchdaten muss jederzeit garantiert werden.
Nachvollziehbarkeit	Ja	Sämtliche Eintragungen im Grundbuch (Hauptbuch) müssen in der Fachanwendung nachvollziehbar sein oder anderweitig dokumentiert werden.

Tabelle 5: Einstufung

Datum der Einstufung	Beschreibung
22.05.2013	Die Einstufung wurde anlässlich von zwei durchgeführten Workshops mit den Vertretern des Kantons SO vorgenommen.
14.10.2016	Die Einstufung wurde durch Vertreter des Fachbereichs Grundbuch, des ASI, dem AIO und dem Finanzdepartement überprüft.

Tabelle 6: Einstufung Chronologie

5. Risikoanalyse

5.1. Grundlagen

- Siehe Risikoanalyse [3].
- Die Risikoanalyse wurde im Rahmen von Workshops mit den Fachvertretern und dem Team Betriebsorganisation Capitastra erstellt. Die technischen Risiken werden vom AIO in einem separaten Konzept dargestellt.
- Bei der Auswahl der Risiken wurde der Umstand berücksichtigt, dass bereits viele der darin aufgeführten Risiken durch übergeordnete Sicherheitskonzepte des AIO abgedeckt werden. Aufgrund dieser Ausgangslage wurde eine Selektion vorgenommen und dabei wurden drei Risiken aus der Gefährdungsgruppe „Organisatorische Mängel“, zwei Risiken aus der Gefährdungsgruppe „Menschliche Fehlhandlung“ und ein Risiko aus der Gefährdungsgruppe „Technisches Versagen“ identifiziert, bei denen Sicherheitsbedürfnisse bestehen und Massnahmen umgesetzt oder geprüft werden müssen.

5.2. Unmittelbarer Handlungsbedarf (Risikostufen 7-20)

Nr.	Gefährdungsgruppe	Risiko
G7	Organisatorische Mängel	Fehlende Kontrollen, Tests, Auswertungen
G9	Organisatorische Mängel	Fehlende Regelungen oder Prozess.
G10	Organisatorische Mängel	Mangelhaftes Management bei Änderungen
G15	Menschliche Fehlhandlung	Fehlverhalten Benutzer
G17	Menschliche Fehlhandlung	Nichtbeachtung Vorschriften
G21	Technisches Versagen	Softwareschwachstelle

Tabelle 7: Risiken (Unmittelbarer Handlungsbedarf)

5.3. Kein unmittelbarer Handlungsbedarf (Risikostufen 4-6)

Nr.	Gefährdungsgruppe	Risiko
G1	Höhere Gewalt	Personenausfall
G7	Organisatorische Mängel	Fehlende Kontrollen, Tests, Auswertungen
G9	Organisatorische Mängel	Fehlende Regelungen oder Prozess.
G10	Organisatorische Mängel	Mangelhaftes Management bei Änderungen
G11	Organisatorische Mängel	Prozess wird nicht gelebt oder Verstoss gegen gültige Regelungen.
G14	Menschliche Fehlhandlung	Fehlerhafte Administration
G15	Menschliche Fehlhandlung	Fehlverhalten Benutzer
G17	Menschliche Fehlhandlung	Nichtbeachtung Vorschriften
G21	Technisches Versagen	Softwareschwachstelle
G23	Vorsätzliche Handlungen	Abhören, Auswerten, Analysen, Hacken, Spoofing
G25	Vorsätzliche Handlungen	Gefälschte Daten Integritäts- und Vertraulichkeitsverlust
G26	Vorsätzliche Handlungen	Manipulieren, kompromittieren, vortäuschen
G27	Vorsätzliche Handlungen	Missbrauchen von Konten, Zutritten, Berechtigungen usw., Erpressen von Mitarbeitern
G28	Vorsätzliche Handlungen	Schwachstellen ausnutzen

Tabelle 8: Risiken (Kein unmittelbarer Handlungsbedarf)

6. Sicherheitsbedürfnisse

6.1. Grundlagen

Siehe Risikoanalyse, Reiter „Bedürfnis Massnahme Restrisiko“ [3].

6.1.1. Sicherheitsbedürfnis / Anforderung

Die nachfolgende Tabelle enthält die Sicherheitsbedürfnisse die mit den ausgewählten Risiken ermittelt wurden.

Nr.	Risiko	Sicherheitsbedürfnis
S1	G7	Sicherstellung Anforderung verbotene Serienabfragen (Art. 26 Ziff. 2 GBV).
S2	G9	Kontrollierte Vergabe der Zugriffsberechtigungen.

