Frank, A. U. "Bemerkungen Zur Norm Datensicherung." 345-64. Zürich: Institut für Geodesie und Photogrammertrie, 1981.

Bemerkungen zur Norm Datensicherung

A. Frank

Institut für Geodäsie und Photogrammetrie, ETH-Hönggerberg, CH-8093 Zürich,
Separata No. 20

Bemerkungen zur Norm Datensicherung

A. Frank

Die Automationskommission des SVVK hat einen Entwurf zu einer Norm Datensicherung erarbeitet, der in diesem Heft publiziert wird.
Die diesem Entwurf zugrunde liegenden Vorstellungen werden im folgenden Aufsatz zusammengefasst. Dabei wird zuerst der Begriff Datensicherung eingeführt. Anschliessend werden einige rechtliche Aspekte der Verantwortung des Ingenieur-Geometers für die von ihm verwalteten Daten dargestellt. Das Konzept von ‹Gefahr – Massnahmen – Sicherheit›, das bei der Erarbeitung der Norm verwendet wurde, wird kurz erläutert, bevor schliesslich die grundlegenden EDV-Methoden zur Datensicherung besprochen werden.
Dieser Überblick soll dem Leser der Norm helfen, die Grundideen der Norm und den Zusammenhang der einzelnen Massnahmen leichter zu verstehen.

La commission d'automation de la SSMAF a développé un projet de norme pour la sécurité des données, qui est publié dans ce numéro. Les idées de base de ce projet sont rassemblées dans cet article. On introduit d'abord la notion de sécurité des données. Puis on présente quelques aspects juridiques de la responsabilité de l'ingénieur géomètre envers les données dont il a la charge. Le concept ‹danger – mesures – sécurité› qui a été utilisé lors de l'élaboration de la norme et les méthodes fondamentales pour garantir la sécurité des données sont également exposés.
Cet aperçu devrait permettre au lecteur de la norme de comprendre plus facilement les idées de base de la norme et la connexion des différentes mesures.

1. Grundlagen

Dieser Aufsatz ist als Einleitung und Kommentar zum nachfolgend publizierten ‹Entwurf zu einer Norm Datensicherung› der Automationskommission des SVVK gedacht.
Zuerst wird der Begriff ‹Datensicherung› eingeführt und die rechtliche Verantwortung des Geometers für die bei ihm gelagerten Daten diskutiert.
Danach wird im Überblick erläutert, welche Vorstellung von Sicherheit der Norm zugrunde liegt und mit welchen EDV-Methoden diese erreicht werden soll.
Damit soll der Normentwurf für den Leser verständlicher und seine Bedeutung leichter überblickbar werden.

1.1 Problemstellung

Heute werden in EDV-Systemen Informationen über viele verschiedene Sachverhalte gespeichert. Solche Daten sind meist von grundlegender Bedeutung für die geordnete Abwicklung von Tätigkeiten in Privatunternehmen und Verwaltung.
Auch im Geometerbüro und an den entsprechenden Stellen der Verwaltung werden mehr und mehr Daten der Grundbuchvermessung in EDV-Systemen gespeichert. In der Bundesrepublik Deutschland und in Österreich macht man sich daran, das Original-Grundbuch samt den zugehörigen Plänen statt auf Papier in einem Computer zu speichern. Auch in der Schweiz wird über solche Verfahren diskutiert (Friedrich 74) (Friedrich 80) (Frank 80) (ZBGR 80).
Wären solche Datenbestände plötzlich nicht mehr vorhanden, verfälscht oder unbrauchbar, so hätte das empfindliche Störungen zur Folge.
Die Wiederherstellung von Datenbeständen ist teuer und zeitraubend: Allein schon eine erneute Eingabe in den Computer verursacht grosse Kosten; häufig müssen die Daten aber aufgrund verschiedenster Unterlagen mit entsprechend grossem Aufwand rekonstruiert werden.
Es müssen somit Massnahmen ergriffen werden, um die Datenbestände vor Zerstörung oder Verfälschung zu schützen.

1.2 Abgrenzung Datensicherung – Datenschutz

Massnahmen der Datensicherung verhindern den Verlust oder die Verfälschung von Daten, wogegen Massnahmen des Datenschutzes die Daten gegen missbräuchliche Verwendung oder unerlaubte Veränderung sichern (Mutter 80) (Zehnder 78).
Die genaue Abgrenzung scheint oft schwierig, weil manchmal die gleichen Massnahmen die Daten sowohl gegen Verlust sichern als auch vor der missbräuchlichen Verwendung schützen.
Regeln für den Datenschutz müssen zuerst auf politisch-rechtlicher Ebene aufgestellt werden, bevor entsprechende technische Massnahmen zu deren Einhaltung festgelegt werden können.

1.3 Abgrenzung Datensicherung – Datenqualität (Validité des données) (Chevallier 81)

Gesammelte Daten sollten die erfassten Sachverhalte der Wirklichkeit richtig wiedergeben. Im Vermessungswesen sind vielfältige Vorkehrungen bei der Datenerfassung üblich, um diese Übereinstimmung zu erreichen und zu prüfen (z. B. überschüssige Beobachtungen mit anschliessender Ausgleichung). Entsprechende Regeln sind in den ‹Tabellen der Fehlergrenzen› oder in der ‹Instruktion für die Triangulation 4. Ordnung› detailliert aufgeführt. Bei der Verifikation wird kontrolliert, ob die dort vorgeschriebenen Ziele erreicht werden.
Von diesen Massnahmen, mit denen Datenqualität erreicht wird, sind die Massnahmen zu unterscheiden, die der Datensicherung dienen: Diese wollen nur sichere Aufbewahrung einmal erfasster Daten, ohne Rücksicht auf deren Qualität, erreichen.

1.4 Datensicherung – ein EDV-Problem?

Die Aufgabe der Datensicherung ist nicht mit der EDV-Anwendung entstanden; sie war schon immer wichtig. Bester Zeuge dafür ist die ‹Verordnung über die Grundbuchvermessung›, die in Art. 4 von den Kantonen verlangt, dass sie unter anderem auch Vorschriften über die Aufbewahrung der Grundbuchvermessungswerke erlassen. Ferner wurden in der ‹Weisung betreffend die Originalgrundbuchpläne auf Aluminiumtafeln› (samt zugehörigen Erläuterungen) schon 1929 detaillierte Massnahmen vorgeschrieben, die die Datensicherung bezwecken.
Anderseits ist klar, dass die Speicherung von Daten in Formen, die der Mensch nicht ohne Hilfsmittel lesen und verstehen kann, nach speziellen Vorschriften ruft. Bisher war es leicht, sich durch einen Augenschein von der sauberen und korrekten Darstellung von Vermessungsdaten in Plänen und Registern zu überzeugen. Die den Daten in konventioneller Form drohenden Gefahren, wie Brand, Wasserschäden usw., lassen sich anhand der gewöhnlichen Lebenserfahrung einschätzen und mit bekannten Verfahren abwehren (Stahl-

Institut für Geodäsie und Photogrammetrie, ETH-Hönggerberg, CH-8093 Zürich, Separata No. 20

schränke, Kopien etc.). Anders bei EDV-Daten: Eine Erfahrung darüber, welche Gefahren den Daten drohen, fehlt beim Anwender weitgehend. Daher können auch kaum zweckmässige Abwehrmassnahmen getroffen werden.

1.5 Anlass zur Norm

Nicht etwa weil Schäden bekanntgeworden sind, sondern um solche Schäden auch in Zukunft zu verhüten, ist von der Automationskommission des SVVK ein Entwurf zu einer Norm Datensicherung erarbeitet worden.
Sie soll dem Anwender, also vor allem dem Grundbuchgeometer, helfen,

- die Gefahren zu erkennen,
- die richtigen Massnahmen zu ergreifen und
- deren Durchführung zu kontrollieren.

2. Datensicherung – rechtliche Gesichtspunkte

Der Ingenieur-Geometer ist für die bei ihm gelagerten Daten verantwortlich. Werden diese aus irgendeinem Grund unbrauchbar oder gehen sie ganz oder teilweise verloren, so können vom Auftraggeber an ihn Schadenersatzansprüche gestellt werden. Diese Haftung des Geometers ist dabei von der Haftung des Staates für Schäden aus Fehlern aus der Grundbuchführung zu unterscheiden.
Die sichere Aufbewahrung der Daten – das heisst heute der Pläne und der zugehörigen Register – gehört im Normalfall zu den dem Nachführungsgeometer überbundenen Aufgaben, auch wenn sie im Vertrag nicht ausdrücklich erwähnt werden.
Der Nachführungsgeometer haftet damit seinem Auftraggeber für die getreue Ausführung (OR 398); das Mass der Sorgfaltspflicht richtet sich nach den Bestimmungen im Arbeitsvertrag (OR 321e): Er ist für absichtlichen oder fahrlässigen Schaden verantwortlich. Das Gesetz führt weiter aus: ‹Das Mass der Sorgfalt ... bestimmt sich nach dem einzelnen Arbeitsverhältnis, unter Berücksichtigung des Berufsrisikos, des Bildungsgrades oder der Fachkenntnisse, die zu der Arbeit verlangt werden ...› Die Anforderungen an die Sorgfaltspflicht dürften für den eidgenössisch patentierten Ingenieur-Geometer als Fachmann hoch sein (BGE 92 II 240).
Besitzt er in einem speziellen Fall die notwendigen Spezialkenntnisse nicht selbst, so muss er sich bei Spezialisten erkundigen und deren Ratschlägen folgen (BGE 93 II 21, BGE 93 II 313).
Der Berufsmann muss sich somit so verhalten, wie es den *Regeln der Kunst* entspricht und normalerweise zum erwarteten Ergebnis führt (BGE 93 II 313).
Die Regeln der Kunst bestehen im gesicherten Wissen eines Fachgebietes, wie es in Lehrbüchern niedergelegt ist. In gewissen Bereichen, insbesondere im Bauwesen, wurden diese Regeln in leicht anwendbarer Form in Normen zusammengefasst.
Sind solche Normen von einer anerkannten, integren und kompetenten Organisation herausgegeben und werden sie ständig dem aktuellen Fachwissen angepasst, so schafft ihre Anwendung zunächst die Vermutung, dass der Verantwortliche sich technisch richtig verhalten habe und die gültigen Regeln seines Fachgebietes anwende (Fischer 80). Der Bestreitende, im allgemeinen der Geschädigte, muss nun zeigen, dass die Norm überholt oder ungenügend ist oder allenfalls deren falsche Anwendung nachweisen.
Wird eine anerkannte technische Norm fahrlässig – und dazu gehört beim Fachmann auch die Unkenntnis der Norm – oder bewusst nicht angewendet, so entsteht daraus die Vermutung, dass er nicht den Regeln der Kunst entsprechend gehandelt habe. Er kann allenfalls beweisen, dass ein anderes, ebenso taugliches Verhalten angewendet wurde, oder aber die Untauglichkeit der Norm im konkreten Fall nachweisen.

(Fischer 80) fasst wie folgt zusammen:

> ‹Die Anwendung der Normen ist zwar nicht befohlen, aber geboten. Ihre Nichtbeachtung kann Nachteile zeitigen.›

Zu beachten ist weiter, dass der Ingenieur-Geometer auch für Schäden einstehen muss, die seine Angestellten verursachen (OR 101). Er muss also nicht nur selber die Norm anwenden, sondern auch dafür sorgen, dass seine Angestellten diese beachten.

3. Sicherheitskonzept

Die Norm Datensicherung will Sicherheit der Daten erreichen. Ihr liegen bestimmte Vorstellungen von *Sicherheit der Daten, Gefahren,* welche diese Sicherheit bedrohen, und *Massnahmen* gegen diese Gefahren zugrunde; diese Vorstellungen werden unter dem Begriff Sicherheitskonzept zusammengefasst (Schneider 80).

3.1 Sicherheit

Nach Brockhaus ist Sicherheit ‹objektiv das Nichtvorhandensein von Gefahren, subjektiv die Gewissheit des Einzelnen, einer Gruppe oder eines Staates, vor möglichen Gefahren geschützt zu sein›.
Dem Normenwerk des SIA liegt die Vermeidung von Schädigung von Personen an Leib und Leben zugrunde. Solche Schäden müssen grundsätzlich vermieden werden, auch wenn keine vollständige Sicherheit erreicht werden kann (Entwurf SIA 260, Ziffer 1.2 al. 1, Ziffer 1.3 al. 4).
Im Unterschied dazu steht die Norm Datensicherung. Mit dieser Norm soll Sicherheit der Daten der amtlichen Vermessung vor Zerstörung und Verfälschung erreicht werden. Personenschäden, die sich aus dem Verlust von Daten des Grundbuches ergeben, sind zum Glück kaum vorstellbar. Dennoch kann die Sicherung der Daten der Grundbuchvermessung nicht allein nach wirtschaftlichen Überlegungen des Geometers erfolgen. Die Allgemeinheit als Auftraggeberin der Vermessungswerke hat einen Anspruch auf eine funktionierende Grundbuchvermessung.

3.2 Sicherheit im Sinne der Norm

‹Sicherheit einer Gefahr gegenüber› besteht dann, wenn die Gefahr durch geeignete Massnahmen eliminiert ist. In Fällen, wo dies nicht umfassend möglich ist, kann im Sinne dieser Weisung eine Situation als sicher bezeichnet werden, in der das verbleibende Risiko auf akzeptierbar kleine Werte beschränkt bleibt (Entwurf SIA 260, Ziffer 2.11 al. 1).

3.3 Gefahren, Gefährdungsbilder

Bevor Massnahmen zur Datensicherung ergriffen werden können, müssen die Gefahren, die die Daten bedrohen, erkannt werden. Drei Gruppen können sofort unterschieden werden:

- Verlust der Daten durch Zerstörung der Datenträger
- Zerstörung oder Verfälschung der Daten durch fehlerhafte Verarbeitung
- Unzugänglichkeit der Daten durch Ausfall der Zugriffsmechanismen.

