



dsb

datenschutzbeauftragte
des kantons zürich

Leitfaden

Informationssicherheit in Volksschulen

Inhalt

1	Einleitung	2
2	Übersicht Dokumente	2
3	Umsetzung der Anforderungen an die Informationssicherheit	3
3.1	Schritt 1: Sicherheitsstrategie festlegen.....	4
3.2	Schritt 2: Organisationsstruktur für Informationssicherheit aufbauen.....	4
3.3	Schritt 3: Schutzbedarf festlegen.....	4
3.3.1	Inventar der Fachanwendungen erstellen.....	4
3.3.2	Anwendungsverantwortliche bestimmen.....	5
3.3.3	Schutzbedarf der Fachanwendungen festlegen.....	5
3.4	Schritt 4: Sicherheitsmassnahmen planen.....	5
3.4.1	Sicherheitsmassnahmen den Verantwortlichen zuweisen.....	5
3.4.2	Basis-Sicherheitscheck vornehmen.....	6
3.4.3	Umsetzung der Sicherheitsmassnahmen planen.....	6
3.4.4	Revision planen.....	6
3.5	Schritt 5: Fehlende Sicherheitsmassnahmen umsetzen.....	7
3.5.1	Weisungen für die Mitarbeitenden erstellen.....	7
3.5.2	Sensibilisierung der Mitarbeitenden planen.....	7
3.5.3	Rollen- und Berechtigungskonzept erstellen.....	7
4	Kontinuierliches Erhalten des Informationssicherheitsniveaus	8
4.1	Regelmässige Überprüfung der Umsetzung der Massnahmen.....	8
4.2	Regelmässige Überprüfung der Massnahmen.....	8
5	Links	8

1 Einleitung

Die Digitalisierung durchdringt sämtliche Lebensbereiche und eine Informationsbearbeitung ohne IT-Unterstützung ist nicht mehr denkbar. Die Risiken nehmen zu und Angriffe auf Systeme häufen sich. Ein bewusster und strukturierter Umgang mit den Themen Informationssicherheit und Datenschutz ist deshalb notwendig. Ein Risikomanagement, klare Weisungen und gute Schutzmassnahmen helfen, die Risiken einzuschränken.

Dieser Leitfaden richtet sich an die Volksschulen des Kantons Zürich und hilft bei der Einführung, Umsetzung und Pflege einer nachhaltigen Informationssicherheit. Er enthält eine Übersicht der vom Gesetz über die Information und den Datenschutz (IDG, [LS 170.4](#)) geforderten Massnahmen zur Informationssicherheit sowie eine Einführung, wie diese umgesetzt werden. Weiter werden die von der Datenschutzbeauftragten (DSB) zur Verfügung gestellten Anleitungen und Vorlagen erläutert.

Das Vorgehen, die Massnahmen und die damit verbundenen Empfehlungen richten sich nach dem international anerkannten Standard des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI).

2 Übersicht Dokumente

Für eine umfassende und integrale Informationssicherheit müssen die erforderlichen Informationssicherheitsdokumente auf der strategischen, taktischen und operativen Ebene erstellt werden. Die nachfolgende Pyramide zeigt die entsprechende Gliederung und Zuweisung der Dokumente in den verschiedenen Ebenen. Idealerweise werden die Dokumente im Top-Down-Ansatz (von oben nach unten) erstellt.

