STADT NIDAU

Konzept für das Management der Informationssicherheit und des Datenschutzes der Stadt Nidau

Vom Gemeinderat verabschiedet am 17. September 2024

Inhalt

Impressum

Dieses Konzept wurde erarbeitet von:

- Peter Fischer, Fischer Digitalisierung und Recht GmbH, Matthias Amgwerd und Rolf Graf
- Stephan Ochsenbein, Stadt Nidau, Stadtverwalter
- Manuela Jennings, Stadt Nidau, Abteilungsleiterin Zentrale Dienste
- Frederik Leyvraz, Stadt Nidau, IT-Koordinator

1. Ausgangslage, Zweck, Geltungsbereich

Die vom Gemeinderat am 29. November 2022 verabschiedete Digitalstrategie der Stadt Nidau formuliert u.a. den Grundsatz, dass die Stadt den Datenschutz und die Informationssicherheit frühzeitig bei der Umsetzung der digitalen Transformation berücksichtigt und deren Risiken identifiziert, systematisiert sowie mit angemessenen Massnahmen und Mitteln begegnet[1]. Cybervorfälle, die immer wieder auch Gemeinden betreffen, unterstreichen die Wichtigkeit eines bewussten und professionellen Umgangs mit den Cyberrisiken[2]. Dementsprechend hat die Stadt Nidau beschlossen, die nötigen Massnahmen zur Gewährleistung des Datenschutzes und der Informationssicherheit als elementaren Bestandteil der Digitalstrategie umzusetzen.

Das vorliegende Konzept richtet sich an alle Personen, die in der und für die Stadt Nidau Daten bearbeiten. Es stellt die von der Stadtverwaltung einschliesslich der Schulen bearbeiteten Informationen, deren Geschäftskontext, deren Schutzbedarf, die eingesetzten Informationssysteme, die relevanten Rollen und Prozesse sowie Massnahmen zur Informationssicherheit und zum Datenschutz dar. Das Konzept beschreibt die Organisation des Informations- und Datenschutzes in Nidau auch zuhanden der Aufsichtsbehörden.

Das Konzept ist nicht anwendbar auf die von der Stadt ausgelagerten Bereiche wie Ver- und Entsorgungsdienste. Die Stadt sorgt in jenen Bereichen dafür, dass die verantwortlichen Organisationen ihrerseits beauftragt sind, den Informations- und Datenschutz sicherzustellen.

2. Grundlagen

Für die Stadt Nidau gelten die kantonalrechtlichen Vorgaben, insbesondere das kantonale Datenschutzrecht[3] und das Organisationsrecht der Gemeinden des Kantons Bern. Auf Gemeindeebene gelten:

- Stadtordnung[4];
- Geschäftsordnung Stadtrat[5];
- Verwaltungsverordnung[6];
- Funktionendiagramm[7];
- Geververordnung[8] und GEVER-Weisung;
- Weisung über die Nutzung der Informatik[9]:

[1] Digitalstrategie der Stadt Nidau vom 29. November 2022, Ziff. 2.3, Digitalstrategie — Nidau
[2] Bsp.: Zollikofen November 2023: Gemeinde Zollikofen von Ransomware-Angriff lahmgelegt (inside-it.ch); Baden Oktober/Dezember 2023, Hackerangriff auf Baden: Über 24'000 Namen und Adressen der Bevölkerung im Darknet aufgetaucht | ArgoviaToday;
Übersicht des Nationalen Zentrums für Cybersicherheit: Aktuelle Zahlen (admin.ch), Aktuelle Vorfälle (admin.ch);
Cyberdelikte verhindern, Wegleitung für Gemeinden, NEDIK, Schweizerischer Gemeindeverband - Cybersicherheit im Fokus des SGV - Schweizerischer Gemeindeverband (chgemeinden.ch)
[3] Datenschutzgesetz, KDSG, BSG 152.04, zurzeit in Revision:
https://www.belex.sites.be.ch/app/de/texts_of_law/152.04
[4] Stadtordnung von Nidau, SRS 101.1, https://nidau.tlex.ch/app/de/texts_of_law/101.1
[5] Geschäftsordnung Stadtrat (GO SR), SRS 151.1, https://nidau.tlex.ch/app/de/texts_of_law/151.1
[6] Verordnung über die Verwaltungsorganisation (VV), SRS 161.11,
https://nidau.tlex.ch/app/de/texts_of_law/161.11
[7] Funktionendiagramme, SRS 162.11ff, https://nidau.tlex.ch/app/de/systematic/texts_of_law
[8] Verordnung über die elektronische Geschäftsverwaltung und Archivierung in der Stadtverwaltung Nidau (Geververordnung), SRS 161.12, https://nidau.tlex.ch/frontend/versions/175
[9] Weisung über die Nutzung der Informatik, SRS 161.14, https://nidau.tlex.ch/frontend/versions/133

Soweit die Stadt mit Aufgaben des Bundes betraut ist, gelten bundesrechtliche Vorgaben[10].