Durch weitere Unterteilung werden schliesslich die konkreten einzelnen Gefahren gefunden (z. B. Zerstörung der Daten durch Brand im Büro des Geometers).
Neben diesen erkannten Gefahren können noch andere Gefahren bestehen: solche, die vergessen wurden, und solche, die objektiv noch nicht bekannt sind.
Jede Gefahr kann auch kombiniert mit andern Gefahren auftreten. Erfahrungsgemäss ist gerade der Schutz gegen Gefahrenkombinationen wichtig. Grosse Schäden entstehen vor allem dann, wenn nach einem ersten (gesicherten) Schaden ein zweites schädigendes Ereignis eintritt. Dazu ein abschreckendes Beispiel:

> Wegen Abwesenheit des Verantwortlichen führt der ungenügend ausgebildete Stellvertreter, nachdem die Originaldaten wegen eines Hardware-Fehlers verloren gegangen sind, eine Wiederherstellung der Daten mit Hilfe der Sicherheitskopien durch. Wegen einer Fehlmanipulation gehen auch diese verloren.

Solche Fälle werden im allgemeinen ‹Verkettung unglücklicher Zufälle› genannt. Konkrete Gefährdungsbilder beschreiben möglicherweise gemeinsam auftretende Gefahren. In Ziffer 6.4 der Norm sind die zu berücksichtigenden Gefahrenkombinationen beschrieben.

3.4 Massnahmen

Verschiedene Massnahmen können und müssen ergriffen werden, damit die Daten vor Verlust gesichert sind.
Im Unterschied zu den Normen im Bauwesen, insbesondere zu denjenigen für die Bemessung von Tragwerken, fehlen modellhafte Vorstellungen über die Funktion und die Zuverlässigkeit von EDV-Anlagen heute noch. Anstelle der rechnerischen Bemessung müssen deshalb Erfahrungswerte über die Wahrscheinlichkeit von Fehlern und die Wirkungsweise von Massnahmen treten. Dies ist kein wesentlicher Mangel, der eine Normierung behindert, da rechnerisch nicht erfassbare menschliche Schwächen ohnehin die wichtigste Gefahrenquelle darstellen.

Die Massnahmen können aufgeteilt werden in

- Massnahmen gegen technisches Versagen oder äussere Einwirkungen
- Massnahmen gegen fehlerhafte Handlungen der Beteiligten
  - Festlegung der Abläufe
  - Festlegung der Kompetenzen
  - Festlegung von Kontrollen.

3.5 Bestimmung der zu erreichenden Sicherheit

Die Norm legt fest, welches Mass an Sicherheit erreicht werden muss. Damit ist auch bestimmt, welches Risiko akzeptiert werden darf (weitere Massnahmen sind selbstverständlich zulässig!).
Weil die Massnahmen nicht auf ein formales Modell abgestützt werden können, ist es auch nicht möglich, formale Sicherheitsfaktoren anzugeben. Das Sicherheitsziel ist vielmehr durch die Bestimmung der zu treffenden Massnahmen fixiert.
Wie in andern Normen, ist auch bei der Datensicherung ein Abweichen von den Vorschriften der Norm zulässig, sofern der Nachweis erbracht wird, dass das Sicherheitsziel erreicht wird. Das heisst konkret, es muss gezeigt werden, dass die gewählten Massnahmen gegen die gleichen Gefahren die gleiche oder höhere Sicherheit bieten als die vorgeschriebenen.

4. Geltungsbereich der Norm

Die Norm ist auf die Datenverarbeitung im Geometerbüro mit kleineren EDV-Anlagen zugeschnitten; für die Verarbeitung von Daten der amtlichen Vermessung in Rechenzentren ist sie sinngemäss anzuwenden.
Die Norm bezieht deshalb in verschiedenen Punkten Leistungen Dritter ein; der verantwortliche Geometer hat diese sorgfältig auszuwählen und auf die entsprechenden Bestimmungen der Norm aufmerksam zu machen und, soweit ihm das möglich ist, deren Einhaltung zu kontrollieren.

5. Grundkonzepte der Datensicherung

Datenbestände sind grundsätzlich von zwei Gefahrentypen bedroht:

- der ganze Datenbestand (oder zumindest grosse Teile davon) geht auf einmal verloren, sei es, dass die aufgezeichneten Daten verlorengehen, sei es, dass die Zugriffsmechanismen unbrauchbar sind;
- einzelne Datenelemente werden bei der Verarbeitung verfälscht, und der Datenbestand wird so im Laufe der Zeit unbrauchbar.

5.1 Verlust des ganzen Datenbestandes

Die einfachste Massnahme, um sich vor dem Verlust der Daten (ob mit EDV gespeichert oder nicht) zu schützen, ist die Herstellung einer Kopie und deren Aufbewahrung an einem sicheren Ort.
Bei der Auswahl des Aufbewahrungsortes der Kopie muss man vor allem darauf achten, dass Original und Kopie nicht gleichzeitig vom gleichen Ereignis zerstört werden können.
Handelt es sich um Daten auf EDV-Datenträgern, so müssen einige Details besonders beachtet werden:

- Generell kann nicht von Auge festgestellt werden, ob die gespeicherten Daten noch vollständig vorhanden sind; erhöhte Vorsicht ist also geboten.
- EDV-Datenträger stellen im Verhältnis zu schriftlichen Aufzeichnungen höhere Anforderungen an die Lagerungsbedingungen (Temperatur, Luftfeuchtigkeit etc.).
- Daten auf magnetischen Datenträgern können relativ rasch (wenige Jahre) ‹verblassen›; sie müssen durch regelmässiges Kopieren aufgefrischt werden.
- Neben den eigentlichen Daten ist auch an die Programme und Anlagen zu denken, die zum Lesen der Daten erforderlich sind: von den Programmen und ihrer Dokumentation müssen ebenfalls Kopien erstellt werden. Es ist zu überlegen, wo allenfalls ein Ersatz für die Anlagen zu finden wäre.

Weil an der amtlichen Vermessung verschiedene Stellen beteiligt sind, ist es notwendig, dass mindestens eine Kopie der Daten so erstellt wird, dass sie auch von andern Anlagen gelesen und interpretiert werden kann. Das bedingt, dass die Aufzeichnung auf einem Datenträger und nach einem Verfahren erfolgt, das standardisiert ist und die Übertragung auf eine andere Anlage ermöglicht (z. B. Magnetbänder, z. T. auch Disketten). Die Daten müssen auf der fremden Anlage aber auch interpretiert werden können. Dies erfordert, dass die Darstellung der Informationen nach einheitlichen, gut dokumentierten Grundsätzen erfolgt. Beispielsweise sind mehrere unterschiedliche Methoden bekannt, um Parzellengrenzen zu speichern. Es scheint eine dringliche Aufgabe des SVVK, für diese Fragen Normen auszuarbeiten.
Leider genügt die Aufbewahrung einer Kopie der Daten allein nicht, um Verluste vollständig zu verhüten: Die Originaldaten werden laufend durch Nachführungsarbeiten verändert, wogegen die Kopie unverändert bleibt. Geht das Original verloren, so gehen damit auch die Veränderungen verloren, denn diese sind in der Kopie nicht enthalten. Man muss also dafür sorgen, dass gesonderte Aufzeichnungen (automatisch oder manuell) über alle Änderungen erstellt werden und dass damit die Kopie auf den neusten Stand nachgeführt werden kann.
Den Rhythmus des Kopierens kann man folgendermassen bestimmen: Die Kosten des Kopierens müssen kleiner sein als der wahrscheinliche Schaden.

$$K(\text{Kopieren}) < K(\text{Nachführen}) \cdot p$$

K (Kopieren): Kosten der Erstellung der Kopie
K (Nachführen): Kosten der Nachführung der Kopie auf den neuesten Stand
p: Wahrscheinlichkeit des Verlustes der Daten

5.2 Verfälschung einzelner Datenelemente bei der Verarbeitung

Die Daten der amtlichen Vermessung müssen langfristig verwendbar sein. Werden bei der Verarbeitung, ob mit EDV oder manuell, Fehler in den Datenbestand hineingetragen, so wird im Laufe der Zeit der Datenbestand unbrauchbar. Solche Fehler sind besonders gefährlich, weil es sehr lange dauern kann, bis sie entdeckt werden, und ihre Korrektur dann ausserordentlich kostspielig ist.
Schon bisher sind bei der Arbeit mit Daten der amtlichen Vermessung sehr hohe Anforderungen an die Kontrollen gegen allfällige Fehler gestellt worden:

- Kontrollmasse
- Kontrolle der Flächeninhalte
- Verifikation von Mutationen
  etc.

Ebenso hohe Anforderungen müssen an die Datenverarbeitung gestellt wer-

den. Die Prüfung der EDV-Verarbeitung kann auf zwei Arten erfolgen:

- ‹um die EDV herum›, d. h. es werden stichprobenweise Einzelfälle nachgerechnet und geprüft, ob die berechneten Ergebnisse korrekt sind. Diese Prüfung geschieht ohne Berücksichtigung der speziellen Eigenschaften von EDV-Arbeiten, gleich wie bei manueller Verarbeitung,
- ‹mit der EDV›, d. h. es wird anhand der Programme sichergestellt, dass die Verarbeitung in jedem Fall korrekt ist.

Bei der Prüfung ‹mit der EDV› nützt man den Unterschied zwischen manueller und automatischer Verarbeitung aus: Der Mensch macht ‹ab und zu› einen Fehler. Führt er genügend Kontrollen korrekt durch, so kann er diese Fehler erkennen. Ein EDV-Programm arbeitet immer gleich; ist ein bestimmter Fall richtig/falsch programmiert, so wird er immer richtig/falsch ausgeführt. Es ist also viel rationeller, das Programm zu prüfen, als zu hoffen, dass der falsch programmierte Fall durch die Stichprobe erfasst werde.

Eine Prüfung von Programmen ist leider keine einfache Sache. Für kleine Programme stehen heute Methoden bereit, ihre Korrektheit nachzuweisen; grosse Programme können nur getestet werden. Aber auch ausführliche und gut zusammengestellte Tests können nicht die Korrektheit eines Programmes zeigen. Tests können uns nur helfen, Fehler in Programmen zu finden, nicht aber die Abwesenheit von Fehlern beweisen.

Ein Schritt, um die Prüfung von Programen zu erleichtern, ist deren Aufteilung in einzelne Teile, die gesondert untersucht werden können. Betrachten wir die verschiedenen Teile eines Programmsystems für die amtliche Vermessung, so sind unter dem Gesichtspunkt der Datensicherung nur wenige Teile relevant: Es sind diejenigen, die die gespeicherten Daten verändern. Programme, die die gespeicherten Daten lediglich verarbeiten, sind vom Standpunkt der Datensicherung aus ungefährlich, aber nicht hinsichtlich des Datenschutzes. Die eigentlichen Verarbeitungs- und Berechnungsprogramme, die von der Datenspeicherung abgetrennt werden sollten, sind ebenfalls ungefährlich für die Datensicherheit (sie sind aber unter dem Gesichtspunkt der Datenqualität genau zu prüfen).

Das führt zum Konzept, dass die Verarbeitungsprogramme alle Daten, die eine Änderung betreffen, vorbereiten und nachher diese Daten den Routinen für die Nachführung des Datenbestandes übergeben.

Änderungen der gespeicherten Daten werden so in *Transaktionen* gruppiert, die die Datenbank jeweils von einem konsistenten Zustand in einen andern konsistenten Zustand überführt. Vom System muss garantiert werden, dass unter allen Umständen – auch bei Stromausfall – eine Transaktion entweder vollständig oder gar nicht ausgeführt wird. Ein einfaches Beispiel: Soll der Betrag X vom Konto A auf das Konto B übertragen werden, so müssen sowohl das Wegnehmen bei A als auch das Zufügen bei B in einer Transaktion zusammengefasst werden; es darf nicht nur eine der beiden Operationen ausgeführt werden.

Besondere Aufmerksamkeit ist bei Systemen erforderlich, mit denen mehrere Benützer gleichzeitig arbeiten können, wie sie neustens auch in Vermessungsbüros eingesetzt werden. In solchen Systemen muss verhindert werden, dass ein Benützer unabsichtlich eine Änderung eines andern Benützers stört, ohne dass dies bemerkt wird.

In den meisten Fällen empfiehlt es sich, vom System automatische Aufzeichnungen über alle Transaktionen erstellen zu lassen; diese können auch zur Nachführung von Sicherheitskopien eingesetzt werden.

Bis bessere Methoden zur Verfügung stehen, wird zweierlei nötig sein: Programme sind ausführlichen Tests zu unterwerfen, und die für Datensicherung wichtigen Teile sind genau zu inspizieren. Solche Prüfungen sind recht aufwendig und verlangen Spezialkenntnisse, weshalb sie nur in besonderen Fällen den verantwortlichen Geometern übertragen werden können. Diese Überprüfung ist eine ähnliche Aufgabe wie die Verifikation und sollte deshalb von der Aufsichtsbehörde übernommen werden.

6. Anwendung

Diese Norm ‹Datensicherung› zeigt, welche Vorkehrungen getroffen werden sollten, um die Daten der amtlichen Vermessung vor Verlust zu schützen. Deshalb sollte sie immer wieder herangezogen werden, um die getroffenen Massnahmen zu prüfen. Wie im Anhang 2 der Norm gezeigt wird, können die Massnahmen, die die Norm vorschreibt, als Check-Liste verwendet werden, um zu prüfen, ob die getroffenen Anordnungen im Einzelfall ausreichen. Nicht alle heute bestehenden Systeme werden diesen Test bestehen. Aus verschiedenen Gründen können aber nicht mehr alle wünschbaren systeminternen Massnahmen ergriffen werden. Allfällige Schwachstellen müssen dann durch entsprechende manuelle Kontrollen gesichert werden.

7. Schluss

Der Normentwurf will dem Ingenieur-Geometer, der in seinem Büro EDV für die Verarbeitung von Daten der amtlichen Vermessung einsetzt, zeigen, welche Gefahren diese Daten bedrohen und wie er sich dagegen schützen kann. Die Norm richtet sich aber auch an die Entwickler von Programmen für die amtliche Vermessung, indem sie zeigt, welche Kontrollen, die heute manuell durchgeführt werden, in Zukunft vom Programm automatisch ausgeführt werden sollen.

Herrn Prof. Dr. H.-P. Friedrich, der mir verschiedentlich wertvolle Auskünfte über die hier dargestellte rechtliche Thematik gegeben hat, danke ich bestens.