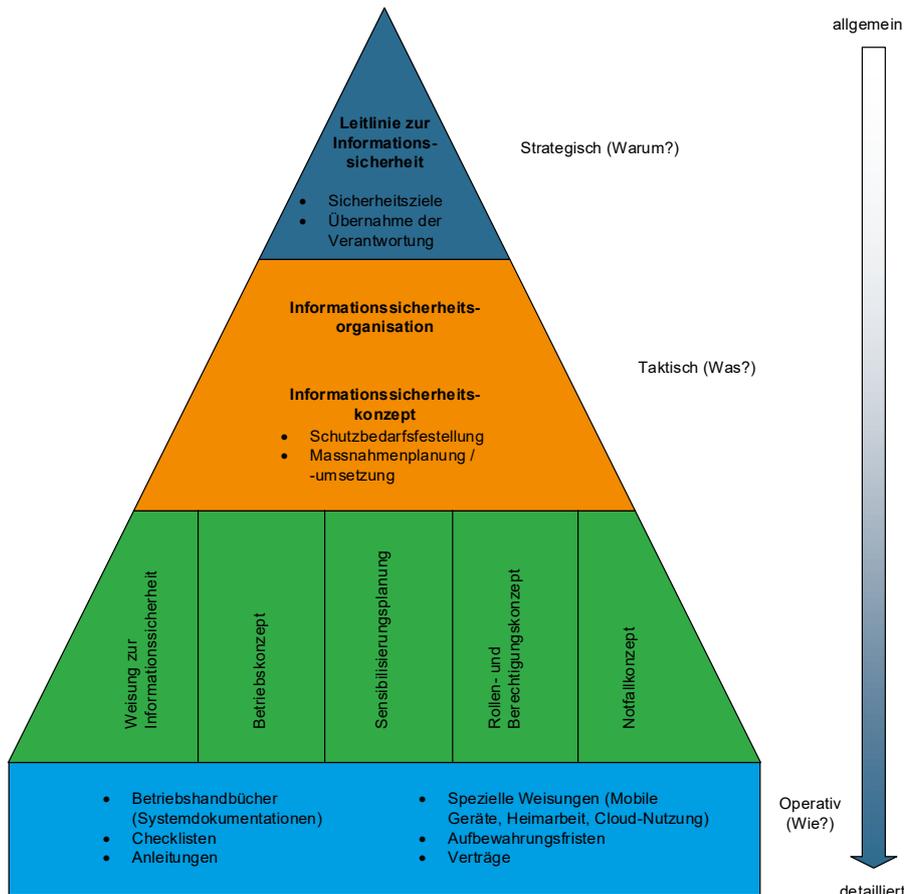


Abbildung 1 – Sicherheitspyramide Übersicht Dokumente Informationssicherheit

Für die Erstellung und Einführung der nötigen Leitlinien, Weisungen und Konzepte stehen folgende Dokumente zur Verfügung.

Dokumente	Thema
Leitfaden	– <u>Informationssicherheit in Volksschulen</u>
Anleitungen	– <u>Sensibilisierung der Mitarbeitenden für Informationssicherheit in Volksschulen</u>
Vorlagen	– <u>Erklärung zur Informationssicherheit in Volksschulen</u> – <u>Leitlinie zur Informationssicherheit in Volksschulen</u> – <u>Rollen- und Berechtigungskonzept in Volksschulen</u> – <u>Schutzbedarfsfeststellung Fachanwendungen in Volksschulen</u> – <u>Weisung zur Informationssicherheit in Volksschulen</u>
Checklisten	– <u>Minimummassnahmenkatalog</u>
Glossar / Abkürzungsverzeichnis	– <u>Glossar und Abkürzungen Informationssicherheit</u>

3 Umsetzung der Anforderungen an die Informationssicherheit

Informationssicherheit ist eine Aufgabe aller Mitarbeitenden von Schulen und der Mitglieder von Behörden über alle Hierarchiestufen hinweg. Je nach interner Organisation können sich die Zuständigkeiten bei der Umsetzung der Informationssicherheit unterscheiden. Die oberste Leitung trägt die Verantwortung, legt entsprechende Abläufe fest und kann Verantwortliche für die Informationssicherheit bestimmen.