3. Grundsätze und Ziele

- Der Gemeinderat trägt die Gesamtverantwortung für die Informationssicherheit und den Datenschutz der Stadt Nidau.
- Ziele der Informationssicherheit und des Datenschutzes sind der Schutz der Bevölkerung und ihrer persönlichen Rechte.
- Die Risiken der digitalen Transformation werden identifiziert, systematisiert und ihnen wird mit angemessenen Massnahmen und Mitteln begegnet.
- Als Ambitionsniveau strebt die Stadt Nidau an, das Vertrauen der Bevölkerung in die Verwaltung zu schützen, indem sie den Datenschutz ernst nimmt und Reputationsschaden möglichst vermeidet. Sie will im Bereich Datenschutz und Informationssicherheit im Vergleich mit anderen Gemeinden mindestens im vorderen Mittelfeld sein.
- Da die Stadt ihre IT-Dienstleistungen hauptsächlich bei externen Dienstleistern bezieht, sieht sie die nötigen Prozesse und Rollen vor, damit das angestrebte Schutzniveau über alle beteiligten Organisationen hinweg mit klaren Verantwortungen und Schnittstellen sichergestellt ist. Sie verankert die nötigen Pflichten und die Transparenz in den Dienstleistungsverträgen ihrer Lieferanten.

4. Bearbeitete Informationen und deren Schutzbedarf

Die Stadt führt ein Verzeichnis ihrer Datensammlungen, aus dem mindestens hervorgeht, welche Personendaten

- mit welchem Schutzbedarf,
- in welchem Geschäftsprozess,
- zu welchem Zweck,
- durch welche Verwaltungsstelle,
- in welchem Informationssystem bearbeitet und während welcher ordentlichen Frist aufbewahrt sowie
- welchen Stellen gegenüber regelmässig bekannt gegeben werden.

Dieses Verzeichnis wird von der Aufsichtskommission veröffentlicht. Die Stadt aktualisiert es mindestens jährlich.

