



Beschlussvorlage

- öffentlich -

VL-115/2026

Abteilung	Hauptamt
Verfasser	Kerstin Ganss
Datum	14.08.2026

Betreff:

Teilnahme/Mitgliedschaft an der IKZ Informationssicherheit

Beratungsfolge	Termin	Beratungsaktion
Gemeindevorstand	19.08.2026	vorberatend
Haupt- Finanz- und Sozialausschuss	31.08.2026	
Gemeindevertretung der Gemeinde Glauburg	28.09.2026	beschließend

Sachdarstellung / Erläuterungen:

Im Wetteraukreis existiert seit einiger Zeit eine interkommunale Informationssicherheitsstelle (ISS), die aus einer interkommunalen Zusammenarbeit (IKZ) zum Thema Informationssicherheit hervorgegangen ist. Vergleichbare Modelle haben sich in anderen hessischen Kreisen bereits bewährt. Die Gemeinde Glauburg war zu Beginn an dieser IKZ beteiligt ist dann aber im Verlauf aus Kostengründen ausgeschieden.

Aktuell nehmen 19 von 25 Kommunen des Wetteraukreises an der ISS teil. Große Kommunen wie Bad Vilbel oder Bad Nauheim sind nicht dabei, da sie über ausreichend eigene Ressourcen verfügen. Neben Glauburg haben sich bisher nur drei weitere Kommunen (Kefenrod, Ranstadt, Altenstadt) gegen eine Teilnahme entschieden. Nach Rücksprache mit dem Kreis ist eine nachträgliche Teilnahme für uns jederzeit möglich. Mittlerweile hat eine der vier verbleibenden Kommunen bereits einen Antrag auf Beitritt gestellt.

Die detaillierte Ausgestaltung der Stelle ist in der beigefügten öffentlich-rechtlichen Vereinbarung geregelt. Die ISS ist bereits operativ tätig.

Die aktuelle Situation hat sich gegenüber dem damaligen Zeitpunkt derart verändert, dass eine Teilnahme trotz finanzieller Engpässe für uns unverzichtbar ist.

Cyberangriffe auf kommunale IT-Infrastrukturen haben in den letzten Jahren dramatisch zugenommen. Allein 2024 meldeten 21 hessische Kommunen mindestens einen schweren Angriff. Das hessische Innenministerium spricht von einer „alarmierend hohen Zahl“ ernstzunehmender Vorfälle. Dass auch kleine Verwaltungen wie Glauburg betroffen sein können, zeigt der Fall Geisenheim (Rheingau-Taunus-Kreis) – eine Kommune vergleichbarer Größe und Personalausstattung.

Die Lage verschärft sich durch den Einsatz KI-gestützter Angriffswerkzeuge. Automatisiertes Aufspüren von Schwachstellen, KI-basierte Phishing-Kampagnen, deutlich höhere Angriffshäufigkeit und -geschwindigkeit sind nur einige Punkte.

Besonders kritisch: Gelangen personenbezogene Daten von Bürgern oder Beschäftigten in falsche Hände, drohen Erpressung, empfindliche datenschutzrechtliche Konsequenzen (Bußgelder, Meldepflichten), Vertrauensverlust in die Verwaltung und ein erheblicher zeitlicher und vor allem finanzieller Aufwand für Schadensbegrenzung.

Zwar besteht für hessische Kommunen derzeit noch keine gesetzliche Pflicht zum Aufbau eines vollständigen Informationssicherheitsmanagementsystems (ISMS) – das HITSiG gilt aktuell nur für die Landesverwaltung und die EU-Richtlinie NIS2 nimmt die lokale Ebene bewusst aus. Doch das entbindet uns nicht von bestehenden Verpflichtungen:

Nach Art. 5 Abs. 2, Art. 24 und Art. 32 DSGVO müssen wir angemessene Schutzmaßnahmen für personenbezogene Daten treffen und jederzeit nachweisen können, dass diese wirksam sind. Reine Absichtserklärungen reichen nicht aus – hier ist eine lückenlose Dokumentation unverzichtbar.