Die Umsetzung der Anforderungen an die Informationssicherheit in Volksschulen erfolgt in fünf Schritten:

1. Sicherheitsstrategie festlegen
2. Organisationsstruktur für Informationssicherheit aufbauen
3. Schutzbedarf festlegen
 - a) Inventar der Fachanwendungen erstellen
 - b) Anwendungsverantwortliche bestimmen
 - c) Schutzbedarf der Fachanwendungen festlegen
4. Sicherheitsmassnahmen planen
 - a) Sicherheitsmassnahmen den Verantwortlichen zuweisen
 - b) Basis-Sicherheitscheck vornehmen
 - c) Umsetzung der Sicherheitsmassnahmen planen
 - d) Revision planen
5. Fehlende Sicherheitsmassnahmen umsetzen

3.1 Schritt 1: Sicherheitsstrategie festlegen

Die Sicherheitsstrategie, das angestrebte Sicherheitsniveau sowie die für die Volksschule gültigen Sicherheitsziele müssen definiert und festgehalten werden. Die DSB stellt eine Vorlage für eine Leitlinie zur Informationssicherheit in Volksschulen zur Verfügung.

Was ist zu tun:

1. Layout der Vorlage Leitlinie zur Informationssicherheit an das eigene Corporate Design anpassen
2. Inhalt überprüfen und ergänzen
3. Leitlinie durch einen Beschluss [des VERANTWORTLICHEN GREMIUMS] der Exekutive in Kraft setzen
4. Leitlinie allen Mitarbeitenden kommunizieren und an einem für diese zugänglichen Ort publizieren

3.2 Schritt 2: Organisationsstruktur für Informationssicherheit aufbauen

Um das von der Schule angestrebte Sicherheitsniveau zu erreichen, muss ein Informationssicherheitsprozess definiert, dokumentiert und umgesetzt werden. Zu diesem Zweck müssen eine Organisationsstruktur aufgebaut, die Rollen festgelegt und den Rollen die Aufgaben zugeordnet werden.

Eine mögliche Regelung ist in der Leitlinie zur Informationssicherheit in Volksschulen dokumentiert.

Was ist zu tun:

1. Rollenträgerinnen und -träger definieren und kommunizieren
2. Aufgaben in die Stellenbeschreibungen integrieren
3. Ressourcen den Rollenträgerinnen und -trägern zuweisen
4. Ausbildungsmassnahmen durchführen

3.3 Schritt 3: Schutzbedarf festlegen

Mit der Schutzbedarfsfeststellung gemäss Verordnung über die Informationsverwaltung und -sicherheit (IVSV, LS 170.8) werden den Risiken angemessene Sicherheitsmassnahmen festzulegen. Dazu sind die folgenden Schritte notwendig.

3.3.1 Inventar der Fachanwendungen erstellen

Für die Schutzbedarfsermittlung sind alle Fachanwendungen zu erheben und zu inventarisieren, welche die Erfüllung oder Unterstützung bestimmter Aufgaben ermöglichen (siehe Vorlage Schutzbedarfsfeststellung Fachanwendungen in Volksschulen):

Ni	Zweck	Anwendungsname
1	Personalverwaltung	PULS-ZH
2	Kreditoren und Debitoren	RufGesoft
3	Internetauftritt	CMS iWeb

Abbildung 2 - Beispiel Inventar Fachanwendungen

Was ist zu tun

- Liste der Fachanwendungen erstellen

3.3.2 Anwendungsverantwortliche bestimmen

Für alle Fachanwendungen beziehungsweise Informationen muss festgelegt werden, wer für ihre Sicherheit verantwortlich ist. Die Aufgaben der Anwendungsverantwortlichen finden sich in der [Leitlinie zur Informationssicherheit in Volksschulen](#).

Was ist zu tun:

1. Interne Verantwortliche bestimmen und dokumentieren
2. Externe Verantwortliche dokumentieren (zum Beispiel Auftragnehmende)
3. Datenstandort dokumentieren (intern / extern)

3.3.3 Schutzbedarf der Fachanwendungen festlegen

Für jede der dokumentierten Fachanwendungen ist der Schutzbedarf zu bestimmen (siehe [Vorlage Schutzbedarfsfeststellung Fachanwendungen in Volksschulen](#)):

Ni	Zweck	Anwendungsname	Vertraulichkeit	Integrität	Verfügbarkeit	Intern
1	Personalverwaltung	PULS-ZH	H	N	N	Schulverwaltung
2	Kreditoren und Debitoren	RufGesoft	N	H	N	Schulverwaltung
3	Internetauftritt	CMS iWeb	N	N	N	IT-Verantwortlicher