Literatur

Chevallier 81
Chevallier, J. J.: Constituants et produits d'un LIS; Problèmes de la cohérence des informations. FIG XVI-Congress 1981, Paper 301.3

Entwurf SIA 260
Sicherheit und Gebrauchsfähigkeit von Tragwerken; Entwurf, 5. Fassung vom Mai 1980

Fischer 80
Fischer, W.: Die SIA-Norm unter rechtlichen Aspekten. Schweizer Ingenieur und Architekt 25/1980, S. 625

Frank 80
Frank, André: Jahresversammlung des Verbandes Schweizerischer Grundbuchverwalter: Grundbuch und elektronische Datenverarbeitung. Vermessung, Photogrammetrie, Kulturtechnik 11/80, S. 458

Friedrich 74
Friedrich, H.-P.: Datenverarbeitung und Grundbuch. Schweizerische Zeitschrift für Beurkundungs- und Grundbuchrecht 4/1974, S. 193

Friedrich 80
Friedrich, H.-P.: Rechtliche Voraussetzungen und Probleme einer EDV-Grundbuchführung in der Schweiz. Schweizerische Zeitschrift für Beurkundungs- und Grundbuchrecht 2/1981, S. 78

Mutter 80
Mutter, Peter: Persönlichkeitsschutz und Datensicherung; Überlegungen zur Durchführbarkeit und zu den Kosten. Diss. Schulthess Polygraphischer Verlag, Zürich 1980.

Schneider 80
Schneider, Jörg: Gefahren, Gefährdungsbild und ein Sicherheitskonzept. Schweizer Ingenieur und Architekt 7/1980, S. 115

ZBGR 80
Schweizerische Zeitschrift für Beurkundungs- und Grundbuchrecht 2/1981 mit den Referaten: Projekt Grundbuchautomation in der BRD.
Göttlinger, Franz: Fachliche Voraussetzungen und Zielvorstellungen.
Zechmeister, Klaus: EDV-Konzeption.

Zehnder 80
Zehnder, C. A.: Datenbank-Einsatz. ETH Zürich, Institut für Informatik 1978.

Adresse des Verfassers:
Dipl. Ing. A. Frank,
Institut für Geodäsie und Photogrammetrie,
ETH-Hönggerberg, CH-8093 Zürich

Entwurf zu einer künftigen Norm Datensicherung in der amtlichen Vermessung

Automationskommission SVVK: A. Frank, U. Höhn

Vorbemerkung:
Der SVVK beabsichtigt, Normen herauszugeben. Der vorliegende Text zur Datensicherung ist so gestaltet, wie sich die Kommission eine künftige Norm ‹Datensicherung› vorstellt. Mit diesem ‹Entwurf› wird einerseits dem Informationsbedürfnis Rechnung getragen; anderseits wird der Frage, wer solche Normen in Zukunft genehmigen und herausgeben soll, nicht vorgegriffen.
Im Text ist zu unterscheiden zwischen
- dem Text, der normierende Aussagen enthält und
- den Erläuterungen dazu.

Die Erläuterungen sind in kleinerer Schrift gedruckt.

Inhaltsverzeichnis:
1. Begriffe
2. Ziel der Datensicherung
3. Zweck der Norm
4. Geltungsbereich
5. Grundlagen
6. Anforderungen an die Datensicherung
   6.1 Verlust der Daten durch Zerstörung oder Alterung der Datenträger
   6.2 Zerstörung oder Verfälschung der Daten durch fehlerhafte Verarbeitung
   6.3 Unzugänglichkeit der Daten durch Ausfall der Zugriffsmechanismen
   6.4 Gefährdungsbilder
7. Beschreibung der Verantwortlichkeitsbereiche
8. Anhang

1. Begriffe[1]

Datensicherung

[1] Datensicherung umfasst alle Massnahmen, die den Verlust oder die Verfälschung gespeicherter Daten verhindern und den Zugriff auf die Daten innert nützlicher Frist sicherstellen.
[2] Durch Datensicherung wird Datensicherheit angestrebt.
[3] Datensicherung ist von Datenschutz und Datenqualität zu unterscheiden.

Datenschutz bedeutet, dass die Daten davor geschützt sein sollen, von Unbefugten eingesehen oder verändert zu werden. Gute Datenqualität (franz. validité des données) bedeutet, dass die Daten die wirklichen Verhältnisse richtig beschreiben.

[1] Die Begriffsbestimmungen sind für alle Normen gesamthaft in einer besonderen Norm zusammenzufassen.
[2] Siehe Norm ...

2. Ziel der Datensicherung

[1] Ziel der Datensicherung ist, die mit Mitteln der automatischen Datenverarbeitung gespeicherten Daten langfristig in jederzeit verwendbarer Form zu erhalten.
Die Daten und die dazugehörigen Zugriffsverfahren sind so zu verwahren, dass sie nicht zerstört oder verfälscht werden können. Die Daten müssen überdies innert nützlicher Frist zur Verfügung stehen.
Es muss dafür gesorgt werden, dass auf keinen Fall sämtliche Sicherheitskopien eines Datenbestandes gleichzeitig zerstört oder verfälscht werden können. Bei unvermeidlichen Pannen müssen die Originaldaten rekonstruiert werden können.
Insbesondere sind folgende Gefahren zu beachten:

a) Daten können zerstört werden, indem die Datenträger, auf denen sie aufgezeichnet sind, zerstört werden.

b) Auch wenn die Datenträger äusserlich unversehrt sind, können einzelne Daten oder ganze Datenmengen bei der Verarbeitung zerstört oder verfälscht werden.

c) Daten, die mit Mitteln der automatischen Datenverarbeitung aufgezeichnet sind, können, wenn die Zugriffsmechanismen (Programme und Anlagen) ausfallen, nicht verwendet werden.

Daten können bei der Übertragung verfälscht werden, oder Programme, die graphische oder alphanumerische Darstellungen erzeugen, können auch die richtig gespeicherten Daten unrichtig wiedergeben; diese Probleme werden an anderer Stelle behandelt.[2]
Die Daten der amtlichen Vermessung werden heute immer mehr auf EDV-Speichermedien aufbewahrt. Die so gespeicherten Angaben sind dem Menschen nicht mehr direkt zugänglich; wir können mit unseren Sinnen nicht feststellen, ob überhaupt Daten gespeichert sind, ob die richtigen Daten in der richtigen Form gespeichert und ob sie richtig nachgeführt sind. Daraus ergeben sich besondere Probleme zur Sicherung von Daten auf solchen Medien. Regeln dafür soll diese Norm aufstellen.
In den Daten der amtlichen Vermessung steckt viel Geld. Man muss sich realistisch vorstellen, wie schwierig und kostspielig es ist, sie bei einem Verlust wieder zu beschaffen. Allein schon eine allfällig nötige Neuerfassung ab Belegen kann sehr teuer sein. Auch wenn man zugestehen muss, dass absolute Sicherheit nicht zu erreichen ist, muss versucht werden, eine wirtschaftlich vertretbare, optimale Lösung zu finden.
Ein kostengünstiges Optimum erreicht man, wenn verschiedene Massnahmen kombiniert werden. Neben den programmgesteuerten Vorkehren, die in den meisten Fällen vorzuziehen sind, können auch konventionelle Massnahmen stehen, etwa:
- Kontrollisten,
- schriftliche Anweisungen über Arbeitsabläufe,
- verbindliche Arbeitsvorlagen,
- ...

3. Zweck der Norm

[1] Die Norm Datensicherung soll festlegen, wie gut Daten gegen Verlust gesichert werden müssen. Diese Normierung erfolgt aber nicht durch formale Sicherheitsvorschriften, sondern dadurch, dass Massnahmen aufgezählt werden, die eine genügende Sicherheit gewährleisten.
Um das zu erreichen, werden die in der EDV allgemein bekannten und angewandten Grundsätze und Methoden der Datensicherung auf die amtliche Vermessung zugeschnitten.
[2] Die Anforderungen der Datensicherung werden erfüllt, indem Massnahmen ergriffen werden, die eine mindestens ebenso grosse Sicherheit erreichen wie die in der Norm erwähnten.
[3] Die Norm muss sowohl bei der Planung neuer EDV-Anwendungen in der amtlichen Vermessung als auch bei der Überprüfung bestehender Anwendungen herangezogen werden.

4. Geltungsbereich

[1] Die Norm Datensicherung befasst sich nur mit Daten der amtlichen Vermessung, die auf Datenträgern gespeichert sind und deshalb vom Menschen in der Regel nicht direkt gelesen werden können.
[2] Sie kann aber sinngemäss auch zur Beurteilung der Sicherung von traditionellen Vermessungswerken herangezogen werden. Die Norm zielt besonders auf die Datenverarbeitung mit Anlagen im Geometerbüro; sie gilt sinngemäss auch für Rechenzentren.
[3] Die Norm erfasst die Daten, die für die Erfüllung der Aufgaben der amtlichen Vermessung notwendig sind: ‹rechtsgültige Daten›, aber auch ‹noch nicht rechtsgültige› und ‹nicht mehr rechtsgültige Daten›. Bei kurzfristigen Zwischenresultaten ist entscheidend, wie einschneidend bei Verlust eine Wiederherstellung wäre.
Die Frage, wie lange nicht mehr rechtsgültige Daten bei einer amtlichen Vermessung aufzubewahren seien, ist nicht geklärt. Die zuständigen Stellen werden aufgefordert, dazu klare Weisungen zu erlassen. Müssen

alte, nicht mehr rechtsgültige Zustände rekonstruiert werden können und wie lange nach einer rechtsgültigen Nachführung?

[4] Die Aufsichtsbehörden legen fest, welche Daten von dieser Norm erfasst werden.

Ein Beispiel für die gespeicherten, von dieser Norm erfassten Daten findet sich im Anhang 2, Ziffer 2.

5. Grundlagen

Die gesetzlichen Bestimmungen gehen den technischen Anweisungen dieser Norm vor.

5.1 Gesetzliche Grundlagen des Bundes

Schweizerisches Zivilgesetzbuch:
besonders Art. 950 und Schlusstitel des Art. 42. (SR 210)[3]
Verordnung über die Grundbuchvermessung:
besonders Art. 4. (SR 211.432.2)
Weisungen für die Anwendung der Automatischen Datenverarbeitung in der Parzellarvermessung:
besonders Art. 2. (SR 211.432.25)

5.2 Gesetzliche Grundlagen der Kantone

Die entsprechenden kantonalen Erlasse sind zu berücksichtigen.

5.3 Technische Grundlagen

EDV-Konzepte in der Parzellarvermessung: Bericht der Automationskommission des SVVK.

5.4 Normungstechnische Grundlagen

J. Schneider: Gefahren, Gefährdungsbild und ein Sicherheitskonzept, Schweizer Ingenieur und Architekt. Nr. 7/80, Seite 115.

Entwurf SIA 260: Sicherheit und Gebrauchsfähigkeit von Tragwerken, Weisung des SIA an seine Kommissionen für die Koordination des Normenwerkes (5. Fassung vom Mai 1980).

Ausländische Auffassungen in:

M.V. Jones: The Documentation and Checking of Computer Aided Engineering Computations, CAD 80 S. 273; (dort findet man eine ausführliche Literaturliste mit Beispielen aus dem englischsprachigen Raum).

(Ziffer 5.4 wird bei der Herausgabe als ‹Norm Datensicherung› weggelassen.)

6. Anforderungen an die Datensicherung

[1] Darstellungsform: Es werden die einzelnen Bedrohungen (Gefahren), denen die Daten ausgesetzt sind, aufgezählt und die Massnahmen beschrieben, die davor schützen sollen. Dadurch werden die Anforderungen an die Datensicherheit indirekt festgelegt.

[2] Diese oder vergleichbare Massnahmen, die entsprechende Sicherheit gegen die gleichen Gefahren bieten, sind zu treffen.

[3] Für jedes EDV-System, das gespeicherte Daten der amtlichen Vermessung verwendet, muss ein *Datensicherungs-Dokument (Sicherheitsplan)* erstellt und jedes Jahr überprüft werden. Darin ist festzuhalten, mit welchen Massnahmen die Anforderungen an die Datensicherung erfüllt werden. Die *Verantwortlichkeiten* zur Durchführung der Massnahmen sind festzulegen. Ausdrücklich sei erwähnt, dass neben technischen auch organisatorische Massnahmen getroffen werden müssen. Diese sind entsprechend zu dokumentieren.

[4] Absolute Sicherheit ist nicht zu erreichen; das *akzeptierte Risiko* ist zu beschreiben, und es ist anzugeben, von wem es getragen wird. Allenfalls ist dafür ein Versicherungsschutz anzustreben.

Unter akzeptiertem Risiko wird das Risiko verstanden, das die Gefahren oder Gefahren-Kombinationen umfasst, die zwar bekannt sind, vor denen aber die getroffenen, programmierten und konventionellen Massnahmen nicht schützen. Beispiel: Gleichzeitiger Brand in mehreren getrennten Gebäuden vernichtet alle Kopien des Datenbestandes; dieses Risiko ist ausserordentlich gering und kann getragen werden.

Versicherungsschutz ist heute gegen fast alle Schadenfolgen erhältlich, die mit der physischen Zerstörung der Datenträger verbunden sind.

Wenn man beurteilen muss, ob ein bestimmtes Risiko akzeptierbar scheint, kommt es darauf an, wie wichtig die gefährdeten Daten sind. So kann ein grösseres Risiko für Daten eingegangen werden, die nur zur Rekonstruktion alter Zustände (historische Daten) dienen oder für die Daten, die nur für statistische Zwecke (Arealstatistik) benötigt werden.

6.1 Verlust der Daten durch Zerstörung oder Alterung der Datenträger

1. Grundsätzliche Massnahme: Die Daten müssen regelmässig kopiert und die Duplikate (Sicherheitskopien) getrennt aufbewahrt werden.

Dadurch beschränkt sich das Risiko höchstens auf die Daten, die seit der Erstellung der Kopie verändert wurden. Es kann nötigenfalls durch weitere Massnahmen verkleinert werden, z. B. dadurch, dass Ausdrucke getrennt aufbewahrt werden.

Wie oft Daten kopiert werden müssen, wird bestimmt durch
- das Risiko, dass ein Verlust eintritt,
- den Aufwand, der bei einem Verlust für die Nachführung der Sicherheitskopie entsteht,
- den Aufwand, den das Kopieren verursacht.