Ohne Dokumentation können wir nicht belegen, dass wir unsere Pflichten erfüllt haben. Im Schadensfall oder bei einer Prüfung durch Aufsichtsbehörden (z. B. den Hessischen Datenschutzbeauftragten) fehlt der rechtssichere Nachweis – mit potenziell schweren Konsequenzen.

Ein ISMS als strukturierter Rahmen (z. B. nach BSI-IT-Grundschutz) ist nicht nur ein Sicherheitskonzept, sondern vor allem ein Dokumentationssystem. Es erfasst:

- Aktuelle Maßnahmen (Was tun wir?)
- Umgesetzte Schutzvorkehrungen (Was haben wir getan?)
- Risikobewertungen und -behandlungen (Wo liegen Schwachstellen, und wie gehen wir damit um?)
- Verantwortlichkeiten und Prozesse (Wer ist wofür zuständig?).
- Datenschutz-Compliance: Die DSGVO verlangt explizit die Dokumentation technischer und organisatorischer Maßnahmen (TOM). Ohne diese Dokumentation riskieren wir Bußgelder und den Vorwurf des Organisationsverschuldens.

Aufgrund unserer Größe/Personalstruktur liegt fast das gesamte Know-how zur Informationssicherheit und IT-Infrastruktur aktuell bei einer einzigen Person. Bei Krankheit, Urlaub oder Ausfall dieser Person kann dies folgendes bedeuten:

- Fehlende Handlungsfähigkeit: Ohne dokumentierte Prozesse, Verantwortlichkeiten und Notfallpläne können wir nicht reagieren – weder auf Sicherheitsvorfälle noch auf Anfragen von Aufsichtsbehörden.
- Wissensverlust: Jahre an Erfahrung und Konfigurationen wären nicht mehr abrufbar, was zu längeren Ausfallzeiten und höheren Kosten führt.
- Haftungsrisiko: Ohne Nachweise über getroffene Maßnahmen haftet die Gemeindeleitung im Schadensfall persönlich.

Die fachliche Kompetenz für Informationssicherheit ist in unserer Verwaltung zwar vorhanden, allerdings erfordert der Aufbau und Betrieb eines ISMS inkl. Dokumentation einen Personal- und Zeitaufwand, den wir mit unserer aktuellen Auslastung nicht leisten können:

Alleine eine Koordinierung einer externen Stelle wird beispielsweise vom Sächsischen Rechnungshof für Kommunen unserer Größe mit 0,1 Vollzeitäquivalente (VZÄ) beziffert – also einen halben Arbeitstag pro Woche zusätzlich zum Tagesgeschäft.

Der eigenständige ISMS-Aufbau geht nach realistischen Schätzungen für eine Basis-Absicherung nach BSI-IT-Grundschutz von 3 bis 6 Monaten konzentrierter Facharbeit aus (bei 94–113 Bausteinen des IT-Grundschutz-Kompendiums und jährlich wiederkehrender Überprüfung und Dokumentation).

Wir sind für den gesamten IT-Betrieb verantwortlich – von der Nutzerbetreuung in Verwaltung, Kindergarten und Bauhof bis zur Unterstützung von Feuerwehren und Bücherei. Dazu kommen Digitalisierung, Datenschutz, IT-Beschaffung, Informationssicherheit sowie die laufende Abstimmung mit unserem kommunalen IT-Dienstleister. Es gibt keine Vertretung. Zeit, um uns über Wochen oder Monate aus dem laufenden Betrieb herauszuziehen, gibt es nicht.

Ein eigenständiger Aufbau würde unser Tagesgeschäft monatelang beeinträchtigen – oder gar nicht stattfinden, weil im Alltag stets dringlichere Aufgaben Vorrang haben.

Genau diese Lücke schließt die ISS.