Abbildung 3 - Beispiele Inventar Fachanwendungen mit entsprechender Schutzbedarfsfeststellung

Schutzbedarfskategorien	
Normal	
Verstoß gegen Gesetze / Vorschriften/Verträge	Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen. Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der B seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnisse beeinträchtigt werden kann.
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung erscheint nicht möglich.
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt wer

Abbildung 4 - Beispiel Schutzbedarfskategorien

Was ist zu tun:

1. Schutzbedarfskategorien überprüfen und ergänzen
2. Einstufung der Fachanwendungen in Bezug auf die Vertraulichkeit, Verfügbarkeit und Integrität anhand der Schutzbedarfskategorien überprüfen und anpassen

3.4 Schritt 4: Sicherheitsmassnahmen planen

Zur Planung von Sicherheitsmassnahmen stellt die DSB einen [Minimummassnahmenkatalog](#) zur Verfügung.

3.4.1 Sicherheitsmassnahmen den Verantwortlichen zuweisen

Sicherheitsmassnahmen werden nur plangemäss umgesetzt, wenn die Verantwortlichkeiten festgelegt sind. Diese können im [Minimummassnahmenkatalog](#) in der Spalte «Verantwortung» dokumentiert werden.

Was ist zu tun:

- Für jede Massnahme ist die oder der für die Umsetzung verantwortliche Mitarbeitende beziehungsweise Auftragnehmende einzutragen.

3.4.2 Basis-Sicherheitscheck vornehmen

Beim Basis-Sicherheitscheck wird geprüft, ob die Massnahmen umgesetzt wurden oder ob Sicherheitsmassnahmen fehlen. Der Sicherheitsstatus wird anhand von Unterlagen, Gesprächen mit Verantwortlichen sowie stichprobenartigen Überprüfungen vor Ort ermittelt.

Werden Dienstleistungen durch externe Auftragnehmer erbracht, ist die Schule dafür verantwortlich, dass die erforderlichen Sicherheitsmassnahmen umgesetzt sind. Bei Unklarheiten bezüglich der Ermittlung des Sicherheitsstatus ist die DSB zu kontaktieren.

Im Minimummassnahmenkatalog stehen vier Möglichkeiten zur Verfügung, um den Umsetzungsgrad der Massnahmen zu dokumentieren:

- ja, wenn alle in der Massnahme genannten Anforderungen vollständig umgesetzt sind,
- teilweise, wenn einige, aber nicht alle Anforderungen umgesetzt sind,
- nein, wenn keine oder nahezu keine der Anforderungen umgesetzt sind,
- entbehrlich, wenn die Massnahme nicht benötigt wird, weil mindestens gleichwertige alternative Massnahmen umgesetzt wurden oder weil das zu schützende Objekt nicht vorhanden ist.

Jeder Massnahme ist eine eindeutige Nummer zugeordnet (zum Beispiel ISMS.1.A1). In einer Internetsuchmaschine kann durch die Eingabe dieser Nummer die vollständige Beschreibung der Massnahme aufgerufen werden. Aufgrund der enthaltenen Prüffragen kann der Status der Massnahme ermittelt werden.

In der Spalte «Umsetzungstermin» kann festgehalten werden, bis wann die Massnahme umgesetzt werden muss.

Was ist zu tun:

1. Status der Massnahmen bestimmen und dokumentieren.
2. Wird bei einer Massnahme der Status «entbehrlich» gewählt, so ist dies im Feld «Bemerkung» zu begründen.
3. Im Feld «Nachweisdokument» ist auf das Dokument, in dem die Massnahme beschrieben ist, zu verweisen.
4. Im Feld «betroffene IT-Systeme» sind die Systeme einzutragen, für die die Massnahme anwendbar ist.