5. Systemübersicht

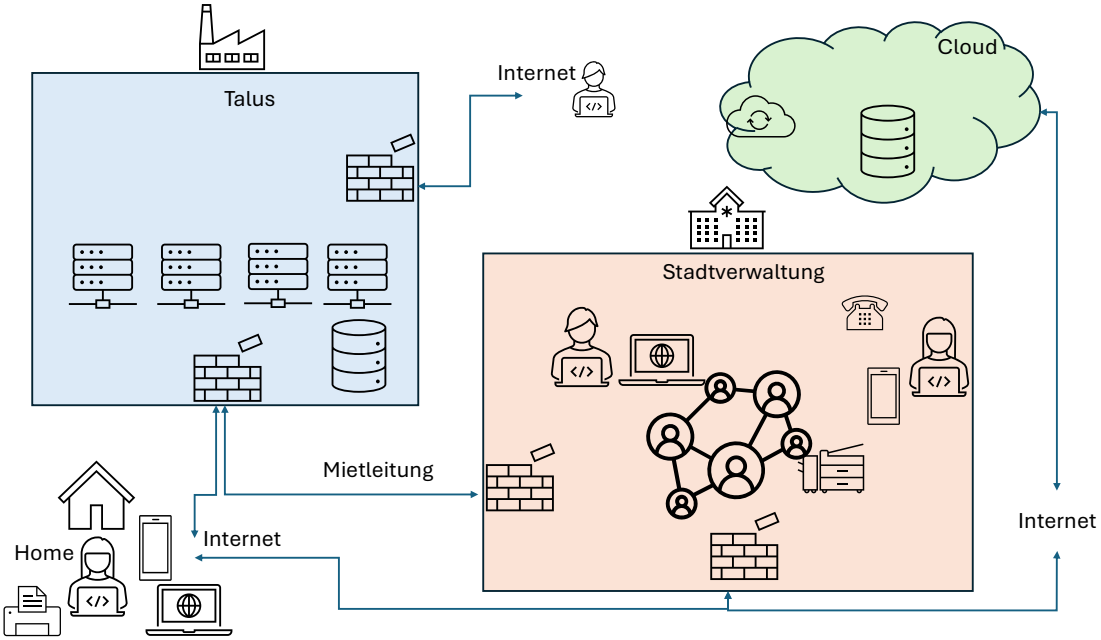
5.1. Systemarchitektur

Die Stadt Nidau unterhält selbst kein Rechenzentrum. Vielmehr werden die Anwendungen von und bei externen Dienstleistern als Managed Service oder als Cloud-Service bezogen. Ebenfalls werden die lokale Infrastruktur und die Endgeräte von externen Partnern bezogen und gewartet. Die entsprechenden Beschaffungen, Verträge und deren Überwachung regeln die Verantwortungen und Massnahmen

[10] Z.B. Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG), SR 235.1, (https://www.fedlex.admin.ch/eli/cc/2022/491/de) oder das Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG), SR 128, (https://www.fedlex.admin.ch/eli/cc/2022/232/de)

zur Sicherstellung der Informationssicherheit und des Datenschutzes. Die Mitarbeitenden können sowohl innerhalb der Räumlichkeiten der Stadtverwaltung wie auch von extern, z.B. im Home-Office, auf die Anwendungen zugreifen.

Generische Übersicht:



Die IT-Service Managerin oder der IT-Service Manager führt eine detaillierte Übersicht der eingesetzten Informationssysteme und aktualisiert die Übersicht regelmässig. Daraus geht insbesondere hervor, wer für welche Systeme zuständig ist und wo welche Daten bearbeitet werden.

5.2. Anwendungen

Die in der Verwaltung der Stadt eingesetzten IT-Anwendungen werden in einem Anwendungsverzeichnis geführt. Dieses wird mindestens jährlich aktualisiert.

5.3. Verantwortungsbereiche

Aufgrund der Systemarchitektur werden die einzelnen Verantwortungsbereiche betreffend die eingesetzten Systeme und deren Schnittstellen sowie damit verarbeiteten Daten zugeordnet.

6. ISDS-Organisation Nidau

Die Aufbauorganisation und Zuständigkeiten der Verwaltung werden in den Organisationserlassen (siehe 2. Grundlagen) abgebildet. Folgende Rollen werden zugeordnet:

- Die *Aufsichtskommission* ist die Aufsichtsstelle für Datenschutz im Sinne der kantonalen Datenschutzgesetzgebung.
- Der *Gemeinderat* hat die Gesamtverantwortung für den Informationssicherheits- und den Datenschutz in der Stadt Nidau.

- *Die Stadtverwalterin oder der Stadtverwalter* hat die Gesamtverantwortung für die operative Umsetzung des Informationssicherheits- und Datenschutzes in der Verwaltung der Stadt Nidau. Sie oder er erlässt die nötigen Weisungen auf Antrag der zuständigen Verwaltungseinheit.
- *Die oder der ISDS-Beauftragte*
    - führt das Management der Informationssicherheits- und Datenschutzrisiken und referiert an die Risiko- und Business Continuitymanagerin oder den -manager der Stadt,
    - führt das Informationssicherheits- und Datenschutzvorfallsmanagement (gegenüber und zusammen mit den externen Dienstleistern),
    - erarbeitet und pflegt die Weisungen für die Informationssicherheit und den Datenschutz,
    - führt das Berechtigungsverzeichnis,
    - führt das Tätigkeits- und Datenverzeichnis.
- *Die IT-Service Managerin oder der IT-Service Manager* ist zuständig für den Einsatz der IT-Mittel der Stadt Nidau aus operativer Sicht und sorgt für:
    - Das Vertragsmanagement mit den Lieferanten einschliesslich der Vertragsüberwachung,
    - das IT-Service Continuity Management,
    - das Incident-Management,
    - die Entsorgung von Datenträgern,
    - die Systemübersicht,
    - das Anwendungsverzeichnis
- Die *Anwendungsverantwortlichen* sind zuständig für die in ihrem Arbeitsbereich eingesetzten Anwendungen, Datenbearbeitungen und Berechtigungen. In der Regel sind dies die Abteilungsleitenden.