Nr.	Risiko	Sicherheitsbedürfnis
S3	G9	Entzug Zugriffsberechtigung bei Austritt eines externen Benutzers (Problem Austritt wird nicht gemeldet).
S4	G9	Die im QM publizierten Prozesse (Produktions- und Betriebsprozesse) sind aktuell und entsprechen dem definierten Ablauf.
S5	G10	Standardisierte Änderungsprozesse und -mechanismen.
S6	G15	Prozesse und Vorgaben sind verstanden, werden angewendet und eingehalten.
S7	G15	Laufende Überprüfung der Einhaltung von Schutzmassnahmen (Prozesse, organisatorische Regelungen).
S8	G17	Keine missbräuchliche Verwendung von Daten.
S9	G21	Keine betriebskritischen Fehler in der Produktion (Fehler bleiben unentdeckt, welche auf Seiteneffekte zurückzuführen sind).

Tabelle 9: Sicherheitsbedürfnis

7. Schutzmassnahmen

7.1. Grundlagen

- Siehe Risikoanalyse, Reiter „Bedürfnis Massnahme Restrisiko“ [3].

Risiken und Gefahren werden teilweise durch übergeordnete Sicherheitskonzepte oder SLA abgedeckt. Risikoanalysen wurden übergeordnet bereits gemacht. Folgende Liste soll zeigen welche übergeordnete Sicherheitskonzepte auf das Projekt wirken.

Konzept / SLA / Grundlage	Version	Freigabe-datum	Beschrieb des Schutzes
Min. Sicherheitsanforderungen gemäss WIsB		1.1.14	Genereller Grundschutz
Dokument "IKT-Grundschutz im Kanton Solothurn" (noch keine formelle Abnahme erfolgt).	0.9	Fehlt noch	Informations- und Kommunikationstechnik -

Tabelle 10: Restrisiken

7.2. Organisatorische Massnahmen zur Risikominimierung

In der nachfolgenden Tabelle sind die organisatorischen Schutzmassnahmen zur Abdeckung der Sicherheitsbedürfnisse für den Betrieb von Capitastra im Kt. SO beschrieben.

Nr.	Risiko	Massnahme	Bemerkung	Verantwortlich
M1	G7	Vertragliche Vereinbarungen zwischen Datenbezüger und Datenlieferant. Periodische Auswertung der Zugriffslogs. Die dafür notwendigen Regelungen sind im Betriebshandbuch festzulegen.	Jede Abfrage im Terravis und Intercapi (Web-Applikation) muss von Gesetzes wegen protokolliert werden.	ch
M2	G7	Im Parametrisierungskonzept sind sämtliche konfigurativen Einstellun-	Nicht nur die erstmalige Erstellung sondern auch die Nachführung auf-	ck

Nr.	Risiko	Massnahme	Bemerkung	Verantwortlich
		gen dokumentiert, welche das Applikationsverhalten steuern.	grund von Erweiterungen resp. Änderungen in der Parametrisierung durch neue SW-Releases muss sichergestellt werden. Die Regelungen sind ins Betriebshandbuch aufzunehmen.	
M3	G9	Die Überprüfung der Zugriffsberechtigungen ist im IKS aufzunehmen und periodisch zu verifizieren.	.	ck
M4	G9	Eine Auswertung zum Ermitteln von Benutzern, welche über längere Zeit kein Login in Intercapi vorgenommen haben (ev. automatische Deaktivierung). Im Betriebshandbuch ist ein Prozess zu konzipieren, welcher den Umgang mit ausgetretenen Benutzern beschreibt.	In der vertraglichen Vereinbarung muss geregelt werden, dass bei einem Austritt dies gemeldet wird.	ck
M5	G9	Die Prozesse werden periodisch auf ihre Aktualität hin überprüft. Bei Änderung von Abläufen werden die Prozesse grundsätzlich aktualisiert.		hf
M6	G10	Releasewechsel und Programmänderungen sind nach festgelegtem Ablauf in Zusammenarbeit mit dem AIO durchzuführen. Dieser Ablauf beinhaltet u.a. einen Softwaretest des Fachbereichs. Die Zuständigkeiten für Aufträge und Freigaben müssen klar festgelegt werden.	Die Nachvollziehbarkeit bei Änderungen muss entweder in Capitastra selber durch die Fachanwendung oder in einer Dokumentation ausserhalb von Capitastra sichergestellt sein.	
M7	G15	Das Vieraugen-Prinzip anwenden: - Grundbucheintrag = Verifikation durch Berechtigte	Das Vieraugen-Prinzip ist mit der Verifikation, welche in den Verordnungen definiert ist, sichergestellt.	
M8	G15	Schulung von neuen Mitarbeitenden.	Es werden sowohl Schulungen am Arbeitsplatz als auch zentral durch die Amtschreibereien durchgeführt.	
M9	G15	Die Anwendung der Prozesse wird jährlich anlässlich der QM-Kontrolle auf den AS überprüft.		
M10	G15	- Inspektionen durch ASI - QM-Kontrollen durch Qualitätsverantwortliche - IKS-Kontrolle durch BWD		
M11	G17	Schulung der Mitarbeitenden und Erlass von Weisungen, welche den Umgang mit Daten regeln.	Bei Grobfahrlässigkeit besteht die Möglichkeit der Sanktionierung.	
M12	G21	Neue Softwarekomponenten sind durch den Fachbereich auf die Einsatzfähigkeit und Fehler mittels Tests zu prüfen.	Tests werden auch von den anderen Kantonen, welche Capitastra einsetzen, durchgeführt.	