Mindestens einmal pro Jahr muss kopiert werden; dabei sind auch Anforderungen, die in Ziffer 6.1.4.1 aufgeführt sind, berücksichtigt.

2. Grundsätzliche Massnahme: Es sind Verfahren vorzubereiten, die Kopien auf den neuesten Stand nachführen. Diese sind regelmässig zu prüfen, zumindest nach jeder Änderung an Programmen, Betriebssystemen oder an der Hardware.

6.1.1 Verlust durch Einwirkung von Elementarschaden-Ereignissen

Die Datenträger sind sehr empfindlich gegen Hitze, Verschmutzung, Wassereinbrüche usw.

1. Massnahme: Die Datenträger sind ausserhalb der unmittelbaren Bearbeitungszeit in abgeschlossenen, abgedichteten Schränken mit hoher Hitzeresistenz aufzubewahren.

2. Massnahme: Eine Kopie der Daten (Sicherheitskopie) ist in einem andern Gebäude, das nicht zum gleichen Risikobereich gehört, aufzubewahren.

6.1.2 Verlust durch absichtliche Zerstörung

6.1.2.1 durch Fremde

1. Massnahme: Die Datenträger sind ausserhalb der Bearbeitungszeit unter Verschluss aufzubewahren. Während der Bearbeitung sind die Räume zu überwachen.

6.1.2.2 durch eigenes Personal (Berechtigte)

1. Massnahme: Das Personal ist sorgfältig auszuwählen und die Arbeit zu überwachen.

2. Massnahme: Es sind organisatorische Regeln aufzustellen, die verhindern, dass eine Person alle Daten, die Sicherheitskopien eingeschlossen, zerstören kann.

6.1.3 Verlust durch unbeabsichtigte Zerstörung oder mangelnde Ordnung

1. Massnahme: Die Datenträger müssen geordnet aufbewahrt werden.

2. Massnahme: Es sind genaue Aufzeichnungen notwendig über
- den Inhalt jedes Datenträgers,
- den Zeitpunkt der Erstellung,
- die benützten Grundlagen,
- den Nachführungsstand,
- den frühesten vorgesehenen Zeitpunkt einer Löschung,
- die Freigabe zur Löschung.

3. Massnahme: Abnormale Erscheinungen bei der Benützung der Datenträger müssen notiert werden. Das Personal muss entsprechend instruiert sein.

6.1.4 Verlust durch physikalische Veränderungen innerhalb der Datenträger

Diese Gefährdung ist je nach Datenträger und Aufzeichnungsverfahren verschieden gross.

1. Grundsätzliche Massnahme: Es dürfen nur Datenträger verwendet werden, die den internationalen Qualitäts-Normen für Datenträger entsprechen (siehe

[3] SR ≙ Systematische Rechtssammlung des Bundes

‹Qualitätsanforderungen an Datenträger› im Anhang 3).
2. Grundsätzliche Massnahme: Die zulässigen Grenzen für Luftfeuchtigkeit, Lufttemperatur und Luftverschmutzung in den Lagerbehältern für die Datenträger sind einzuhalten (siehe internationale Normen ‹Umgebungsbedingungen für die Aufbewahrung von Datenträgern› im Anhang 4).

6.1.4.1 Magnetische Speichermedien
1. Massnahme: Die Speichermedien sind vor der (Wieder-)Verwendung auf Alterungserscheinungen zu kontrollieren.
2. Massnahme: Der Inhalt der Speichermedien ist regelmässig – mindestens einmal jährlich – zu kopieren. Dies gilt sinngemäss auch für die Sicherheitskopien.
3. Massnahme: Schutz vor magnetischen Streufeldern und elektrostatischen Aufladungen.

6.1.4.2 Lochkarten und Lochstreifen
1. Massnahme: Die Lagerungsbedingungen, insbesondere Luftfeuchtigkeit, sind zu kontrollieren.
2. Massnahme: Lochkarten und Lochstreifen sind regelmässig zu kopieren.
3. Massnahme: Es wird empfohlen, die Daten auf ein sichereres Speichermedium zu kopieren.

6.2 Zerstörung oder Verfälschung der Daten durch fehlerhafte Bearbeitung

1. Grundsätzliche Massnahme: Regelmässiges Kopieren der Datenbestände und laufende Aufzeichnung der vorgenommenen Änderungen – als Journal oder *Log* bezeichnet – ermöglichen es, die aktuellen Datenbestände wiederherzustellen.
Anzustreben sind Verfahren, die jede Veränderung am Datenbestand automatisch auf einem separaten Datenträger festhalten. Solche Log-Dateien können verwendet werden, um beim Verlust der Originaldaten die angelegten Kopien nachzuführen.
Werden die Originaldatenbestände anhand vorbereiteter und geprüfter Daten, die auf separaten Datenträgern gespeichert sind, ergänzt bzw. verändert, so können diese vorbereiteten Daten anstelle der Log-Dateien treten.
Programmierte Verfahren können auch durch Aufzeichnungen auf Papier ersetzt werden. Diese müssen Auskunft über alle vorgenommenen Änderungen geben. Verbindliche Arbeitsanweisungen müssen sicherstellen, dass diese Aufzeichnungen lückenlos sind.
2. Grundsätzliche Massnahme: Plausibilität und Konsistenz des ganzen Datenbestandes sind regelmässig zu kontrollieren. Dadurch werden Fehler, die sich trotz anderer Sicherheitsmassnahmen eingeschlichen haben, entdeckt. Über die so aufgedeckten Fehler sind Protokolle zu führen, die Auskunft über die Ursache des Fehlers und dessen Korrektur geben, und ist zu vermerken, welche Massnahmen getroffen wurden, um diese Art von Fehlern in Zukunft zu vermeiden.
In die gespeicherten Daten ist Redundanz so einzubauen, dass unbeabsichtigte Veränderungen erkannt werden können. Beispiele: ‹Checksum› für Dateien, Paritäts-Bits.

6.2.1 Unabsichtliche Zerstörung durch den Benützer
1. Massnahme: Das Personal muss sorgfältig ausgebildet werden und klare, übersichtliche Bedienungsanleitungen benützen.
2. Massnahme: Die Programme müssen so gebaut sein, dass es ausgeschlossen ist, dass die Daten durch Bedienungsfehler zerstört werden können.
3. Massnahme: Der Zugriff zu den Datenbeständen und deren Veränderung sind von den übrigen Programmteilen zu trennen.
4. Massnahme: Operationen, die Datenbestände gefährden, wie z. B. das beabsichtigte Löschen von Daten, dürfen nur von besonders qualifizierten Benützern ausgelöst werden.
Die Massnahmen, die unter Ziffer 6.1 gegen den Verlust der Daten durch Zerstörung der Datenträger zu ergreifen sind, helfen in Extremfällen ebenfalls mit, diesen Gefahren zu begegnen.

6.2.2 Absichtliche Verfälschung durch den Benützer
1. Massnahme: Umfassende Kontrollen, auch Plausibilitätsprüfungen genannt, die in die Programme einzubauen sind, sollen verhindern, dass der Benützer mit absichtlich verfälschten Daten arbeiten kann.
2. Massnahme: Die Anwender haben zu den Programmen im Original-Code keinen Zugang.
Die Programme im Original-Code (Quellenprogramme, Source) geben Aufschluss, welche Plausibilitätsprüfungen vorgenommen werden. Mit diesen Kenntnissen wäre es möglich, Lücken bei den Kontrollen zu erkennen und diese gezielt auszunützen.
3. Massnahme: Die Dokumentation eines Programmes wird unterteilt in die Programm-Dokumentation, die dem Unterhalt des Programms dient, und in die Anwender-Dokumentation.
4. Massnahme: Die Entwicklung der Programme und deren Anwendung sind strikte zu trennen.
5. Massnahme: Es muss in der Log-Datei aufgrund der persönlichen Passwörter jederzeit ersichtlich sein, welcher Bediener mit welcher Version welches Programmes welche Änderung durchgeführt hat.
Programmierte Aufzeichnungen sind anzustreben; aber auch Aufzeichnungen auf Papier, die lückenlos sind und geordnet aufbewahrt werden, können diesem Nachweis dienen.

6.2.3 Zerstörung oder Verfälschung durch Fremde
1. Massnahme: Der Zugang zur Anlage muss kontrolliert sein.
Arbeitsplätze bei der Anlage und der Zugang zur Anlage müssen von ständig besetzten Arbeitsplätzen eingesehen werden können.
2. Massnahme: Der Zugang zur Anlage über Datenleitungen muss durch Passwörter oder Erkennungsprozeduren so gesichert sein, dass Unberechtigte abgewiesen werden.

6.2.4. Zerstörung durch äussere Einwirkungen auf die Anlage
1. Massnahme: Die Anlagen sind so zu installieren, dass sie vor äusseren Einwirkungen möglichst geschützt sind. Die beanspruchten Räume müssen abschliessbar sein.
2. Massnahme: Die Stromversorgung ist sicherzustellen, gegebenenfalls auch für die Klimaanlage. Wenn nötig ist zu verhindern, dass Stromausfälle zu Schäden führen.

6.2.5 Verfälschung durch richtige Verarbeitung falscher Ausgangsdaten
1. Massnahme: Es muss kontrolliert werden, dass bei der Verarbeitung auf die richtigen Datenträger, d. h. auf diejenigen, die die nachgeführten Daten enthalten, zugegriffen wird.
Anzustreben sind Kontrollen, die vom Programm automatisch vorgenommen werden. Andernfalls sind organisatorische Massnahmen zu treffen, die mit Sicherheit verhindern, dass nicht mehr aktuelle Daten anstelle der aktuellen verarbeitet werden.

6.2.6 Zerstörung oder Verfälschung durch Fehler in der Hardware
1. Massnahme: Fehler in der Anlage müssen vom Betriebssystem erkannt werden und dürfen nicht zum Verlust oder zur Verfälschung der Daten führen.
Als Beispiel diene: ‹read after write›, die Paritätsprüfung und ähnliches.

6.2.7 Zerstörung oder Verfälschung durch Fehler in den Programmen
1. Massnahme: Verarbeitungsprogramme und Datenbankverwaltungsprogramme sind zu trennen. In den letzteren sind umfassende Plausibilitätsprüfungen vorzusehen.
Ob grössere Programme fehlerfrei sind, lässt sich heute noch nicht beweisen. Um die Datensicherheit zu erhöhen, sind die Programme aufzuteilen, einerseits in Teile, die auf die gespeicherten Daten zugreifen und diese verändern, und anderseits in Teile, die diese Daten verarbeiten. Letztere sind für die Datensicherung nicht problematisch. Diejenigen Programme, die auf die gespeicherten Daten zugreifen, sind weiter zu trennen in Teile, die nur lesen – sie gefährden die gespeicherten Daten nicht –, und solche, die Daten verändern oder löschen. Die reinen Leseprogramme sind nur in Mehrfachbenut-

zer-Systemen kritisch, indem gelesene Daten innerhalb einer Transaktion gegen Veränderungen zu schützen sind.
Die Konsistenz der Datenbanken muss auch bei aussergewöhnlichen Ereignissen, wie z. B. Unterbruch der Stromversorgung während einer Änderung, erhalten bleiben.

2. Massnahme: Änderungen am Datenbestand müssen in Transaktionen gegliedert sein, die den Datenbestand von einem konsistenten Zustand in einen neuen konsistenten Zustand überführen.
3. Massnahme: Transaktionen müssen so ausgeführt werden, dass inkonsistente Zwischenphasen nur sehr kurzfristig bestehen und andern Benützern unter keinen Umständen zugänglich werden.
4. Massnahme: Führt eine Prozedur eine Änderung (Transaktion) des Datenbestandes durch, so muss sichergestellt sein, dass auch bei Unterbruch der Prozedur entweder die Änderung vollständig durchgeführt wurde oder überhaupt nicht, d. h. alle angefangenen Änderungen rückgängig gemacht werden.
5. Massnahme: Die Programme sind vor ihrer Zulassung in der amtlichen Vermessung durch die Aufsichtsbehörde umfassend zu prüfen.
Die Aufsichtsbehörde kann eine solche Prüfung an andere Stellen delegieren. Im Hinblick auf die Datensicherung ist insbesondere die Prüfung der Programmteile wichtig, die Daten verändern.
6. Massnahme: Für die Entwicklung von Programmen sind Richtlinien aufzustellen.
Programmierrichtlinien erleichtern die Prüfung und den Unterhalt von Programmen. Die Aufsichtsbehörden kontrollieren, dass bei der Erstellung von Programmen von den Auftraggebern geeignete Richtlinien vorgegeben werden.

6.3 Unzugänglichkeit der Daten durch Ausfall der Zugriffsmechanismen

Daten sind nicht nur verloren, wenn sie auf den Datenträgern nicht mehr vorhanden sind, sondern auch, wenn die Anlagen, die diese Datenträger lesen könnten, nicht mehr funktionieren oder nicht mehr existieren.
1. Grundsätzliche Massnahme: Die Daten sind, zumindest bei den Sicherheitskopien, auf Standard-Datenträger in Standard-Formaten aufzuzeichnen. Dabei sind die Normen für die Ausgestaltung der Schnittstellen einzuhalten.
Anlagen und Datenträger, bei denen der Datentransfer auf Standard-Datenträger nicht möglich ist, bieten keine genügende Sicherheit.

6.3.1 Unzugänglichkeit durch Verlust der zugreifenden Software

1. Massnahme: Auch von der Software und der zugehörigen Dokumentation sind Sicherheitskopien anzulegen und getrennt zu lagern.
2. Massnahme: In der Programmdokumentation müssen alle Angaben enthalten sein, die es gegebenenfalls ermöglichen, Programme zum Lesen der Daten neu zu erstellen.

6.3.2 Unzugänglichkeit durch Störungen an der zugreifenden Hardware

1. Massnahme: Die Wartung der Anlagen muss vertraglich sichergestellt sein.
2. Massnahme: Es muss dafür gesorgt werden, dass die Daten auch auf einer andern, benachbarten Anlage gelesen werden können. Die Benützung dieser fremden Anlage muss mit deren Besitzer zum vornherein abgesprochen sein. Die dafür notwendige Software muss erstellt und das Vorgehen regelmässig getestet werden.