7. Prozesse, Rollen und Verantwortlichkeiten

7.1. ISDS-Risikomanagement

a. Ziel und Ergebnis
   Informationssicherheits- und Datenschutzrisiken werden identifiziert und beurteilt, mittels Massnahmen mitigiert oder als Restrisiken akzeptiert.
b. Beschreibung
   Informationssicherheits- und Datenschutzrisiken werden mindestens erhoben mit Eintretenswahrscheinlichkeit und Schadenspotenzial (Risiko). Dazu werden verhältnismässige mitigierende Massnahmen erfasst sowie zur Umsetzung ausgelöst. Diese Analyse wird mindestens jährlich aktualisiert. Die Umsetzung und Wirkung der Massnahmen werden ebenfalls jährlich kontrolliert. Die Restrisiken werden ausgewiesen und von der Stadtverwalterin oder dem Stadtverwalter akzeptiert.
c. Rollen und Verantwortung
   Die oder der ISDS-Beauftragte führt den ISDS-Risikomanagement-Prozess einschliesslich der Dokumentation.
   Der Gemeinderat beurteilt die Risiken, beschliesst Massnahmen und genehmigt die Restrisiken.

d. Messbarkeit
   Bewertung der Risiken nach Umsetzung der mitigierenden Massnahmen
e. Dokumentation
   Analyse, Aktualisierung und Massnahmen sind im GEVER-System dokumentiert.

7.2. IT-Service Continuity Management

a. Ziel und Ergebnis
   Das IT-Service Continuity Management ist eine Teilmenge des Business Continuity Managements und kümmert sich darum, dass die notwendigsten Informatikdienstleistungen im Falle einer kritischen Störung möglichst schnell wieder zur Verfügung stehen. Es stellt damit sicher, dass Ausfälle, Verfügbarkeitseinschränkungen, Kosten und geschäftliche Auswirkungen von Vorfällen mit verhältnismässigem Aufwand minimiert werden und die Stadt Nidau bei Störungen die unmittelbar notwendigen, vitalen Leistungen weiterhin erbringen kann.
b. Beschreibung
   Die Verfügbarkeiten der (extern) bezogenen IT-Dienstleistungen werden entsprechend den Geschäftsanforderungen vertraglich geregelt, vereinbart und die Einhaltung der Regelung mindestens anhand entsprechender Berichterstattungen der Dienstleister jährlich überprüft. Die geschäftskritischen Anwendungen (Anwendungen, die im Falle einer kritischen Störung zwingend notwendigen Geschäftsprozesse der Stadt unterstützen bzw. gewährleisten) werden identifiziert und vom Gemeinderat bestimmt. Anhand einiger typischer Szenarien werden die Geschäftsanforderungen an die Verfügbarkeit der entsprechenden Anwendungen abgleitet.
c. Rollen und Verantwortung
   Die IT-Service Managerin oder der IT-Service Manager stellt den beschriebenen Prozess sicher.
d. Messbarkeit
   Anzahl der nach Kritikalität bewerteten Systeme und Prozesse, Verfügbarkeit/Ausfalldauer, Schadenssumme bei Vorfällen.
e. Dokumentation
   Der Prozess ist im GEVER-System dokumentiert.

7.3. Vorfallsprozess, Security Incident Management

a. Ziel und Ergebnis
   Das Incident- und Vorfallsmanagement stellt sicher, dass bei Incidents sowie bei Informationssicherheits- und Datenschutzvorfällen schnell und wirksam reagiert wird, um Ausfälle und Schäden (sachliche, finanzielle, Reputation) möglichst zu vermeiden bzw. klein zu halten.
b. Beschreibung
   Der Prozess beschreibt die Abläufe, Zuständigkeiten, Erreichbarkeiten, etc. im Falle eines Incidents oder in einem Vorfall, der die von der Stadt eingesetzten Systeme sowie die bearbeiteten Daten betrifft oder betreffen kann, sei es bei der Bearbeitung von Daten durch

Angehörige der Stadtverwaltung oder sei es bei einem Dienstleister der Stadt oder bei einem Nutzenden der Dienstleistungen der Verwaltung.

c. Rollen und Verantwortung
   Die IT-Service-Managerin oder der IT-Service Manager stellt den beschriebenen Prozess und dessen Umsetzung insbesondere in den Dienstleistungsverträgen sicher. Sie oder er sorgt für das entsprechende Monitoring und die Aktualität der Prozessinformationen (Prozess, Erreichbarkeiten, etc.).
d. Messbarkeit
   Anzahl Incidents, Dauer der Behebung
e. Dokumentation
   Der Prozess ist im GEVER-System dokumentiert.

