



Leitlinie Informationssicherheit

A-050

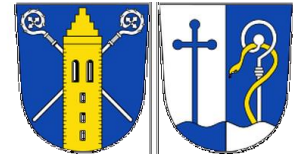
Verweise auf

A-060 Zieleplan

A-090 ISMS-Team

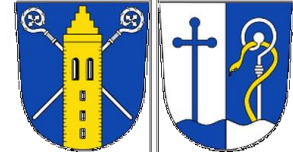
F-010 Sicherheitskonzept

A-130 Organisationsplan



Inhalt

1. Stellenwert der Informationssicherheit	3
2. Geltungsbereich der Informationssicherheitsleitlinie	3
3. Zielsetzungen	4
4. Bezug der Informationssicherheit zu den Aufgaben	4
5. Kernelemente der Sicherheitsstrategie	4
6. Verpflichtung zur Umsetzung	5
7. Verpflichtung zur kontinuierlichen Verbesserung (PDCA)	6
8. Aktualisierung der Leitlinie Informationssicherheit	6
9. Inkraftsetzung	7



1. Stellenwert der Informationssicherheit

Die Verwaltungsgemeinschaft IImmünster besitzt eine enorme Aufgabenvielfalt die permanenten Änderungen unterliegt. Eine wirtschaftliche, zeitnahe Aufgabenerfüllung stützt sich dabei zunehmend auf die Möglichkeiten der Informationstechnologie und ist für die Verwaltungsgemeinschaft IImmünster unabdingbar. Sie eröffnet völlig neue Möglichkeiten, die auch die Verwaltungsgemeinschaft IImmünster aktiv nutzt. In Abwägung der zu schützenden Werte, der gesetzlichen Anforderungen, Informationen und der damit verbundenen Risiken wird ein angemessenes Informationssicherheitsniveau geschaffen. Durch diese Informationssicherheitsleitlinie (ISL) wird die Übernahme der Gesamtverantwortung durch den Unterzeichner zum Ausdruck gebracht.

Informationssicherheit umfasst neben IT-Systemen auch Papierunterlagen in Form von Akten und sonstigen Papierunterlagen und Daten im allgemeinen Sinn. Sie umfasst die Summe aller organisatorischen, personellen und technischen Maßnahmen, um die Informationssicherheit zu gewährleisten. Somit ist jede*r Beschäftigte*r für die Informationssicherheit in seinem oder ihrem Zuständigkeitsbereich mitverantwortlich.

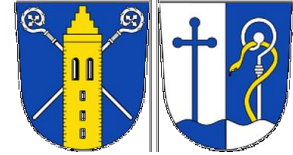
Modernes Handeln erfordert den Einsatz aktueller Informationstechnologien, um die Aufgabenerfüllung der Kommunalverwaltung im Sinne der Bürgerschaft, ortsansässiger Unternehmen oder weiterer Partner effizient und effektiv zu gestalten. Dies trifft auch auf die Verwaltungsgemeinschaft IImmünster zu. Beim Einsatz von Informationstechnologie muss darauf geachtet werden, dass der Sensibilität, der ihr übertragenen und von ihnen verarbeiteten Informationen und Daten, mit der nötigen Sorgfalt Rechnung getragen wird. Die Informationssicherheit ist eine unverzichtbare Grundlage für ein Handeln, dem die Bürgerschaft, die Unternehmen und alle Partner ihr Vertrauen schenken können. Daher muss sich die Verwaltungsgemeinschaft IImmünster dem Thema Sicherheit in der Informationstechnik in geeigneter Form stellen und die verarbeiteten Daten geeignet schützen.

2. Geltungsbereich der Informationssicherheitsleitlinie

Der Geltungsbereich der Informationssicherheitsleitlinie wird für den gesamten Tätigkeitsbereich der Verwaltungsgemeinschaft IImmünster folgendermaßen festgelegt:

- Das Rathaus der Verwaltungsgemeinschaft IImmünster in der Freisinger Straße 3 in 85304 IImmünster
- Der Bauhof VG IImmünster, Logenweg 15, 85276 Hettenshausen
- Das Rathaus der Gemeinde Hettenshausen, Hauptstraße 65, 85276 Hettenshausen
- Der gemeindliche Kindergarten Kreuzberg 2A in 85276 Hettenshausen
- Der gemeindliche Kindergarten Kirchberg 2, 85304 IImmünster
- Die Gemeindebücherei im Benefiziatenhaus, St.-Arsatius-Straße 4, 85304 IImmünster

Die Umsetzung der Maßnahmen (Scope für Prüfabnahme) zum gewählten Informationssicherheitsmanagementsystem (ISMS) wird bis zum geplanten Internen Wiederholungsaudit auf den zentralen Verwaltungsbereich (Rathaus) festgelegt.