6.3.3 Unzugänglichkeit durch Ausfall von Personal

1. Massnahme: Die Programme für die Datenverarbeitung müssen so dokumentiert sein, dass sie von jedem EDV-Sachverständigen eingesetzt werden können.
2. Massnahme: Neben der innerbetrieblichen Stellvertretung muss allenfalls auch eine überbetriebliche Stellvertretung organisiert sein.

6.4 Gefährdungsbilder

[1] Schadenfälle treten gelegentlich nicht nur als einzelne isolierte Ereignisse auf. Es sind auch Kombinationen von schädigenden Ereignissen zu beachten.
[2] Die zu treffenden Massnahmen müssen zumindest gegen folgende Kombinationen von schädigenden Ereignissen Sicherheit bieten:

A) Verlust der Daten durch Zerstörung der Datenträger
- durch Elementarschaden-Ereignis oder
- durch Zerstörung
  - durch Fremde oder
  - durch eigenes Personal

gleichzeitig mit
Unzugänglichkeit der Daten durch Ausfall der Zugriffsmechanismen
- wegen Ausfalls der Programme und/oder
- wegen Ausfalls der Anlage.

Auch für die Wiederherstellung muss mit dem Ausfall des Personals gerechnet werden.

B) Versehentliche Zerstörung der Daten gleichzeitig mit
Ausfall der Programme.

C) Zerstörung der Daten durch fehlerhafte Bearbeitung gleichzeitig mit
Unzugänglichkeit der Daten durch Ausfall der Zugriffsmechanismen; beides entweder durch Störung der Anlage oder Ausfall der Programme verursacht.

7. Beschreibung der Verantwortungsbereiche

[1] Zur Verhütung von Schäden ist es wichtig, die Verantwortungsbereiche klar abzugrenzen. Im folgenden werden die Verantwortungsbereiche und die darin auszuübenden Funktionen beschrieben.
[2] Das Datensicherungsdokument jeder Anlage (vgl. Ziffer 6, Einleitung) legt die Verantwortungsbereiche schriftlich fest. Ferner wird jeder Funktion eine verantwortliche Person zugeteilt. Gegenüber der Norm abgeänderte Abgrenzungen der Verantwortungsbereiche sind detailliert zu beschreiben.
Für Schäden, die aus Verlust oder Verfälschung von Daten entstehen, ist gegenüber dem Auftraggeber der beauftragte patentierte Ingenieur-Geometer bzw. die Vermessungsfirma verantwortlich. Haftpflicht-rechtliche Ansprüche können allenfalls vermindert werden, wenn nachgewiesen werden kann, dass die zumutbare Sorgfalt angewendet wurde.
Die Funktion der Aufsichtsbehörden des Kantons und des Bundes ergibt sich aus den Gesetzen, insbesondere aus der ‹Instruktion über die Parzellarvermessung› SR 211.432.23. Diese Funktion kann nicht durch eine Norm erfasst werden.

7.1 Verantwortlicher Ingenieur-Geometer

[1] Er ist generell dafür verantwortlich, dass die gesetzlichen Vorschriften eingehalten und in dieser Norm vorgesehene Massnahmen getroffen werden. Insbesondere muss er:
A) das Datensicherungsdokument erstellen und regelmässig überprüfen,
B) die Verantwortlichkeitsbereiche abgrenzen,
C) für die im folgenden beschriebenen Funktionen Mitarbeiter einsetzen, die den Anforderungen der Aufgaben gewachsen sind (Ziff. 6.1.2.2(1)),
D) seine Mitarbeiter richtig anleiten und die Einhaltung der Anweisungen überprüfen (6.1.2.2(2), 6.2.1(1)),
E) die Stellvertretungen regeln (Ziff. 6.3.3(2)).
Im Anhang 2 ist ein Beispiel aus der Praxis beigefügt. Auch wird auf die Tabelle im Anhang 1 verwiesen.

7.2 Funktion: langfristige Datensicherung

[1] Diese Funktion umfasst die Massnahmen 6.1, 6.1.1, 6.1.2.2(2), 6.1.3(2), 6.1.4, 6.1.4.1, 6.1.4.2, 6.2(2), 6.3, 6.3.1, 6.3.2(2).
Hier sind alle im wesentlichen periodischen Massnahmen aufgeführt, die für die langfristige Sicherung der Daten notwendig sind.

7.3 Funktion: laufende Datensicherung

[1] Diese Funktion umfasst die Massnahmen 6.1.1(1), 6.1.2.1(1), 6.1.2.2(2), 6.1.3, 6.1.4, 6.1.4.1, 6.1.4.2(1), 6.1.4.2(2), 6.2(1), 6.2.2(5), 6.2.3, 6.2.4, 6.2.5, 6.3.1(1).

Hier sind die Massnahmen aufgeführt, die im täglichen Gebrauch die Daten vor Verlust schützen. Dazu gehört insbesondere, dass kontrolliert wird, ob die Datenträger geordnet aufbewahrt werden.

7.4 Funktion: Unterhalt der Anlage

[1] Diese Funktion umfasst die Massnahmen 6.1.3(3), 6.3.2(1).

Die diese Funktion ausübende Person sorgt entweder selbst für den Unterhalt oder sie überwacht diese Arbeit.

Für den Unterhalt der Anlage sind zusätzlich langfristige vertragliche Abmachungen mit dem Hersteller bzw. dessen Vertreter empfohlen.

7.5 Funktion: Erstellen und Unterhalt der Programme

[1] Diese Funktion umfasst die Massnahmen 6.1.2(2), 6.2, 6.2.1, 6.2.2, 6.2.5, 6.2.6, 6.2.7, 6.3.1, 6.3.3(1).

Diese Massnahmen müssen bei der Gestaltung und Erstellung der Programme berücksichtigt werden. Durch die Prüfung der Programme wird dies kontrolliert.

7.6 Funktion: Ausführen von ‹gefährlichen› Programmen

[1] Die diese Funktion ausübende Person erhält die Berechtigung, ‹gefährliche› Programme gemäss Ziffer 6.2.1(4) auszuführen.

[2] Sie ist auf die entsprechenden Gefahren hinzuweisen und besonders sorgfältig zu instruieren (6.2.2(5)).

[3] Sie trifft die Massnahmen 6.1.3(2), 6.1.3(3).

Gewisse Programme, insbesondere Hilfsprogramme des Betriebssystems (sogenannte Utilities), können ganze Datenbestände unbrauchbar machen (z. B. löschen).

Diese Programme enthalten i. a. keine Sicherungen gegen falsche Verwendung und dürfen deshalb nicht allgemein zur Verfügung stehen, sondern ihre Verwendung darf nur speziell instruiertem Personal möglich sein.

7.7. Funktion: Ausführen von Programmen, die Daten verändern

[1] Diese Funktion umfasst die Berechtigung, Programme auszuführen, die Veränderungen im Datenbestand bewirken.

[2] Dazu sind sachkundige, erfahrene Mitarbeiter zu ermächtigen, die auch darüber instruiert sind, wie sie in Ausnahmefällen vorzugehen haben.

[3] Sie treffen die Massnahmen 6.1.3(2), 6.1.3(3), 6.2(1), 6.2.2(5).

Die Programme dieser Gruppe dienen zur Veränderung einzelner Datenelemente unter Kontrolle des Programmes; Fehlmanipulationen, die grössere Teile des Datenbestandes durch die Kontrollen des Programmes unbrauchbar machen, sind verunmöglicht.

7.8 Funktion: Ausführen von Programmen, die Daten lesen

[1] Die diese Funktion ausübenden Personen haben die Berechtigung, Programme auszuführen, die zwar Daten lesen, den Datenbestand aber nicht verändern können.

[2] Diese Mitarbeiter sind genau zu instruieren und regelmässig zu kontrollieren. Die Gefahr allfälliger Fehlmanipulationen muss ihnen bewusst gemacht werden.

Anhänge

1. Tabelle über Zuordnung der Massnahmen zu den Funktionen
2. Beispiel eines Datensicherungsdokumentes
3. Qualitätsanforderungen an Datenträger
4. Umgebungsbedingungen für die Aufbewahrung von Datenträgern

Anhang 1

Massnahme / Funktion	Nr.	Stichwort	7.1 Verantwortlicher Ingenieur-Geometer	7.2 langfristige Datensicherung	7.3 bürointerne Datensicherung	7.4 Unterhalt der Anlage	7.5 Erstellen und Unterhalt der Programme	7.6 Ausführen von ‹gefährlichen› Programmen	7.7 Ausführen von Programmen, die Daten verändern	Aufgaben der Aufsichtsbehörde (pro memoria)
	6. (1)	Datensicherungsdokument erstellen	X							
	6. (2)	Verantwortlichkeitsbereiche abgrenzen	X							
	6.1	*Verlust der Daten durch Zerstörung oder Alterung der Datenträger*								
	(1)	regelmässige Kopien		X						
	6.1. (2)	Verfahren zum Nachführen der Kopien		X			X			
	6.1.1	*Verlust durch Einwirkung von Elementarschaden-Ereignissen*								
	(1)	Datenträger sicher aufbewahren		X	X					
	6.1.1 (2)	Sicherheitskopien in anderem Gebäude		X						
	6.1.2.1	*Verlust durch absichtliche Zerstörung*								
	(1)	Datenträger unter Verschluss			X					
	6.1.2.2 (1)	Personal sorgfältig auswählen	X							
	6.1.2.2 (2)	niemand kann alle Kopien zerstören	X	X	X					
	6.1.3	*Verlust durch unbeabsichtigte Zerstörung oder mangelnde Ordnung*								
	(1)	Datenträger geordnet aufbewahren			X					
	6.1.3 (2)	Aufzeichnungen über Datenträger		X	X			X	X	
	6.1.3 (3)	Abnormale Erscheinungen notieren			X	X		X	X	
	6.1.4	*Verlust durch physikalische Veränderungen innerhalb der Datenträger*								
	(1)	Qualitäts-Datenträger verwenden		X	X					

Massnahme / Funktion			7.1 Verantwortlicher Ingenieur-Geometer	7.2 langfristige Datensicherung	7.3 bürointerne Datensicherung	7.4 Unterhalt der Anlage	7.5 Erstellen und Unterhalt der Programme	7.6 Ausführen von «gefährlichen» Programmen	7.7 Ausführen von Programmen, die Daten verändern	Aufgaben der Aufsichtsbehörde (pro memoria)
Nr.		Stichwort								
6.1.4	(2)	Lagerungsbedingungen		X	X					
6.1.4.1	(1)	*Magnetische Speichermedien* Kontrolle Wiederverwendung		X	X					
6.1.4.1	(2)	regelmässig kopieren		X	X					
6.1.4.1	(3)	Schutz vor Magneten		X	X					
6.1.4.2	(1)	*Lochkarten und Lochstreifen* Luftfeuchtigkeit		X	X					
6.1.4.2	(2)	regelmässig kopieren		X	X					
6.1.4.2	(3)	Kopie auf anderen Medien		X						
6.2	(1)	*Zerstörung oder Verfälschung der Daten durch fehlerhafte Bearbeitung* Log erstellen			X		X		X	
6.2	(2)	regelmässige Konsistenzprüfung		X			X			
6.2.1	(1)	*Unabsichtliche Zerstörung durch den Benützer* Personal ausbilden und Bedienungsanleitung	X				X			
6.2.1	(2)	Bedienungsfehler können nicht Daten zerstören					X			
6.2.1	(3)	Programme aufteilen					X			X
6.2.1	(4)	gewisse Operationen besonders qualifizierten Personen vorbehalten					X	X		
6.2.2	(1)	*Absichtliche Verfälschung durch den Benützer* Plausibilitätsprüfung					X			X
6.2.2	(2)	Anwender kennen Original-Code nicht					X			
6.2.2	(3)	Dokumentation unterteilen					X			
6.2.2	(4)	Programm-Entwicklung und Anwendung trennen					X			
6.2.2	(5)	festhalten, wer Daten ändert			X		X	X	X	
6.2.3	(1)	*Zerstörung oder Verfälschung durch Fremde* Zugang zur Anlage kontrollieren			X					
6.2.3	(2)	Zugang über Datenleitungen sichern			X					
6.2.4	(1)	*Zerstörung durch äussere Einwirkungen auf die Anlage* Anlage geschützt aufstellen			X					
6.2.4	(2)	Stromversorgung sicherstellen			X					
6.2.5	(1)	*Verfälschung durch richtige Verarbeitung falscher Ausgangsdaten* Kontrolle, dass aktuelle Datenträger verwendet werden			X		X			
6.2.6	(1)	*Zerstörung oder Verfälschung durch Fehler in der Hardware* Fehler der Anlage müssen erkannt werden					X			
6.2.7	(1)	*Zerstörung oder Verfälschung durch Fehler in den Programmen* Verarbeitung und Datenzugriff trennen					X			X
6.2.7	(2)	Änderungen in Transaktionen gliedern					X			

Massnahme / Funktion			7.1 Verantwortlicher Ingenieur-Geometer	7.2 langfristige Datensicherung	7.3 bürointerne Datensicherung	7.4 Unterhalt der Anlage	7.5 Erstellen und Unterhalt der Programme	7.6 Ausführen von ‹gefährlichen› Programmen	7.7 Ausführen von Programmen, die Daten verändern	Aufgaben der Aufsichtsbehörde (pro memoria)
Nr.		Stichwort								
6.2.7	(3)	Inkonsistente Zustände möglichst vermeiden					X			
6.2.7	(4)	Unvollständige Transaktionen rückgängig machen					X			
6.2.7	(5)	Programme vor der Verwendung prüfen lassen					X			X
6.2.7	(6)	Richtlinien für Programm-Entwicklung					X			X
6.3	(1)	*Unzugänglichkeit der Daten durch Ausfall ddr Zugriffsmechanismen* Kopieren in Standard-Format auf Standard-Datenträger		X						
6.3.1	(1)	*Unzugänglichkeit durch Verlust der zugreifenden Software* Auch Software und Dokumentation kopieren		X	X		X			
6.3.1	(2)	Beschreibung, wie Daten zu lesen sind		X			X			
6.3.2	(1)	*Unzugänglichkeit durch Störungen an der zugreifenden Hardware* Wartung der Anlage sicherstellen				X				
6.3.2	(2)	Ausweichanlage vorbereiten		X						
6.3.3	(1)	*Unzugänglichkeit durch Ausfall von Personal* Programm-Dokumentation					X			
6.3.3	(2)	Stellvertretung organisieren	X							

Anhang 2

Beispiel eines Datensicherungs-Dokumentes

Grundbuchvermessung Gemeinde A

Datensicherungs-Dokument

Gestützt auf Ziffer 6 der Norm Datensicherung in der amtlichen Vermessung wird für die Gemeinde A ein Datensicherungs-Dokument (Sicherheitsplan) formuliert.

