
IT-Strategie 2026–2031

IT-Gesamtstrategie der Stadt Schmallenberg



Organisationseinheit	Hauptamt / Sachgebiet IT (10.1 / 10.3)
Stand	Juni 2026
Status	Freigegeben
Aktenzeichen	10.3

Inhalt

1. Strategischer Rahmen	4
2. Ausgangslage und Rahmenbedingungen	4
3. Meilenstein- und Terminplanung	4
3.1 Jahr 2026 – Grundlagen und laufende Stabilisierung	4
3.2 Jahr 2027 – Sanierungsabschluss und strategische Weichenstellungen	5
3.3 Jahr 2028 – Umsetzung und erste Überprüfung	5
3.4 Jahre 2029–2031 – Konsolidierung und Vorbereitung Folgestrategie	5
4. Architekturprinzipien	6
5. Herstellerstrategie und digitale Souveränität	7
6. Desktop-Betriebsmodell und Secure Endpoints	7
7. Infrastrukturbedingte Zurückstellung von Softwareentscheidungen	8
Zielbild nach Abschluss der Sanierung	9
8. Ressourcenplanung	9
8.1 Personelle Ressourcen	9
8.2 Externe Dienstleister und Verbundstrukturen	9
8.3 Finanzielle Ressourcen	9
8.4 Fördermöglichkeiten	10
9. Erfolgskennzahlen und Steuerungsgrößen	10
9.1 Leitziel 1 – Betriebsstabilität	10
9.2 Leitziel 2 – Digitale Souveränität	10
9.3 Leitziel 3 – Informationssicherheit	10
9.4 Leitziel 4 – Digitalisierung	11
9.5 Leitziel 5 – Wirtschaftlichkeit	11
9.6 Leitziel 6 – Technologieneutrale Steuerung	11
9.7 Berichtswesen	11
Governance und Steuerung	11
10. Fachverfahren-Strategie	11
10.1 Überblick und Bestandsaufnahme	11
10.2 Sonderstellung des Finanzwesens	12
10.3 Strategische Neuausrichtung bei der Dienstleisterauswahl	12
10.4 Steuerungsgrundsätze für Fachverfahren	12
11. Risikokatalog	13
12. Datenschutz und Notfallplanung	16
12.1 Datenschutz	16
12.2 Notfallplanung und Business Continuity	16
13. Wirtschaftlichkeit und Entscheidungsgrenzen	17
13.1 Schwellenwerte für strategische IT-Entscheidungen	17
13.2 Definition strategischer Relevanz	17

13.3 Wirtschaftlichkeitsanforderungen.....	17
14. Maßnahmenrahmen 2026–2031.....	17
15. Strategische Bewertung.....	18
16. Freigabevermerk	18

1. Strategischer Rahmen

Die IT der Stadt Schmallingenberg ist als zentraler interner Infrastruktur- und Servicedienstleister der Verwaltung auszurichten. Ihr Auftrag besteht darin, die kommunale Aufgabenerfüllung zuverlässig, wirtschaftlich, rechtssicher und zukunftsfähig zu unterstützen. Leitend ist dabei das Ziel, eine resiliente, steuerbare und schrittweise souveränere IT-Landschaft aufzubauen, die betriebliche Stabilität gewährleistet und Abhängigkeiten von einzelnen Herstellern gezielt reduziert, ohne die Kontinuität der Verwaltungsprozesse zu gefährden.

Die Stärkung digitaler Souveränität ist ein von Bund, Ländern und Kommunen ausdrücklich verfolgtes Ziel; der IT-Planungsrat hat 2021 die Förderung digitaler Souveränität in der öffentlichen Verwaltung beschlossen. Für die Stadt Schmallingenberg bedeutet dies, dass IT-Strategie nicht allein als Technikplanung verstanden wird, sondern als Bestandteil der Verwaltungssteuerung.