3. Zielsetzungen

Für die Umsetzung der Informationssicherheit werden jährlich Ziele festgelegt. Diese werden im Dokument **A-060 Ziele Informationssicherheit** festgeschrieben.

4. Bezug der Informationssicherheit zu den Aufgaben

Es ist notwendig, das Zusammenspiel der Informationen, IT-Verfahren und Aufgaben sowie der Infrastruktur der Informationstechnik und Kommunikationskanälen ganzheitlich zu betrachten. Bei den Aufgaben der Verwaltungsgemeinschaft IImünster, intern und für Kunden, werden Informationen verarbeitet. Sowohl bei der Erbringung der Pflichtaufgaben als auch der Aufgaben, die Verwaltungsgemeinschaft IImünster auf freiwilliger Basis übernimmt, werden Informationen erhoben und verarbeitet, deren **Vertraulichkeit, Integrität** und **Verfügbarkeit** ein hohes Gut darstellen. Hierbei handelt es sich z. B. um Daten, die entsprechend gesetzlichen Anforderungen geschützt werden müssen, oder auch um wettbewerbsrelevante Informationen von Unternehmen, die Unberechtigten nicht bekannt werden dürfen.

Begriffserklärung:

Vertraulichkeit

Vertraulichkeit bedeutet Schutz vor unberechtigtem Einblick und Verrat von Informationen oder vertraulichen Daten.

Integrität

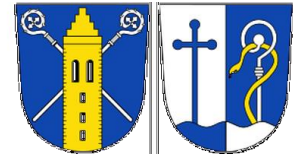
Integrität bezeichnet das durchgängige Funktionieren von IT-Systemen sowie die Vollständigkeit und Richtigkeit von Daten und Informationen. In Bezug auf die Informationssicherheit bedeutet Integrität das Verhindern von nicht genehmigten Veränderungen oder Löschen von wichtigen Informationen. Integrität von Daten kann man z. B. durch Verschlüsselung erreichen.

Verfügbarkeit

Verfügbarkeit definiert, zu welchem Grad IT-Systeme, IT-Anwendungen, IT-Netzwerke und elektronische Informationen einer oder einem Benutzer*in zur Verfügung stehen und ohne Einschränkung verwendet werden können.

5. Kernelemente der Sicherheitsstrategie

- Informationssicherheit ist für das Handeln der Verwaltungsgemeinschaft IImünster sehr wichtig.
- Jede*r Beschäftigte ist für Informationssicherheit verantwortlich. Die Informationssicherheit gehört zu den Dienstpflichten aller Beschäftigten. Nur wenn alle Beschäftigten ihre Verantwortung in der täglichen Arbeit wahrnehmen, kann ein geeignetes Niveau der Informationssicherheit erreicht werden.
- Dieses Dokument ist für alle Beschäftigten verbindlich und wird von dem Gemeinschaftsvorsitzendem und der Behördenleitung voll unterstützt.



Als zentrale Sicherheitsinstanz ernennt der Gemeinschaftsvorsitzende eine*n Informationssicherheitsbeauftragte*n (ISB), der oder die für alle Belange, Fragen und Umsetzung der Informationssicherheit zuständig ist. Er oder Sie ist der Behördenleitung in dieser Rolle direkt unterstellt. Dem/Der ISB sind sowohl geeignete Qualifizierungsmaßnahmen als auch zeitliche Ressourcen zu ermöglichen, um seine oder ihre Verantwortung fachlich und zeitlich zu erfüllen. Ein Informationssicherheits-Managementsystem (ISMS) ist weiterhin im Einsatz und wird angepasst. In regelmäßigen Abständen ist zu prüfen, ob die ausgewählten Sicherheitsmaßnahmen noch ausreichend sind.

Die Verwaltungsgemeinschaft Ilimünster verankert das Thema Informationssicherheit in der Organisation. Eine vereinfachte Übersicht über die Geschäftsverteilung kann im Dokument **A-130 Organisationsplan** eingesehen werden.

Die Verwaltungsgemeinschaft Ilimünster verankert das Thema Informationssicherheit in

- einer geeigneten Informationssicherheitsorganisation, die aktiv das Thema Informationssicherheit betreibt - siehe **A-090 Informationssicherheitsteam**,
- klar formulierte Sicherheitsvorgaben in Form von Dienstanweisungen, die für alle Beschäftigten verbindlich sind,
- die Integration von Sicherheitsaspekten in alle aus Sicht der Informationssicherheit relevanten Prozesse,
- kontinuierliche und flächendeckende Sensibilisierungsmaßnahmen für alle Beschäftigten.

Die Verwaltungsgemeinschaft Ilimünster sorgt auch für eine Absicherung der IT-Infrastruktur durch Umsetzung geeigneter Sicherheitsmaßnahmen auf der Infrastrukturebene.