Die vorhandenen Hilfsmittel, insbesondere die Programme, erlauben nicht, alle in der Norm aufgeführten Massnahmen sofort zu ergreifen. Vorübergehend muss durch zusätzliche Kontrollen und administrative Massnahmen das verbleibende Risiko auf ein akzeptierbares Mass gedrückt werden.

Beim Ersatz der vorhandenen Hard- oder Software sind bessere Voraussetzungen für die Einhaltung der Norm anzustreben.

Inhaltsverzeichnis:

1. Grundlage
2. Gegenstand
3. Hilfsmittel
4. Personaleinsatz, Verantwortlichkeit
5. Massnahmen, akzeptiertes Risiko
6. Gefährdungsbilder

1. Grundlage

1.1 Norm Datensicherung in der amtlichen Vermessung

1.2 Weisungen des kantonalen Vermessungsamtes vom ..... und .....

1.3 Bestimmungen des Nachführungs-Vertrages Ziffer ..... und .....

2. Gegenstand

Alle auf EDV-Datenträger erfassten Vermessungsdaten der Gemeinde A, bestehend aus:

- Koordinatenverzeichnis der
  Triangulationspunkte
  Polygonpunkte
  Grenzpunkte
  Situationspunkte
  Baulinienpunkte
- Grenzliniendefinitionen.

3. Hilfsmittel

3.1 Software

Programmpaket für Grundbuchvermessungen der Firma B vom .....

3.2 Hardware

Tischcomputer Fabrikat C, bestehend aus:

- Rechner
- Floppy-Disk-Station (2 Laufwerke)
- Schreibeinheit

3.3 Dokumentation

- Beschreibung der Programme
- Bedienungsanleitung für Programme
- Beschreibung Hardware

3.4 Datenträger

Floppy-Disketten (Lieferant D). Der Lieferant garantiert, dass die Disketten die Anforderungen der ECMA-Normen für Disketten erfüllen.

4. Verantwortlichkeiten

Die Aufteilung der Verantwortlichkeitsbereiche folgt der Ziffer 7 der Norm.

Verantwortlicher Geometer ist A (Norm Ziffer 7.1); er wird im Notfall durch C vertreten.

Die Funktion ‹langfristige Datensicherung› (Norm Ziffer 7.2) und ‹bürointerne Datensicherung› (Norm Ziffer 7.3) übernimmt B; er wird durch C vertreten.

Der Unterhalt der Anlage (Norm Ziffer 7.4) wird vom Lieferanten, dem Vertreter der Firma C, besorgt. Betriebsintern ist B, stellvertretend C, zuständig.
Der Unterhalt der Programme (Norm Ziffer 7.5) erfolgt durch den Lieferanten, die Firma B. Betriebsintern ist B, stellvertretend C, zuständig.
Das Ausführen von ‹gefährlichen› Programmen (Norm Ziffer 7.6) ist nur B erlaubt. Eine Stellvertretung ist nicht notwendig.
Bearbeitungs-Programme, die Daten verändern (Norm Ziffer 7.7), dürfen von B, C und D ausgeführt werden.
Programme, die nur Daten lesen, sind keine vorhanden.

5. Massnahmen

Ziffer der Norm		Stichwort	M: Massnahme V: Verantwortung, sofern nicht gem. Ziffer 4 R: Akzeptiertes Risiko
6.	(1)	Datensicherungs-Dokument erstellen	M: Das Datensicherungs-Dokument ist anlässlich des jährlichen Berichtes über das Vermessungswerk auf Richtigkeit und Vollständigkeit zu prüfen
	(2)	Verantwortlichkeitsbereiche abgrenzen	M: Die Beschreibung der Verantwortlichkeitsbereiche und die Bezeichnung der entsprechenden Personen erfolgt in Ziffer 4 dieses Datensicherungs-Dokumentes V: Ing.-Geometer
6.1		*Verlust der Daten durch Zerstörung oder Alterung der Datenträger*	
	(1)	Regelmässiges Kopieren	M: Von jedem Datenträger (Floppy-Diskette) wird jährlich einmal eine Sicherheitskopie des neuesten Standes erstellt, geprüft und im Gemeindearchiv aufbewahrt M: Eine zusätzliche Kopie wird halbjährlich oder nach grossen Mutationen erstellt und im verschlossenen Schrank im Raum X aufbewahrt
	(2)	Verfahren zum Nachführen der Kopien	M: Müssen die Daten rekonstruiert werden, so werden die Sicherheitskopien mit den üblichen Programmen anhand der schriftlichen Aufzeichnungen bei den Mutationsakten nachgeführt
6.1.1		*Verlust durch Einwirkung von Elementarschaden-Ereignissen*	
	(1)	Datenträger sicher aufbewahren	M: Die Originaldatenträger werden bei der EDV-Anlage in einem Schrank mit feuerhemmender Verkleidung aufbewahrt
	(2)	Sicherheitskopien in anderen Gebäuden	M: Die Sicherheitskopien werden im Gemeindearchiv aufbewahrt, und zwar dürfen die alten Kopien erst zurückgezogen werden, nachdem die neu erstellten archiviert sind
6.1.2		*Verlust durch absichtliche Zerstörung*	
6.1.2.1	(1)	Datenträger unter Verschluss	M: Die Rechenanlage mit den Originaldatenträgern steht in einem separaten Raum. Dieser wird abgeschlossen, sobald er nicht beaufsichtigt ist M: Der Schrank im Raum X, der die Kopien enthält, ist ebenfalls verschlossen zu halten M: Die Sicherheitskopien im Gemeindearchiv sind genügend geschützt
6.1.2.2	(1)	Personaleinsatz	M: Die Sachbearbeiter werden unter Ziffer 4 namentlich bezeichnet
	(2)	Niemand kann alle Daten zerstören	M: Der Zugang zu den Daten im Gemeindearchiv unterliegt einer zusätzlichen Kontrolle. Die Sachbearbeiter haben freien Zutritt R: Böswillige Zerstörung der Daten durch die Sachbearbeiter ist nicht vollständig ausschliessbar
6.1.3		*Verlust durch unbeabsichtigte Zerstörung oder mangelnde Ordnung*	
	(1)	Datenträger geordnet aufbewahren	M: Die Original-Datenträger werden in einem Spezialschrank nach der in Beilage 1 angegebenen Ordnung abgelegt
(2)		Aufzeichnungen über Datenträger	M: Alle Disketten-Hüllen sind nach dem in Beilage 2 angegebenen Muster zu numerieren und zu beschriften; über die Verwendung der Disketten wird in der Disketten-Kontrolle
	(3)	Abnormale Erscheinungen	Buch geführt, wo auch abnormale Erscheinungen notiert werden

Ziffer der Norm		Stichwort	M: Massnahme V: Verantwortung, sofern nicht gem. Ziffer 4 R: Akzeptiertes Risiko
6.1.4		*Verlust durch physikalische Veränderungen innerhalb der Datenträger*	
	(1)	Qualitätsdatenträger	M: Es werden nur Datenträger des Fabrikates D verwendet (vgl. Ziffer 3.3)
	(2)	Lagerungsbedingungen	M: Die Raumtemperatur und die Luftfeuchtigkeit bleiben immer im Rahmen der Vorschriften des ECMA Standard-69. Eine spezielle Überwachung erübrigt sich
6.1.4.1		*Magnetische Speichermedien*	
	(1)	Kontrolle bei Wiederverwendung	M: Vor der Wiederverwendung von Disketten sind diese mit Programm X zu überprüfen
	(2)	regelmässig kopieren	M: Vgl. Ziffer 6.1 (1)
	(3)	Schutz vor Magneten	M: Das Personal ist informiert
6.1.4.2		*Lochkarten und Lochstreifen*	Nicht vorhanden
6.2		*Zerstörung oder Verfälschung der Daten durch fehlerhafte Bearbeitung*	
	(1)	Kopieren und Journal	M: vgl. Ziffer 6.1 M: Änderungen an den Daten werden nur auf Grund von Mutationsakten vorgenommen; diese werden aufbewahrt
	(2)	regelmässige Konsistenzprüfung	M: Mit den vorhandenen Programmen nicht möglich R: Fehler können über längere Zeit unentdeckt bleiben
6.2.1		*Unbeabsichtigte Zerstörung durch den Benützer*	
	(1)	Ausbildung, Bedienungsanleitung	M: Die Bedienungsanleitung ist streng einzuhalten M: Änderungen bei der Bedienung sind in der Bedienungsanleitung nachzutragen und alle Benützer zu instruieren V: B
6.2.1	(2)	Folgen von Bedienungsfehlern	M: Diese Massnahmen können in die bestehenden Programme nicht mehr eingebaut werden
	(3)	Programme aufteilen	R: Durch Bedienungsfehler können Daten zerstört werden
	(4)	Folgenschwere Operationen	M: Das Löschen bzw. Formatieren von Disketten erfolgt ausschliesslich durch die Person B. Das selbe gilt für die Erstellung der Sicherheitskopien B
6.2.2		*Absichtliche Verfälschung durch den Benützer*	
	(1)	Plausibilitätsprüfung	M: vgl. 6.2.1 (2) und (3)
	(2)	Anwender kennt Originalcode nicht	M: Programmierung und Programmwartung durch Lieferfirma R: Programme sind nicht gegen Veränderung und Kenntnisnahme geschützt (systembedingt)
	(3)	Dokumentation unterteilen	M: vgl. 6.2.2 (2)
	(4)	Programmentwicklung und Anwendung trennen	M: vgl. 6.2.2 (2)
	(5)	Festhalten, wer Daten verändert	M: Der Sachbearbeiter wird bei jeder Auftragseröffnung namentlich aufgeführt
6.2.3		*Zerstörung oder Verfälschung durch Fremde*	
	(1)	Zugang zur Anlage kontrollieren	M: Vgl. Ziffer 6.1.2.1, Raum abgeschlossen
	(2)	Zugang über Datenleitung sichern	Keine Datenleitungen vorhanden
6.2.4		*Zerstörungen durch äussere Einwirkungen auf die Anlage*	
	(1)	Anlage geschützt aufstellen	M: Vgl. Ziffer 6.1.2.1, Raum abgeschlossen
	(2)	Stromversorgung sicherstellen	M: Strom-Hauptschalter nach Gebrauch der Anlage ausschalten (Kurzschlussgefahr) R: Datenverlust infolge Stromausfalls unwahrscheinlich
6.2.5		*Verfälschung durch richtige Verarbeitung falscher Ausgangsdaten*	
	(1)	Kontrolle, dass aktuelle Datenträger verwendet werden	M: Die Sicherheitskopien im Gemeindearchiv und die Kopien im Raum X müssen ständig unter Verschluss aufbewahrt werden und dürfen nicht für normale Arbeiten herangezogen werden. Andere Kopien dürfen nicht erstellt werden (Verwechslungsgefahr)
6.2.6		*Zerstörung oder Verfälschung durch Fehler in der Hardware*	
	(1)	Fehler der Anlage müssen erkannt werden	M: Der Datenaustausch zwischen Rechner und Diskette wird durch ‹Read after write›-Test kontrolliert M: Unregelmässigkeiten sind der Person B zu melden (vgl. Ziffer 4)

Ziffer der Norm		Stichwort	M: Massnahme V: Verantwortung, sofern nicht gem. Ziffer 4 R: Akzeptiertes Risiko
6.2.7		*Zerstörung oder Verfälschung durch Fehler in den Programmen*	
	(1)	Verarbeitung und Datenzugriff trennen	Diese Massnahmen können mit der bestehenden Software nicht realisiert werden
	(2)	Änderungen in Transaktionen gliedern	R: Risiko tragbar, da die Daten auf eine grosse Zahl von Einzeldisketten verteilt sind. Schäden wirken sich nur auf kleine Datenmengen aus (1 Grundbuchplan)
	(3)	Inkonsistente Zustände möglichst vermeiden	
	(4)	Unvollständige Transaktionen rückgängig machen	
	(5)	Programme vor der Verwendung prüfen lassen	M: Die Verarbeitungsprogramme sind von der Aufsichtsbehörde anerkannt
	(6)	Richtlinien für Programmentwicklung	M: Vgl. Ziffer 6.2.1 (3), Programmierung durch Lieferfirma
6.3		*Unzugänglichkeit der Daten durch Ausfall der Zugriffsmechanismen*	
	(1)	Kopien in Standard-Formaten auf Standard-Datenträgern	M: Umformatierung der Daten auf Standard-Formate ist durch den Software-Lieferanten möglich
6.3.1		*Unzugänglichkeit durch Verlust der zugreifenden Software*	
	(1)	Auch Software und Dokumentation kopieren	M: Die Software wird automatisch mit den Fixpunktkoordinaten kopiert und sichergestellt
	(2)	Beschreibung, wie Daten zu lesen sind	M: Information beim Software-Lieferanten vorhanden
6.3.2		*Unzugänglichkeit durch Störungen an der zugreifenden Hardware*	
	(1)	Wartung der Anlage sicherstellen	M: Der Verkäufer hat zugesagt, Wartungs- und Reparaturarbeiten auszuführen M: Eine Ausweichanlage kann notfalls beim Lieferanten sowie beim Geometerbüro X in Z benützt werden M: Einmal jährlich ist zu prüfen, dass Disketten dieser Anlage dort verarbeitet werden können V: B
6.3.3		*Unzugänglichkeit durch Ausfall von Personal*	
	(1)	Programm-Dokumentation	M: Programm-Dokumentation durch Software-Lieferanten erstellt
	(2)	Stellvertretung organisieren	M: Vgl. Ziffer 4, Personaleinsatz

3. Gefährdungsbilder

Solange nicht die Originaldatenträger und die Sicherheitskopien im Gemeindearchiv gleichzeitig zerstört werden, scheint eine Wiederherstellung der Daten gewährleistet. Notfalls müssen dabei Personal und Anlage beim Software-Hersteller beansprucht werden; entsprechende Zusagen sind im Briefwechsel vom ..... gemacht worden.

