



---

## Weisung über die Nutzung der Informatik

Vom 4. Dezember 2001 (Stand 4. Dezember 2001)

---

### **Art. 1** Zweck und Geltungsbereich

<sup>1</sup> Die Weisung legt verbindlich den Umgang mit den Informatikmitteln fest, die am Netzwerk der Gemeinde Nidau angeschlossen sind, oder als lokale Arbeitsstationen der Gemeinde Nidau (z.B. Gemeindebibliotheken) betrieben werden. Sie gilt für alle Mitarbeitenden.

### **Art. 2** Hardware

<sup>1</sup> Es dürfen keine privaten PCs am Kommunikationsnetz angeschlossen werden.

<sup>2</sup> Die Informatik-Arbeitsplatzausrüstung (z.B. PC, Terminal, Printer, Peripheriegeräte) darf nur durch den IT-Support oder durch eine vom IT-Support beauftragte Firma gewartet oder in irgend einer Weise erweitert/verändert werden.

<sup>3</sup> Es ist untersagt, Kommunikationsmittel (z.B. Modem) an das Kommunikationsnetz oder den Arbeitsplatz-PC anzuschliessen.

<sup>4</sup> Bei Verdacht auf Vireninfection ist der PC sofort physisch vom Kommunikationsnetz zu trennen (d.h. Netzwerkstecker ausziehen); der IT-Support ist umgehend zu informieren.

<sup>5</sup> Die Mitarbeitenden sind für die periodische Reinigung des Bildschirms, des Gehäuses, der Maus und der Tastatur selber besorgt.

### **Art. 3** Software

<sup>1</sup> Es ist untersagt, ohne Wissen des IT-Supports Software (SW) entweder lokal auf dem eigenen Arbeitsplatz oder auf den zentralen Server zu installieren. Neue oder unbekannte SW kann dem IT-Support zum Testen abgegeben werden. Der IT-Support entscheidet über eine ev. Installation der SW. Davon betroffen sind ausdrücklich auch Bildschirmschoner und Hintergrundbilder.

<sup>2</sup> Der automatische Virensan (in der Regel freitags ab 12.00 Uhr) und das automatische Update des Virensanners (in der Regel montags ab 12.00 Uhr) darf nicht ausgeschaltet oder angehalten werden.

<sup>3</sup> Die private Nutzung geschäftlich lizenzierter SW auf andern Rechnern (z.B. auf Privat-PC) ist aus Lizenzrechtsgründen untersagt. Ebenso ist es verboten, solche SW zu kopieren.

#### **Art. 4**      Einschränkungen allgemein

<sup>1</sup> Es stehen i.d.R. am Arbeitsplatz keine Speichermedien (A: für Diskette, C: für lokale Harddisk, CD-Rom Laufwerk) zur Verfügung. Sämtliche Daten müssen auf den Servern in jenen Verzeichnissen abgelegt werden, die der Berechtigung entsprechen.

<sup>2</sup> Werden Daten per Diskette importiert oder exportiert, ist der Datenträger vorerst auf Viren zu testen. Der IT-Support ist zu informieren.

#### **Art. 5**      Sicherheit

<sup>1</sup> Der Zugang von Drittpersonen zum Arbeitsplatz-PC bzw. zu den gespeicherten Daten ist durch die Mitarbeitenden mit organisatorischen und technischen Massnahmen angemessen zu erschweren bzw. zu verunmöglichen (Büros und Gebäude in Randzeiten abschliessen, Passwort geschützte Bildschirmschoner bei Verlassen des Arbeitsplatzes aktivieren).

<sup>2</sup> Passwörter müssen entweder auswendig gelernt oder unter Verschluss aufbewahrt werden. Sie dürfen nicht an Dritte weitergegeben oder am Bildschirm angeschrieben werden.

<sup>3</sup> Die Mitarbeitenden des IT-Supports haben gegenüber der Präsidialabteilung eine Verschwiegenheitserklärung zu unterzeichnen, worin sie sich insbesondere verpflichten, die Sorgfalts- und Schweigepflicht immer zu wahren und das in sie gesetzte Vertrauen in keiner Weise zu missbrauchen. Weiter erklären sie, ausdrücklich auf Art. 320 Strafgesetzbuch (Verletzung des Amtsgeheimnisses) hingewiesen worden zu sein.

<sup>4</sup> Es ist den Mitarbeitenden des IT-Supports ohne ausdrückliche Ermächtigung der Berechtigten strengstens verboten, fremde Dateien anzuschauen, zu öffnen oder zu bearbeiten.