Tabelle 11: Organisatorische Schutzmassnahmen

Legende:
ch = C. Hirschi, ck = C. Kaiser, hf = H. Fontana

7.3. Technische Massnahme zur Risikominimierung

In der nachfolgenden Tabelle sind die technischen Schutzmassnahmen zur Abdeckung der Sicherheitsbedürfnisse für den Betrieb von Capitastra im Kt. SO beschrieben.

Nr.	Risiko	Massnahme	Bemerkung	Verantwortlich
M--	G--	…	…	…

Tabelle 12: Technische Schutzmassnahmen

8. Notfallkonzept

Im vorliegenden Sicherheitskonzept gehen wir davon aus, dass die übergeordnete Notfallplanung und die Katastrophenvorsorge im Betrieb AIO (Save/Restore, Gebäude usw.) sichergestellt werden.

9. Restrisiken

Gemäss Risikoanalyse bleiben Schwachstellen bestehen, die sich nicht vollständig bereinigen lassen.

Nr.	Wert	Verbleibendes Risiko	Weitergehende Massnahmen / Bemerkungen
RS-1		Das grösste Risiko sind die Mitarbeitenden, welche durch Fehlverhalten sensitive Daten oder Informationen an unberechtigte Dritte weitergeben oder Daten korrumpieren.	Schulung der Mitarbeitenden
RS-2		Mitarbeitende, welche durch Fehlmanipulation Daten ändern und die Integrität der Daten gefährden.	Schulung der Mitarbeitenden Prozessanleitungen erstellen und vermitteln
RS-3		Bei einem Softwarerelease wird die neue Version auf Fehler getestet. Es werden in erster Linie alle Neuerungen getestet, ein umfassender Gesamttest ist nicht möglich.	Der Softwarerelease wird an alle Capitastra-Kantone ausgeliefert und wird von denen getestet. Dieser Testumfang reduziert das Risiko eines unentdeckten Fehlers.

Tabelle 13: Restrisiken

10. Einhaltung / Überprüfung der Schutzmassnahmen

Die Sicherstellung für die Einhaltung der Schutzmassnahmen erfolgt durch die laufende Überprüfung mittels internen Kontrollsystems (IKS), durch die jährliche Prüfung der Qualitätssicherung und der periodischen Inspektion des Amtschreiberei-Inspektorates.

11. Verzeichnis der sicherheitsrelevanten Dokumente

Die nachfolgende Tabelle beinhaltet die Auflistung aller informationssicherheitsrelevanten Ge-

setze, Verordnungen, Weisungen, Regelungen etc.

Ref	Dokumenttyp	Titel
R1	Gesetz	Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992.
R2	Gesetz	Bundesgesetz über die Archivierung (Archivierungsgesetz, BGA) vom 26. Juni 1998
R3	Gesetz	Informations- und Datenschutzgesetz (InfoDG) vom 21. Februar 2001 des Kantons Solothurn.
R4	Verordnung	Informations- und Datenschutzverordnung (InfoDV) vom 10. Dezember 2001 des Kantons Solothurn.
R5	Gesetz	Schweizerisches Zivilgesetzbuch (ZGB) (SR 210).
R6	Verordnung	Grundbuchverordnung (GBV) (SR 211.432.1).
R7	Verordnung	Technische Verordnung des EJPD und des VBS über das Grundbuch (TGBV) (SR 211.432.11).
R8	Verordnung	Verordnung über die elektronische öffentliche Beurkundung (EÖBV) (SR 943.033).
R9	Gesetz	Einführungsgesetz zum schweizerischen Zivilgesetzbuch (EG ZGB; BGS 211.1).
R10	Verordnung	Verordnung über die Führung des Grundbuches (GBVo; BGS 212.472).
R11	Konzept	Betriebskonzept für die Organisation und die Rollen des Betriebes von Capitastra vom 16.10.2014
R12	Handbuch	Handbücher zur Bedingung von Capitastra und Intercapi ergänzt mit Anleitungen zur Abwicklung bei kantonsspezifischen Besonderheiten
R12	Workflow	QM-System der Amtschreibereien – Prozessbeschreibungen aller Produktionsprozesse im Intranet
R13	Konzept	IKS Amtschreibereien – Verzeichnis der Kontrollen innerhalb der Amtschreibereien
R14	Konzept	Prüfkonzept für die Auditierung der SIX Terravis AG und der Plattform Terravis – wird durch den Verein TerrAudit erarbeitet

Tabelle 14: Verzeichnis der sicherheitsrelevanten Dokumente

12. Liquidation

Die Daten des Grundbuches sind dauernd aufzubewahren und vor einer Ausserbetriebnahme des Systems muss sichergestellt werden, dass die Daten in lesbarer Form aufbewahrt werden oder in ein neues System überführt werden.