Anhang 3

Qualitätsanforderungen an Datenträger

Im ECMA Standard-69* werden in Sektion II und III genaue Anforderungen an die Disketten aufgestellt. Diese können aber ohne spezielle Einrichtungen nicht geprüft werden. Ähnliches gilt für Lochstreifen (ECMA Standard-10) usw.

Es ist deshalb darauf zu achten, dass der Hersteller der Datenträger die Qualität nach ISO-, ECMA- oder ANSI-Normen garantiert.

Anhang 4

Umgebungsbedingungen für die Aufbewahrung von Datenträgern

Die folgenden Ausführungen stützen sich auf verschiedene ECMA Standards.

Umgebungsbedingungen für Disketten (nach ECMA Standard-69):

Benützung Temperatur 10 °C ... 50 °C
rel. Luftfeuchtigkeit 20% ... 80%

Die Temperatur sollte sich nicht mehr als um 20 °C/Stunde ändern. Disketten, die Umgebungsbedingungen ausserhalb der Benützungsbedingungen ausgesetzt waren, sollte mindestens 24 Stunden Zeit zur Anpassung gelassen werden.

Lagerung Temperatur 4 °C ... 53 °C
rel. Luftfeuchtigkeit 8% ... 80%

Transport Temperatur – 40 °C ... 53 °C
rel. Luftfeuchtigkeit 8% ... 90%

Umgebungsbedingungen für Lochstreifen (nach ECMA Standard-10):

Die bevorzugten Bedingungen für die Lagerung von Lochstreifen sind:

Temperatur 23 °C
rel. Luftfeuchtigkeit 50%

Extreme Hitze, Trockenheit und Feuchtigkeit müssen vermieden werden.

* erhältlich bei: ECMA European Computer Manufacturers Association, Rue du Rhône 114, CH-1204 Genève

Projet pour une future norme Sécurité des données dans la mensuration officielle

Commission d'automation SSMAF: A. Frank, U. Höhn
(Traduction française: J. J. Chevallier, R. Durussel

Remarque préliminaire:
La SSMAF envisage la publication de normes. Le présent texte sur la sécurité des données correspond à l'image que se fait la Commission d'une future norme sur ce thème. De cette manière, le besoin en information est satisfait, en même temps que restent réservées les questions de compétence pour l'approbation et l'édition de telles normes.
Il convient de distinguer dans ce texte
- les parties normatives
- les commentaires y relatifs.

Les commentaires sont écrits en petites lettres.

Table des matières:
1. Notions
2. But de la sécurité des données
3. But de la norme
4. Domaine de validité
5. Bases
6. Exigences en matière de sécurité
   6.1 Perte des données par destruction ou altération du support
   6.2 Destruction ou falsification des données du fait d'un traitement défectueux
   6.3 Inaccessibilité des données par défaillance des mécanismes d'accès
   6.4 Dangers envisageables
7. Description des secteurs de responsabilité
8. Annexe

1. Notions[1]

Sécurité des données

[1] La sécurité des données comprend toutes les mesures destinées à prévenir la perte ou l'altération des données stockées, et garantissant leur accès dans un délai normal.

[3] Il convient de distinguer les notions de sécurité et de protection ou de validité.

La protection a pour but d'empêcher l'accès ou la modification des données aux tiers non autorisés. La validité des données garantit que celles-ci décrivent effectivement la réalité.

2. But de la sécurité des données

[1] Il s'agit de maintenir les données stockées par des moyens informatiques dans un état rendant possible en tout temps leur utilisation.

Les données et les moyens d'accès sont à conserver de telle manière qu'ils ne puissent être détruits ou altérés. Les données doivent de plus être en tout temps accessibles dans un délai convenable.

Il convient pour cela de s'assurer qu'en aucun cas toutes les copies de sécurité puissent être détruites ou altérées simultanément. Lors de pannes inévitables, les données originales doivent pouvoir être reconstituées.

Il faut être particulièrement attentif aux dangers suivants:

a) Des données peuvent être détruites du fait de la destruction de leur support.

b) Des données isolées ou l'ensemble d'un fichier peuvent être détruits par un traitement, quand bien même le support semble intact.

c) Des données stockées par des moyens informatiques peuvent ne plus être accessibles si les moyens d'accès (programmes et installations) sont défaillants.

Des données peuvent être altérées lors d'une transmission, ou des programmes élaborant des représentations alphanumériques ou graphiques peuvent restituer des données correctes de façon incorrecte; ces problèmes sont abordés dans la norme ...[2]

Le stockage des données de la mensuration officielle se fait de plus en plus sur des supports informatiques. Les éléments ainsi stockés ne sont plus directement accessibles à l'homme; nos sens ne nous permettent pas de déceler s'il y a des données stockées, si des données correctes sont sous une forme correcte, et si elles sont correctement mises à jour. Il s'en suit des problèmes tout particuliers pour la sécurité des données sur de tels supports. Cette norme doit présenter des règles y relatives.

Les données de la mensuration officielle représentent un capital considérable. Il faut s'imaginer à quel point il est difficile et onéreux de les saisir à nouveau si on les perd. La seule réintroduction à partir des formules de levé peut être déjà très coûteuse. S'il faut bien avouer qu'une sécurité absolue est inaccessible, il convient de trouver une solution optimale économiquement supportable.

Un optimum est atteint par des solutions combinées. A côté des solutions programmées, auxquelles on donnera en général la préférence, on peut aussi trouver des moyens conventionnels, comme:
- listes de sécurité
- instructions écrites sur le déroulement des opérations
- directives de travail impératives
- ...

3. But de la norme

[1] La norme ‹sécurité› doit préciser jusqu'à quel point des données doivent être garanties contre la perte. Cela n'est cependant pas réalisé par des prescriptions formelles de sécurité, mais bien par la présentation de mesures propres à assurer une sécurité suffisante.

Dans ce but, les principes et méthodes classiques en informatique seront adaptés aux problèmes de la mensuration officielle.

[2] Les exigences en matières de sécurité seront satisfaites, si les mesures prises garantissent une sécurité au moins équivalente à celle préconisée dans la norme.

[3] La norme doit être prise en considération, tant lors de l'étude de nouvelles applications de l'informatique en mensuration officielle, que pour l'examen d'applications existantes.

4. Domaine de validité

[1] La norme ‹sécurité› ne concerne que les données stockées sur supports informatiques, et donc dans la règle, non lisibles directement par l'homme.

[2] Elle peut cependant servir par analogie à l'appréciation de la sécurité des documents traditionnels de la mensuration. La norme vise tout spécialement l'informatique distribuée dans les bureaux de géomètre; elle peut s'appliquer par analogie aux centres de calculs.

[3] La norme se préoccupe des données qui sont nécessaires à l'accomplissement des tâches de la mensuration officielle: données ‹valides›, mais aussi ‹non encore valides› ou ‹plus valides›. Dans le cas de résultats intermédiaires, sera déterminant l'ampleur du handicap provoqué par la reconstitution après une perte éventuelle.

La durée de conservation de données périmées d'une mensuration officielle n'est par clairement fixée. Les autorités compétentes doivent donner à ce sujet des directives précises. Il s'agit de fixer, si des données périmées doivent pouvoir être reconstituées, et si oui dans quels délais.

[4] Les autorités compétentes fixent quelles données sont soumises à cette norme.

En annexe 2, on trouvera un exemple de données soumises à cette norme.

5. Bases

Les prescriptions légales ont le pas sur les indications techniques de cette norme.

[1] Les définitions sont à rassembler pour toutes les normes dans une norme spéciale.
[2] Voir norme ...

5.1 Bases légales fédérales

Code civil suisse:
En particulier art. 950 et titre final, art. 42 (RS 210)[3]
Ordonnance sur la mensuration parcellaire:
en particulier art. 4 (RS 211.432.2)
Directives pour l'emploi du traitement automatique des données en mensuration parcellaire:
en particulier art. 2 (RS 211.432.25)

5.2 Bases légales cantonales

Les prescriptions cantonales correspondantes sont à respecter.

5.3 Bases techniques

Emploi de l'informatique en mensuration parcellaire: rapport de la Commission d'automation de la SSMAF.

5.4 Bases techniques normatives

J. Schneider, Gefahren, Gefährdungsbilder und ein Sicherheitskonzept, Schweizer Ingenieur und Architekt, Nr. 7/80, p. 115.
Norme SIA 260: Sicherheit und Gebrauchsfähigkeit von Tragwerken (projet, 5e version de mai 1980)
Conceptions étrangères dans:
N. V. Jones, The Documentation and Checking of Computer Aided Engineering Computations, CAD 80 p. 273; (on y trouvera une abondante bibliographie avec des exemples des pays anglosaxons).
(Lors de la publication en tant que norme, le texte 5.4 sera supprimé)

6. Exigences en matière de sécurité

[1] Forme du texte: on décrira les diverses menaces (dangers) auxquelles sont exposées les données, ainsi que les mesures susceptibles de les en protéger. Les exigences en matières de sécurité seront ainsi indirectement définies.

[2] On prendra les mesures décrites, ou d'autres équivalentes, offrant la même sécurité contre les mêmes dangers.

[3] Il faut établir un *document de sécurité (plan de sécurité)* pour tout système d'ordinateur traitant des données de la mensuration officielle, et le réviser chaque année. Il doit préciser quels sont les moyens mis en œuvre pour assurer la sécurité des données. Il faut aussi définir les *responsabilités* pour l'exécution des mesures prévues. Mentionnons explicitement que les mesures techniques sont à compléter par des mesures d'organisation. Les documents correspondants sont à rédiger.

[4] Une sécurité absolue est illusoire; le *risque admis* sera décrit, et il sera précisé par qui il est supporté. On peut, le cas échéant, le couvrir en concluant une assurance.

Par risque admis, on entend les dangers ou combinaisons de dangers qui, bien qu'ils soient connus, ne sont pas combattus par les mesures prises, programmées ou conventionnelles. Exemple: des incendies simultanés dans plusieurs bâtiments séparés détruisent toutes les copies des fichiers; ce risque est extrêmement faible et peut être couru.

Il est actuellement possible de s'assurer contre presque tous les dangers tendant à la destruction physique des supports de données. Lorsqu'on évaluera si un risque est supportable, on considérera l'importance des données. On pourra accepter un risque plus grand pour des données ne servant qu'à la reconstruction d'anciens états des fichiers (données historiques), ou pour les données à buts statistiques (statistique des superficies).

6.1 Perte des données par destruction ou vieillissement du support

1re mesure fondamentale: Les données doivent être régulièrement copiées et les doubles (copies de sécurité) entreposées séparément.

Le risque est ainsi limité aux données modifiées depuis l'établissement de la copie. On peut encore le réduire par d'autres mesures, par exemple en conservant des imprimés séparément.

L'intervalle séparant l'établissement des copies est défini par
- le risque de perte
- le travail nécessaire pour la mise à jour de la copie en cas de perte de l'original
- le travail nécessaire pour réaliser la copie.

On établira au moins une copie par année; les exigences posées au chiffre 6.1.4.1 seront également prises en considération.

2e mesure fondamentale: Il faut mettre au point des procédés de mise à jour des copies. Elles sont à contrôler régulièrement, au minimum après toute modification apportée aux programmes, au système d'exploitation ou au matériel.

6.1.1 Perte du fait de dégâts dus aux éléments

Les supports de données sont très sensibles à la chaleur, aux poussières, à l'eau, etc.

1re mesure: En dehors des périodes d'emploi proprement dit, les supports de données sont à conserver dans des armoires fermées, étanches et hautement thermofuges.
2e mesure: Une copie des données (copie de sécurité) est à conserver dans un autre bâtiment, non soumis aux mêmes dangers.

6.1.2 Perte par destruction volontaire

6.1.2.1 par des tiers

1re mesure: en dehors du temps d'emploi, les supports de données sont à conserver sous clé. Pendant leur utilisation, il faut surveiller les locaux.

6.1.2.2 par le personnel

1re mesure: le personnel est à choisir soigneusement, et le travail est à surveiller.
2e mesure: Des mesures d'organisation doivent être prises pour éviter qu'une même personne puisse détruire toutes les données, copies de sécurité comprises.

6.1.3 Perte par destruction involontaire ou par désordre

1re mesure: Les supports de données doivent être entreposés avec ordre.
2e mesure: Ils doivent porter des indications sur
- leur contenu
- la date de leur création
- les bases utilisées pour cette création
- leur état de mise à jour
- le délai le plus court prévu pour son effacement
- la compétence pour l'effacement

3e mesure: Les anomalies apparaissant lors de l'emploi des supports de données doivent être notées. Le personnel doit être instruit en conséquence.

6.1.4 Perte par modification interne du support

Ce danger est variable selon le support et le mode d'écriture.
1re mesure fondamentale: Il ne faut utiliser que des supports de données répondant aux normes internationales de qualité (cf. «exigeances de qualité pour les supports de données» à l'annexe 3).
2e mesure fondamentale: les limites d'humidité, de température et d'empoussièrement doivent être respectées (cf. normes internationales «Conditions posées à l'environnement des supports de données» à l'annexe 4).

6.1.4.1 Supports magnétiques

1re mesure: Avant tout (ré-)emploi, l'état de vieillissement du support doit être contrôlé.
2e mesure: Le contenu doit être copié régulièrement – au moins une fois par année. Ceci est valable par analogie pour les copies de sécurité.
3e mesure: Il faut protéger les supports contre les champs magnétiques parasites et les charges statiques.

6.1.4.2 Cartes et bandes perforées

1re mesure: Les conditions de stockage sont à contrôler, en particulier l'humidité de l'air.
2e mesure: les cartes et bandes perforées sont à copier régulièrement.
3e mesure: Il est recommandé de conserver une copie sur un support plus sûr.

6.2 Destruction ou falsification des données dues à un traitement erroné

1re mesure fondamentale: Des copies régulières des bases de données et l'inscription immédiate des modifications survenues – tenue d'un journal ou d'un *log* – permettent de rétablir les bases de données actuelles.

[3] RS ≙ recueil systématique des textes légaux fédéraux

Il faut tendre vers des méthodes qui fixent automatiquement chaque modification sur un support de données indépendant de la base de données. De tels fichiers «log» peuvent être utilisés pour mettre à jour les copies conservées lors de la perte des données originales.
Si les bases de données originales sont complétées ou modifiées par d'autres données traitées et contrôlées issues d'autres supports, ces dernières peuvent être intégrées dans les fichiers «log».
Les processus programmés peuvent également être remplacés par des indications inscrites sur du papier. Celles-ci doivent donner les renseignements concernant toutes les modifications effectuées. Des directives de travail obligatoires doivent assurer que ces renseignements sont sans lacunes.