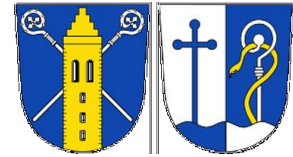
Personen und Unternehmen, die nicht zur Verwaltungsgemeinschaft Ilimünster gehören, für diesen aber Leistungen erbringen (Auftragnehmer), haben die Vorgaben des Auftraggebers zur Einhaltung der Informationssicherheitsziele gemäß dieser ISL einzuhalten. Der Auftraggeber informiert den Auftragnehmer über diese Regeln und verpflichtet ihn in geeigneter Weise zur Einhaltung (durch AVV = Auftragsverarbeitungsvertrag).

Sicherheitsanforderungen von übergeordnetem Interesse, für deren Umsetzung eine vertragliche oder gesetzliche Verpflichtung besteht, sind zu erfüllen. Entsprechende Vorschriften und Maßnahmen stellen den Mindeststandard bei der Formulierung interner Vorschriften und Maßnahmen dar.

6. Verpflichtung zur Umsetzung

Der/die Unterzeichner*in trägt die Gesamtverantwortung für die Informationssicherheit. Es obliegt ihr/ihm, für die Umsetzung der Maßnahmen zur Gewährleistung der Informationssicherheit zu sorgen und die dafür benötigten Ressourcen bereitzustellen. Die Verwaltungsgemeinschaft Ilimünster plant, sich für die Umsetzung von Informationssicherheit am Standard BSI Kommunalprofil zu orientieren.

Alle Beschäftigten sind verpflichtet, sorgfältig mit den zur Verfügung stehenden Informationen umzugehen und aktiv bei der Umsetzung der Maßnahmen zur Gewährleistung der Informationssicherheit mitzuwirken. Einzelne Maßnahmen zur Verbesserung des Sicherheitsniveaus



werden in Informationssicherheitsrichtlinien und Dienstanweisungen konkretisiert und umgesetzt. Erlassene Informationssicherheitsrichtlinien und Dienstanweisungen sind für alle Beschäftigten bindend.

Für bereits betriebene und geplante Informationstechnik ist eine Sicherheitskonzeption (**F-010 Sicherheitskonzept**) zu erstellen. Die sich daraus ergebenden Maßnahmen sind auch dann umzusetzen, wenn sich Beeinträchtigungen für die Nutzung ergeben. Der Verantwortliche hat bei Verstößen und Beeinträchtigungen die zur Aufrechterhaltung des Betriebes und der Informationssicherheit geeignete und angemessene Maßnahmen zu ergreifen. Die Sicherheitskonzeption wird von der oder dem ISB jährlich auf Aktualität und Wirksamkeit geprüft und bei Bedarf angepasst.

7. Verpflichtung zur kontinuierlichen Verbesserung (PDCA)

Der Gemeinschaftsvorsitzender verpflichtet sich die Optimierung der Informationssicherheit in die Geschäftsprozesse zu integrieren. Der Gemeinschaftsvorsitzender ist regelmäßig bzw. im Einzelfall akut über den aktuellen Sicherheitszustand durch den oder die ISB zu informieren und ist für die Absicherung der Kontinuität des Sicherheitsprozesses verantwortlich.

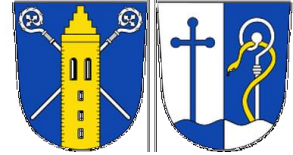
Der oder Die ISB ist bei allen organisatorisch-technischen Neuerungen oder Änderungen, die Auswirkungen auf die Informationssicherheit haben können, frühzeitig einzubinden. Verantwortlich für die Weiterentwicklung der ISL und der Sicherheitskonzeption ist der oder die ISB, wobei er oder sie von den Fachverantwortlichen bestmöglich unterstützt wird. Die Beschäftigten sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben.

Informationssicherheit ist kein unveränderlicher Zustand, sondern hängt von vielen internen und externen Begebenheiten und Einflüssen ab, wie z. B. neuen Bedrohungen, neuen Gesetzen oder auch der Entwicklung neuer technischer Lösungen, denen Rechnung getragen werden müssen.

8. Aktualisierung der Leitlinie Informationssicherheit

Das Sicherheitskonzept wird von der/dem ISB jährlich auf seine Aktualität und Wirksamkeit geprüft und bei Bedarf angepasst. Der Gemeinschaftsvorsitzender unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mögliche Verbesserungen oder Schwachstellen sind an den/die ISB weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der Sicherheitstechnik zu halten.



9. Inkraftsetzung

Die Informationssicherheitsleitlinie tritt mit Unterzeichnung in Kraft, ersetzt damit die bisherige Leitlinie und wird allen Beschäftigten nach Unterschrift umgehend zur Kenntnis gebracht.

Ilmünster, den 06.02.2024

Georg Ott,
Gemeinschaftsvorsitzender