Die Teilnahme an der ISS bringt konkrete, sofort wirksame Vorteile, die wir im Alleingang nicht erreichen können:

- Fachkompetenz ohne Personalgewinnung (das vom Kreis gewonnene Personal verfügt über jahrelange Berufserfahrung in dem Bereich).

- Die Kostenbeteiligung liegt weit unter denen einer eigenen Fachkraft oder externen Beauftragung.
- Durch gebündelte Kompetenzen und standardisierte Verfahren erreichen wir schneller ein belastbares Sicherheitsniveau.
- Dokumentation und ISMS-Unterstützung – wir erhalten Zugriff auf ein für Kommunen gestaltetes ISMS, dass wir nur noch an unsere Bedingungen vor Ort anpassen müssen. Die ISS übernimmt die strukturierte Dokumentation nach BSI-IT-Grundschutz inkl..
 - Erstellung und Pflege von Sicherheitskonzepten,
 - Risikoanalysen und -bewertungen,
 - Nachweise für DSGVO-Compliance (TOM),
 - Notfallpläne und Prozessdokumentation.
- Wissenssicherung: Das Know-how wird zentral dokumentiert und ist unabhängig von einzelnen Personen verfügbar.
- Einheitliches Sicherheitsniveau im Kreis: Abgestimmte Standards nach BSI-IT-Grundschutz statt Einzellösungen.
- Erfahrungsaustausch und Netzwerk: Regelmäßiger fachlicher Austausch mit den ISBs der anderen Wetterau-Kommunen und dem Hessen3C.
- Unterstützung im Ernstfall: Begleitung bei Sicherheitsvorfällen ist Teil der laufenden Leistung. Eine vergleichbare externe Unterstützung würde im Einzelfall mehrere tausend Euro kosten.

Die Gesamtverantwortung für die Informationssicherheit verbleibt unverändert bei der Gemeindeleitung (Bürgermeister/Gemeindevorstand). Der örtliche IT-Sicherheitsbeauftragte bleibt für die operative Umsetzung und Überwachung vor Ort zuständig. Die ISS übernimmt ausschließlich eine ergänzende, beratende und unterstützende Funktion – ohne Weisungsrecht gegenüber der Gemeinde.

Die Teilnahme an der IKZ-Informationssicherheit ermöglicht uns:

- den gesetzlichen und datenschutzrechtlichen Pflichten nachzukommen (inkl. lückenloser Dokumentation)
- das Haftungsrisiko für den Vorstand zu minimieren (durch Nachweisführung und ISMS)
- den wachsenden Cyberbedrohungen wirksam zu begegnen
- Know-how und Standards zu nutzen, die wir allein nicht aufbauen könnten
- Wissensverlust bei Personalausfall zu vermeiden (durch zentrale Dokumentation)
- Kosten zu sparen (keine teure externe Beauftragung oder Personalaufstockung).

Wir bitten den Vorstand, der Teilnahme an der ISS zuzustimmen, um die Sicherheit unserer IT-Infrastruktur und Daten nachhaltig zu stärken, rechtliche sowie finanzielle Risiken für die Gemeinde und die Leitungsebene zu vermeiden und die Handlungsfähigkeit auch bei Personalausfall zu sichern.

Beschlussvorschlag:

Die Gemeindevertretung beschließt die Teilnahme der Gemeinde Glauburg an der IKZ-Informationssicherheit des Wetteraukreises und stimmt der öffentlich-rechtlichen Vereinbarung zu.

Haushaltsrechtliche Darstellung:

Die Kosten (Sockelbetrag plus einwohnerbezogener Anteil) liegen deutlich unter den Kosten einer eigenen Fachkraft (EG 12 TVöD) oder externer Beauftragung. Für die Gemeinde Glauburg liegt der jährliche Anteil bei 3. 735,10 EUR pro Jahr.

gez.

DER GEMEINDEVORSTAND
DER GEMEINDE GLAUBURG

gez. Henrike Strauch
Bürgermeisterin

Anlage:

1. ör Vereinbarung IKZ Informationssicherheit unterzeichnet mit Anlagen