2e mesure fondamentale: la plausibilité et la validité de toute la base de données sont à contrôler régulièrement. C'est par ce moyen que l'on détectera les erreurs qui se sont glissées malgré les autres mesures de sécurité. Les erreurs ainsi mises en évidence doivent faire l'objet de procès-verbaux donnant les informations sur les sources de l'erreur et sur sa correction, ainsi que sur les mesures qui sont touchées, pour éviter, dans l'avenir, ce type de faute.
Il faut ménager des redondances dans les données mémorisées afin de pouvoir dépister des modifications. Par exemple: somme de contrôle des fichiers, «bits» de parité.

6.2.1 Destruction involontaire par l'utilisateur

1re mesure: le personnel doit être formé avec soin et utiliser des indications d'utilisation claires et complètes.
2e mesure: les programmes doivent être conçus de telle manière qu'il est exclu que les données soient détruites par une faute de l'utilisateur.
3e mesure: l'accès aux bases de données et à leur modification sont à séparer des autres parties des programmes.
4e mesure: les opérations qui mettent les bases de données en danger, comme par exemple l'effaçage volontaire de données, ne doivent être effectuées que par des utilisateurs particulièrement qualifiés.
Les mesures, décrites en 6.1, pour lutter contre la perte de données en cas de destruction du support informatique, peuvent également aider, dans les cas extrêmes, à lutter contre ces dangers.

6.2.2 Falsification volontaire par l'utilisateur

1re mesure: des contrôles généraux, aussi appelés tests de plausibilité, doivent être intégrés dans les programmes et permettre d'empêcher l'utilisateur de travailler avec des données erronées.
2e mesure: les utilisateurs n'ont pas accès aux programmes en langage original.
Les programmes en langage original (programmes source) donnent la clef des tests de plausibilité prévus. Avec leur connaissance, il serait possible de trouver des lacunes dans les contrôles et de les utiliser de manière préméditée.
3e mesure: la documentation concernant un programme doit être divisée en une documentation spécifique à la maintenance du programme et une documentation destinée à l'utilisateur.
4e mesure: le développement et l'application des programmes doivent être séparés de manière stricte.
5e mesure: il doit être possible de retrouver en tout temps sur le fichier «log», sur la base des mots de passe personnels, quel utilisateur a effectué telle modification et avec quelle version de quel programme.
Il faut promouvoir l'inscription d'annotations programmées *et* rédigées sur papier, archivées sans lacunes et de manière ordrée et permettant ce type de recherche.

6.2.3 Destruction ou falsification provenant de l'extérieur

1re mesure: l'accès à l'installation doit être contrôlé.
Les places de travail liées à l'installation et à l'accès à celle-ci doivent être surveillées depuis des places de travail occupées en permanence.
2e mesure: l'accès à distance aux installations, doit être régi par des mots de passe et des procédures d'identification, afin d'écarter les personnes non autorisées.

6.2.4 Destruction due à une force externe agissant sur l'installation

1re mesure: les installations doivent être conçues de telle manière qu'elles soient protégées au maximum contre les effets extérieurs. Les locaux concernés doivent pouvoir être fermés.
2e mesure: l'alimentation électrique doit être assurée, pour la climatisation également, si elle existe. Si nécessaire, il faut empêcher que des interruptions de courant électrique entraînent des dégâts.

6.2.5 Falsification par traitement correct de données initiales fausses

1re mesure: il faut contrôler, lors du traitement, que les données sont saisies sur les bons supports, c'est à dire sur les supports qui contiennent les données à jour.
Il faut, avant tout, promouvoir des contrôles qui peuvent être intégrés aux programmes. D'autre part, il faut mettre en place des mesures d'organisation qui empêchent que des données dépassées soient traitées à la place des données actuelles.

6.2.6 Destruction ou falsification dues à un disfonctionnement de l'installation

1re mesure: un disfonctionnement dans l'installation doit être dépisté par le système de gestion et ne doit pas conduire à la perte ou à la falsification des données.
Comme exemple: «read after write», test de parité et autres.

6.2.7 Destruction ou falsification dues à des erreurs dans les programmes

1re mesure: les programmes de traitement des données et les programmes de gestion de la banque de données sont à séparer. Dans les derniers, il faut envisager des tests de plausibilité complets.
On ne peut pas encore assurer aujourd'hui que les gros programmes sont exempts de fautes. Pour augmenter la sécurité des données, les programmes doivent être conçus par blocs, d'une part ceux qui accèdent et modifient les données enregistrées et d'autre part ceux qui traitent ces données. Les derniers ne sont pas problématiques du point de vue de la sécurité des données. Les programmes qui accèdent aux données enregistrées doivent être encore divisés en parties, qui ne font que lire – ils ne mettent pas les données en danger – et celles qui modifient ou qui effacent. De programmes uniquement lecteurs ne sont critiques que dans les systèmes à utilisateurs multiples où les données lues doivent être protégées contre des altérations pendant la transaction.
La validité des banques de données doit être maintenue, même lors d'événements inhabituels comme, par exemple, une coupure de courant électrique.
2e mesure: les modifications de la base de données doivent être structurées en transactions qui amènent la base de données d'un état de validité à un nouvel état de validité.
3e mesure: les transactions doivent être menées de telle manière que les phases intermédiaires non valides ne soient que passagères et qu'elles ne soient absolument pas accessibles aux autres utilisateurs.
4e mesure: si une procédure entraîne une modification (transaction) dans la base de données, il doit être assuré, qu'en cas d'interruption de la procédure, soit la modification a été menée à bien, soit pas du tout, c'est-à-dire que toute modification commencée est annulée avec retour à l'état antérieur.
5e mesure: les programmes doivent être entièrement examinés par l'autorité de surveillance avant leur acceptation dans la mensuration officielle.
L'autorité de surveillance peut déléguer cet examen à d'autres instances. Dans l'optique de la sécurité des données, l'examen des parties de programmes qui modifient les données est particulièrement important.
6e mesure: Il faut édicter des directives pour l'élaboration des programmes.
Des directives de programmation facilitent l'examen et la maintenance des programmes. Les autorités de surveillance doivent veiller à ce que les directives sont bien en possession des adjudicataires de tâches de programmation.

6.3 Accès impossible aux données par panne des mécanismes d'accès

Ce n'est pas seulement lorsque les données ont disparu d'un support de données qu'elles sont perdues, mais c'est aussi lorsque les installations, qui étaient capables de lire ces supports, ne fonctionnent ou n'existent plus.

1re mesure fondamentale: les données doivent, au moins pour les copies de sécurité, être sur des supports standards dans des formats standards. A ce propos, des normes pour l'organisation des interfaces doivent être suivies.

Les installations et les supports de données qui ne permettent pas un transfert de données sur des supports standardisés, n'offrent pas une sécurité suffisante.

6.3.1 Accès impossible par perte du logiciel d'accès

1re mesure: des copies de sécurité concernant le logiciel doivent aussi être faites et stockées de manière séparée

2e mesure: la documentation des programmes doit contenir toutes les indications qui permettent, le cas échéant, de rétablir les programmes permettant la lecture des données.

6.3.2 Accès impossible dû à la panne des installations d'accès

1re mesure: la maintenance des installations doit être assurée par contrat.

2e mesure: il faut rechercher à ce que les données puissent également être lues sur une autre installation voisine. L'utilisation de cette installation ‹étrangère› doit être convenue à l'avance avec son propriétaire. Le logiciel nécessaire à cette opération doit être élaboré et testé régulièrement.

6.3.3 Accès impossible à cause du personnel

1re mesure: les programmes pour le traitement des données doivent être documentés de telle manière à ce que toute personne initiée à l'informatique puisse les mettre en marche.

2e mesure: en plus d'une organisation interne des remplaçants du personnel, il faut prévoir des mesures équivalentes à l'aide de personnel externe.

6.4 Dangers envisageables

[1] Les dommages ne se produisent pas seulement à cause d'événements isolés. Il faut également considérer des combinaisons d'événements malheureux.

[2] Les mesures prises doivent au moins contrer les combinaisons d'événements malheureux suivants:

A) Perte des données par destruction du support de données
- due à un dommage élémentaire ou
- par destruction
  - par un tiers ou
  - par le personnel propre,

combiné avec
accès impossible aux données dû à la panne des mécanismes d'accès
- à cause d'une défaillance des programmes et/ou
- à cause d'une panne de l'installation.

Pour la remise sur pied, il faut compter également avec une désaffection du personnel.

B) Destruction accidentelle des données
simultanée avec
non-fonctionnement des programmes

C) Destruction des données par manipulation erronée simultanée avec
accès impossible aux données par panne des mécanismes d'accès. Les deux étant provoqués soit par la destruction de l'installation ou le non-fonctionnement des programmes.

7. Description des domaines de responsabilité

[1] Pour se protéger contre des dommages, il est important de définir clairement l'étendue des diverses responsabilités. Dans ce qui suit, les domaines de responsabilité et les fonctions y relatives sont décrites.

[2] Le document de sécurité des données de chaque installation (voir chiffre 6.) pose par écrit et de manière fixe les domaines de responsabilité. En plus, chaque fonction est attribuée à une personne responsable. Il faut décrire en détail tout domaine de responsabilité qui s'écarterait de la norme.

Pour les dommages, dus à la perte ou à la falsification des données, c'est, vis-à-vis de l'extérieur, le géomètre ingénieur breveté adjudicataire, éventuellement la firme de mensuration, qui est responsable. Les prétentions dues à la responsabilité légale peuvent être diminuées s'il peut être prouvé après coup que les précautions exigibles avaient été prises.

Pour la réparation des dommages, c'est au géomètre à œuvrer lui-même. A la rigueur, il peut se retourner contre un employé coupable. La fonction des autorités de surveillance du canton et de la confédération est indiquée dans les lois, en particulier dans l'IAMP 1919 SR 211.432.23. Cette fonction ne peut pas être traitée par une norme.

7.1 L'ingénieur-géomètre responsable

[1] Il est globalement responsable du respect des prescriptions légales et des mesures prévues par cette norme. En particulier, il doit:

A) établir le document de sécurité et le contrôler régulièrement,

B) délimiter les domaines de responsabilité,

C) distribuer aux collaborateurs aptes à les recevoir, les diverses fonctions définies plus loin (voir 6.1.2.2[1]),

D) instruire correctement ses collaborateurs et contrôler l'application des instructions (6.1.2.2[2], 6.2.1[1]),

E) régler la question des suppléances des postes de travail (6.3.3[2]).

Dans l'annexe 2, un exemple issu de la pratique est donné. Voir aussi l'annexe 1.

7.2 Fonction: sécurité des données à long terme

[1] Cette fonction contient les mesures 6.1, 6.1.1(1), 6.1.1(2), 6.1.2.2(2), 6.1.3(2), 6.1.4, 6.1.4.1, 6.1.4.2, 6.2(2), 6.3, 6.3.1, 6.3.2(2).

On considère ici toutes les mesures (surtout périodiques) indispensables à la sécurisation des données à long terme.

7.3 Fonction: sécurité permanente

[1] Cette fonction comprend les mesures 6.1.1(1), 6.1.2.1(1), 6.1.2.2(2), 6.1.3, 6.1.4, 6.1.4.1, 6.1.4.2, 6.2(1), 6.2.2(5), 6.2.3, 6.2.4, 6.2.5, 6.3.1(1).

On considère ici les mesures qui protègent les données contre une perte dans l'utilisation journalière. Il lui appartient en particulier de contrôler que les supports de données sont rangés avec ordre.

7.4 Fonction: entretien de l'installation

[1] Cette fonction comprend les mesures 6.1.3(3), 6.3.2(1).

La personne apte, choisie pour cette fonction, opère elle-même l'entretien ou le supervise.

Pour l'entretien des installations, il est conseillé de passer des contrats complémentaires à long terme avec le constructeur, respectivement avec le représentant.

7.5 Fonction: élaboration et maintenance des programmes

[1] Cette fonction comprend les mesures suivantes: 6.2, 6.2.1, 6.2.2, 6.2.5, 6.2.6, 6.2.7, 6.3.1(1), 6.3.3(1).

Ces mesures doivent être considérées lors de la création et de l'élaboration des programmes. Par l'examen des programmes, ceci sera contrôlé.

7.6 Fonction: utilisation de programmes ‹dangereux›

[1] La personne apte qui exerce cette fonction obtient le droit d'utiliser des programmes dangereux au sens de 6.2.1(4).

[2] Elle doit être instruite des dangers spécifiques et formée de manière particulièrement soignée (6.2.2[5]).

[3] Elle touche les mesures 6.1.3(2), 6.1.3(3).

Certains programmes, en particulier des routines du système d'exploitation, peuvent rendre inutilisables des fichiers entiers (par effacement, par exemple).

Ces programmes ne contiennent aucune sécurité contre un emploi erroné; ils ne doivent pas être disponibles sans restriction, mais être réservés aux personnes spécialement formées.

7.7 Fonction: utilisation des programmes qui modifient les données

[1] Cette fonction comprend le droit d'utiliser des programmes qui modifient la base de données.

[2] Pour cette fonction, il faut considérer des collaborateurs instruits et expérimentés, qui sont également formés pour agir dans des cas spéciaux.
[3] Elle touche les mesures 6.1.3(2), 6.1.3(3), 6.2(1), 6.2.2(5).
Les programmes de cette catégorie servent à modifier certaines données isolées; les fautes de manipulations, rendant sous contrôle du programme inutilisables une grande partie des données, sont rendues impossibles.

7.8 Fonction: utilisation de programmes qui lisent des données

[1] Les personnes aptes, qui exercent cette fonction, ont l'autorisation d'utiliser les programmes qui lisent mais ne modifient pas les données.

[2] Ces collaborateurs doivent être instruits exactement et contrôlés régulièrement. Le danger de manipulations erronées éventuelles doit être porté à leur attention.

Annexes

1. Exemple d'un document de sécurité
2. Tableau des rapports entre mesures et fonctions
3. Exigences de qualité pour les supports de données
4. Conditions environnementales pour la conservation de supports de données