7.4. Erarbeiten und Pflegen von Vorgaben für die Informationssicherheit und den Datenschutz

a. Ziel und Ergebnis
   Den Adressaten sind die Pflichten im Umgang mit Informatikmitteln und Daten der Stadt klar. Die Vorgaben sind verhältnismässig, verständlich und aktuell. Die Vorgaben dienen dem Schutz der damit bearbeiteten Informationen, der Persönlichkeit der Benutzenden und Betroffenen, sowie dem sicheren und wirtschaftlichen Einsatz der Mittel.
b. Beschreibung
   Die Stadtverwalterin oder der Stadtverwalter erlässt eine Weisung über die Nutzung der Informatik der Stadt durch Mitarbeitende der Stadt, durch externe Dienstleister und durch die Bevölkerung.
c. Rollen und Verantwortung
   Die oder der ISDS-Beauftragte erarbeitet die Vorgaben. Die Stadtverwalterin oder der Stadtverwalter erlässt sie.
d. Messbarkeit
   Bekanntheit der Vorgaben beim Zielpublikum.
e. Dokumentation
   Die Vorgaben sind im GEVER-System dokumentiert.

7.5. Projektmanagement (Änderungsprozess) und Beschaffung

a. Ziel und Ergebnis
   Die Informationssicherheit und der Datenschutz werden in allen Projekten und Beschaffungen von Anfang an berücksichtigt und deren Stand regelmässig kontrolliert.
b. Beschreibung
   Die Stadtverwalterin oder der Stadtverwalter erlässt Vorgaben zur Berücksichtigung der Informationssicherheit und des Datenschutzes im Rahmen von Projekten und Beschaffungen auf Vorschlag der oder des ISDS-Beauftragten. Die oder der ISDS-Beauftragte überprüft regelmässig die Einhaltung der Vorgaben.
c. Rollen und Verantwortung
   Die oder der ISDS-Beauftragte erarbeitet die Vorgaben. Die Stadtverwalterin oder der Stadtverwalter erlässt sie. Die oder der ISDS-Beauftragte überprüft die Einhaltung anhand

der Projektunterlagen und der Lieferanten-Reportings. Sie oder er meldet Verletzungen an die Vorgesetzten.

d. Messbarkeit
   Anzahl Verletzungen pro Jahr.
e. Dokumentation
   Die Vorgaben und die Reportings sind im GEVER-System dokumentiert.

7.6. Berechtigungswesen

a. Ziel und Ergebnis
   Nur dazu berechtigte Personen haben Zugriff auf die relevanten Anwendungen der Stadt Nidau und können diese nur im definierten Umfang nutzen.
b. Beschreibung
   Die Anwendungsverantwortlichen definieren Rollen zur Nutzung der in ihrem Tätigkeitbereich relevanten Anwendungen und teilen diese den einzelnen Nutzenden zu. Die oder der ISDS-Beauftragte erstellt eine Vorlage und führt eine Übersicht über die Rollen, Berechtigungen und Anwendungen. Sie oder er überprüft diese mindestens einmal jährlich mit den Abteilungsleitenden sowie anhand der Reportings der externen Dienstleister.
c. Rollen und Verantwortung
   Die Anwendungsverantwortlichen sind verantwortlich für die Adäquanz und Aktualität der Rollen und Rechtezuweisungen der von ihnen verantworteten Anwendungen. Die oder der ISDS-Beauftragte konsolidiert die Zuweisungen und führt das Controlling bei den Anwendungsverantwortlichen und anhand der Lieferanten-Reportings durch.
d. Messbarkeit
   Anzahl festgestellte Abweichungen bei der jährlichen Kontrolle.
e. Dokumentation
   Die Übersicht ist im GEVER-System dokumentiert.

7.7. Schulung und Sensibilisierung

a. Ziel und Ergebnis
   Mitarbeitende, Vorgesetzte sowie weitere Nutzende (z.B. Schülerinnen und Schüler) sind befähigt zur verantwortungsvollen Nutzung der IT-Mittel sowie zur Gewährleistung von Informationssicherheit und Datenschutz.
b. Beschreibung
   Der Schulungsbedarf wird mithilfe von Eindrücken aus dem Alltag und der Bewertung der Einhaltung von Vorgaben sowie externen Entwicklungen regelmässig erhoben sowie entsprechende Massnahmen (Informationspakete, Schulung, Sensibilisierungskampagnen, Beratung) werden konzipiert und umgesetzt. Alle neu eintretenden Mitarbeitenden werden geschult.
c. Rollen und Verantwortung
   Die oder der ISDS-Beauftragte führt die Erhebungen durch und schlägt Massnahmen vor. Massnahmen werden von der Stadtverwalterin oder vom Stadtverwalter beschlossen.
d. Messbarkeit
   Erhebungen.

e. Dokumentation
   Die Schulungen sind im GEVER-System dokumentiert.