3.4.3 Umsetzung der Sicherheitsmassnahmen planen

Was ist zu tun:

1. Umsetzungstermin festlegen, falls die Massnahme noch nicht oder nur teilweise umgesetzt ist
2. Bei Bedarf zusätzlich Priorität und Kosten eintragen

3.4.4 Revision planen

Bei der Durchführung von Revisionen kann der Minimummassnahmenkatalog zur Unterstützung beigezogen werden. Bei jeder Massnahme kann der Termin der letzten und der nächsten Revision sowie die verantwortliche Revisorin beziehungsweise der verantwortliche Revisor dokumentiert werden. Der Status der Massnahmen sollte mindestens alle drei Jahre überprüft werden.

Was ist zu tun:

- Termin für Revision festlegen

3.5 Schritt 5: Fehlende Sicherheitsmassnahmen umsetzen

Bei der Umsetzung sind die folgenden Massnahmen prioritär zu behandeln.

3.5.1 Weisungen für die Mitarbeitenden erstellen

Die DSB stellt die Vorlage Weisung zur Informationssicherheit in Volksschulen zur Verfügung. Sie kann als Grundlage für die Weisung für die Mitarbeitenden verwendet werden.

Was ist zu tun:

1. Layout der Vorlage Weisung zur Informationssicherheit an das eigene Corporate Design anpassen
2. Inhalt überprüfen und ergänzen
3. Weisung durch die zuständige Leitung (z.B. Schulpflege) in Kraft setzen
4. Weisung den Mitarbeitenden kommunizieren und allenfalls mit Unterschrift bestätigen lassen (siehe Erklärung zur Informationssicherheit)
5. Weisung an einem für alle Mitarbeitenden zugänglichen Ort publizieren

3.5.2 Sensibilisierung der Mitarbeitenden planen

Sensibilisierungsmassnahmen müssen geplant und umgesetzt werden. Die Anleitung ist im Dokument Sensibilisierung der Mitarbeitenden für Informationssicherheit in Volksschulen enthalten.

Was ist zu tun:

1. Bedürfnisse betreffend Sensibilisierungsmassnahmen abklären
 2. Massnahmen planen und umsetzen
- Anleitung BSI Baustein ORP.3 Sensibilisierung und Schulung zur Informationssicherheit

3.5.3 Rollen- und Berechtigungskonzept erstellen

Die DSB stellt die Vorlage Rollen- und Berechtigungskonzept in Volksschulen zur Verfügung.

Was ist zu tun:

- Rollen- und Berechtigungskonzept an die Bedürfnisse anpassen
- Anleitung BSI Baustein ORP.4 Identitäts- und Berechtigungsmanagement

4 Kontinuierliches Erhalten des Informationssicherheitsniveaus

Die Informationssicherheit ist ein fortlaufender Prozess. Um das Informationssicherheitsniveau erhalten zu können, sind die Massnahmen sowie deren Status regelmässig zu überprüfen und bei Bedarf anzupassen.

4.1 Regelmässige Überprüfung der Umsetzung der Massnahmen

Der Stand der Umsetzung muss regelmässig überprüft werden und die zuständige Stelle (zum Beispiel die / der Informationssicherheitsverantwortliche) ist über das Ergebnis zu informieren.

4.2 Regelmässige Überprüfung der Massnahmen

Die Erkenntnisse aus sicherheitsrelevanten Zwischenfällen, Veränderungen im technisch-organisatorischen Umfeld sowie Änderungen von Sicherheitsanforderungen erfordern eine Anpassung der bestehenden Sicherheitsmassnahmen.

Deshalb sollten die Massnahmen mindestens jährlich respektive immer, wenn sich das Umfeld verändert, überprüft und angepasst werden.

Anleitung BSI Baustein ISMS.1 Sicherheitsmanagement

5 Links

- [Sicherheitsthemen benutzerfreundlich erklärt](#)
- [Anleitung für das Erstellen eines IT-Sicherheitskonzepts nach IT-Grundschutz, detaillierte Massnahmenbeschreibungen](#)
- [Anwendung zur Überprüfung der Sicherheit von Passwörtern](#)

V 1.4 / Oktober 2022