Entwurf zu einer künftigen Norm Datensicherung in der amtlichen Vermessung

Autor(en): **Frank, A. / Höhn, U.**

Objekttyp: **Article**

Zeitschrift: **Vermessung, Photogrammetrie, Kulturtechnik : VPK = Mensuration, photogrammétrie, génie rural**

Band (Jahr): **79 (1981)**

Heft 9

PDF erstellt am: **27.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-230680

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[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:

N. 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

Nr.		Stichwort	7.1 Verantwortlicher Ingenieur-Geometer	7.2 langfristige Datensicherung	7.3 büroninterne 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		*Unzugänglichkeit der Daten durch Ausfall ddr Zugriffsmechanismen*								
	(1)	Kopieren in Standard-Format auf Standard-Datenträger		X						
6.3.1		*Unzugänglichkeit durch Verlust der zugreifenden Software*								
	(1)	Auch Software und Dokumentation kopieren		X	X		X			
6.3.1	(2)	Beschreibung, wie Daten zu lesen sind		X			X			
6.3.2		*Unzugänglichkeit durch Störungen an der zugreifenden Hardware*								
	(1)	Wartung der Anlage sicherstellen				X				
6.3.2	(2)	Ausweichanlage vorbereiten		X						
6.3.3		*Unzugänglichkeit durch Ausfall von Personal*								
	(1)	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 Buch geführt, wo auch abnormale Erscheinungen notiert werden
	(3)	Abnormale Erscheinungen	

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

6. 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.

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

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.