7.8. Ausnahmeprozess und -regelung

a. Ziel und Ergebnis
   Begründete Ausnahmen von den Vorgaben werden bewusst und insbesondere in Beurteilung derer Auswirkungen auf Informationssicherheit und Datenschutz behandelt und dokumentiert.
b. Beschreibung
   Ausnahmen von den Vorgaben werden schriftlich über die Vorgesetzten bei der Stadtverwalterin oder beim Stadtverwalter begründet beantragt. Diese oder dieser entscheidet. Die Ausnahmen werden im GEVER-System dokumentiert und periodisch überprüft.
c. Rollen und Verantwortung
   Die oder der ISDS-Beauftragte führt die Liste der Ausnahmen und überprüft deren Aktualität einmal jährlich zuhanden der Stadtverwalterin oder des Stadtverwalters.
d. Messbarkeit
   Anzahl festgestellter nicht genehmigter Ausnahmen.
e. Dokumentation
   Die Ausnahmen sind im GEVER-System dokumentiert.

7.9. Auskunfts-, Einsichts-, Korrektur- und Löschungsprozess (KDSG)

a. Ziel und Ergebnis
   Das Auskunfts-, Einsichts-, Korrektur- und Löschungsrecht nach kantonalem Datenschutzrecht ist in einem nachvollziehbaren Prozess rechtskonform abgewickelt und dokumentiert.
b. Beschreibung
   Das entsprechende Recht und die zur Geltendmachung zu verwendende Adresse (Post und E-Mail) wird auf der Gemeindewebseite geeignet publiziert. Das Geschäft wird in GEVER geführt. Zur Beurteilung wird die zuständige Abteilungsleitung konsultiert.
c. Rollen und Verantwortung
   Die sachlich zuständigen Sachbearbeitenden führen die Verfahren durch. Im Zweifelsfall legen sie das Geschäft der Stadtverwalterin oder dem Stadtverwalter zum Entscheid vor. Die oder der ISDS-Beauftragte dokumentiert die entsprechenden, einfachen Prozessbeschreibungen.
d. Messbarkeit
   Einträge im GEVER-System.
e. Dokumentation
   Die Gesuche und deren Beurteilung bzw. der Entscheid sowie die Prozesse sind im GEVER-System dokumentiert.

7.10. Kontinuierlicher Verbesserungsprozess

a. Ziel und Ergebnis
   Die Erfahrungen aus Projekten, aus Vorfällen, aus Ausnahmegesuchen, etc. fliessen in kontinuierliche Verbesserungen der Prozesse und damit der Sicherheit ein.

b. Beschreibung
   Folgerungen aus Projektabschlussberichten, aus Vorfallsstatistiken, aus Schulungen, aus der Ausnahmeliste, aus Führungsgesprächen etc. werden mindestens zweimal pro Jahr gesichtet und sinnvolle Massnahmen zur Verbesserung formuliert.
c. Rollen und Verantwortung
   Die oder der ISDS-Verantwortliche sichtet die verschiedenen Folgerungen und legt sie seiner oder ihrer Abteilungsleitung vor. Diese beurteilt die Sinnhaftigkeit von Audits und verbessernden Massnahmen und löst sie zuständigenorts aus.
d. Messbarkeit
   Erhebungen.
e. Dokumentation
   Die Massnahmen sind im GEVER-System dokumentiert.

8. Information

a. Die Information richtet sich nach dem Informationskonzept der Stadt Nidau.
b. Der Gemeinderat genehmigt das vorliegende Konzept und wird im Rahmen der Berichterstattung zur Umsetzung der Digitalstrategie periodisch und über Vorfälle zeitnah konkret informiert.
c. Die Bevölkerung wird im Rahmen der Berichterstattung zur Umsetzung der Digitalstrategie periodisch und über Vorfälle zeitnah konkret informiert.
d. Die von Datenschutzverletzungen Betroffenen werden zeitnah und direkt informiert.
e. Der Aufsichtskommission wird das Register der Datensammlung zur Veröffentlichung zugestellt. Es wird mindestens jährlich aktualisiert. Weiter wird der Aufsichtsstelle das vorliegende Konzept und allfällig weitere von ihr geforderte Information zur Verfügung gestellt.
f. Die Mitarbeitenden werden bei ihrem Eintritt und dann in periodischen Abständen über ihre Pflichten zum Schutz der Daten informiert.