<sup>5</sup> Aus Datenschutzgründen ist es untersagt, irgendwelche elektronischen Datenträger (Disketten, Magnetbänder, CD-ROM etc.), selber zu entsorgen. Die zu entsorgenden Medien sind dem IT-Support zur sachgemässen Vernichtung zuzuführen.

<sup>6</sup> Alle Mitarbeitenden sind für die in ihrem Arbeitsbereich bearbeiteten Daten in Bezug auf die Vertraulichkeit, Verfügbarkeit und Richtigkeit verantwortlich (Daten aus dem eigenen Verantwortungsbereich dürfen weder an Dritte weiter gegeben, noch ohne Auftrag gelöscht oder verändert werden).

<sup>7</sup> Um die Leistungsfähigkeit und Verfügbarkeit der Server sicher zu stellen, ist das Personal des IT-Supports verpflichtet, mit Hilfe von speziellen Tools laufend die Server zu überwachen. Dadurch erhält das Personal des IT-Supports unvermeidbar auch Informationen zu den Usern, ihren genutzten Applikationen und den bearbeiteten Dateien. Diese so genannten "Userdaten" dürfen nur konsultiert werden, wenn es aus betrieblichen Gründen (Verhalten der Server) notwendig ist.

**Art. 6** Neue Hardware und/oder Software

<sup>1</sup> Die Beschaffung von neuer oder Ersatz-Hardware (HW) und SW erfolgt ausschliesslich über den IT-Support.

<sup>2</sup> Im Rahmen der ordentlichen Budgetierung und der Investitionsplanung werden die Abteilungen durch den IT-Support aufgefordert, ihre Informatik-Bedürfnisse anzumelden.

**Art. 7** Internet-Nutzung

<sup>1</sup> Die vom IT-Support angebotenen Internet-Dienste sind während der Arbeitszeit nur zu dienstlichen Zwecken zu nutzen.

<sup>2</sup> Die private Nutzung des Internets (z.B. Buchung von Ferien, Shopping etc.) ist nur ausserhalb der Arbeitszeit zulässig.

<sup>3</sup> Der Zugang zu Internet-Informationen mit rechtswidrigem (bspw. rassistischem) oder sittenwidrigem (bspw. pornografischem) Inhalt ist verboten.

<sup>4</sup> Die Internet-Aktivitäten werden beim Netzanbieter und beim Internetprovider im Sinne eines kontinuierlichen Verlaufes aufgezeichnet. Weiter werden auf dem jeweiligen Internet-Arbeitsplatz in betriebssystemnahen Dateien Einträge dokumentiert, die eine Rückverfolgung auf die im Internet besuchten Web-Sites möglich machen.

<sup>5</sup> Bei Verdacht auf Missbrauch kann die vorgesetzte Stelle über die Präsidialabteilung befristet Kontrollen und Auswertungen dieser Daten veranlassen. Die Überwachung muss der betreffenden Person angekündigt worden sein.

<sup>6</sup> Missbräuche bei der Internet-Nutzung werden geahndet.

**Art. 8** Mailwesen

<sup>1</sup> Das E-Mail-System darf wie das Telefon für kurze private Mitteilungen genutzt werden.

---

<sup>2</sup> Der IT-Support setzt zur Sicherung des Informatikbetriebes Überwachungs-SW ein, die insbesondere verhindern sollen, dass E-Mails mit ausführbaren Programmen und/oder Viren eingeschleust werden.

<sup>3</sup> Das Starten (Doppelklicken) oder Abspeichern von an Mails angehängten Dateien mit den Endungen: .exe, .mpg, .avi, .mp3, .vbs auf dem Informatik-System ist verboten. Diese Anhänge müssen ungeöffnet gelöscht und bei Bedarf vorher an die private E-Mail-Adresse gesendet werden. Der IT-Support behält sich zur Aufrechterhaltung der Betriebssicherheit und zur Sicherung der Leistungsfähigkeit der Server vor, die Postfächer der Anwendenden periodisch nach den vorgenannten Dateien zu durchsuchen und diese Dateien automatisch zu löschen.

**Änderungstabelle - Nach Beschluss**

<b>Beschluss</b>	<b>Inkrafttreten</b>	<b>Element</b>	<b>Änderung</b>	<b>CRS Fundstelle</b>
04.12.2001	04.12.2001	Erlass	Erstfassung	2017-009

**Änderungstabelle - Nach Artikel**

<b>Element</b>	<b>Beschluss</b>	<b>Inkrafttreten</b>	<b>Änderung</b>	<b>CRS Fundstelle</b>
Erlass	04.12.2001	04.12.2001	Erstfassung	2017-009