2. Ausgangslage und Rahmenbedingungen

Die Stadt Schmallingenberg ist als Mittelstadt im ländlichen Raum in ein kommunales IT-Umfeld eingebettet, das wesentlich durch die Zusammenarbeit mit der Südwestfalen-IT geprägt ist. Zugleich verbleibt die strategische Steuerungsverantwortung für die eigene IT bei der Verwaltung selbst; kommunale IT-Steuerung ist nach KGSt-Verständnis nicht delegierbar und muss organisatorisch in der Verwaltung verankert sein.

Ein wesentlicher infrastruktureller Rahmenfaktor ergibt sich aus der baulichen und technischen Ausgangslage des Rathauses. Das Gebäude wurde 1995 mit einer passiven Verkabelungsinfrastruktur errichtet, die an den Arbeitsplätzen lediglich 100-Mbit/s-Verbindungen ermöglicht. Diese strukturelle Begrenzung bestand seit Inbetriebnahme des Gebäudes und wirkte sich über viele Jahre unmittelbar auf Betriebsmodell, Softwareeinsatz und Modernisierungsgeschwindigkeit aus. Seit rund zwei Jahren läuft die Sanierung des Rathauses; im Zuge dieser Maßnahme wird die Netzwerkinfrastruktur grundlegend erneuert.

Die unzureichende Verkabelung war nicht nur ein technisches Detail, sondern ein strategisch relevanter Hinderungsgrund. Sie begrenzte den wirtschaftlichen Einsatz klassischer Fat-Client-Modelle ebenso wie die Einführung bandbreiten- und datenintensiver Fach- und Querschnittslösungen. Softwareentscheidungen, insbesondere zur Einführung eines Dokumentenmanagementsystems, wurden daher aus infrastrukturellen Gründen zurückgestellt. Diese Zurückstellung ist als sachgerechte Priorisierung zu bewerten und nicht als Digitalisierungsdefizit im engeren Sinne.

3. Meilenstein- und Terminplanung

Die Meilenstein- und Terminplanung konkretisiert den Maßnahmenrahmen der IT-Gesamtstrategie auf Ebene von Kalenderjahren. Sie ist als verbindlicher Orientierungsrahmen für das IT-Sachgebiet und die Verwaltungsführung zu verstehen, nicht als starres Projektplan-Dokument. Terminliche Anpassungen sind im Rahmen der jährlichen Umsetzungsberichte zu dokumentieren und zu begründen. Die Planung folgt einer zentralen strukturellen Abhängigkeit: Der Abschluss der Rathaus-Netzwerksanierung, geplant für Ende 2027, ist der maßgebliche Wendepunkt für mehrere strategische Folgeentscheidungen und bestimmt daher die Phasierung aller davon abhängigen Maßnahmen.

3.1 Jahr 2026 – Grundlagen und laufende Stabilisierung

Im Jahr 2026 liegt der Schwerpunkt auf der Schaffung belastbarer Steuerungsgrundlagen sowie der Fortführung des laufenden Betriebs unter Sanierungsbedingungen. Das IT-Portfolioregister ist aufzubauen oder fortzuschreiben; es bildet die dokumentarische Basis für alle Folgeentscheidungen. Parallel sind die bestehenden Herstellerabhängigkeiten

strukturiert zu erfassen und den Kategorien „nicht ersetzbar“, „teilersetzbar“ und „neu zu besetzen“ zuzuordnen.

Die laufende Markterkundung für ein Dokumentenmanagementsystem ist 2026 abzuschließen. Auf dieser Grundlage ist der Verwaltungsführung eine Entscheidungsvorlage vorzulegen, die Produktoptionen, Kosten und Einführungsszenarien vergleicht. Ergänzend sind Open-Source-Optionen für Querschnittsdienste, insbesondere Collaboration, Passwortmanagement und Monitoring, pilotfähig zu bewerten. Der bestehende Citrix-Betrieb wird während der gesamten Sanierungsphase unverändert stabil weitergeführt.

3.2 Jahr 2027 – Sanierungsabschluss und strategische Weichenstellungen

Das Jahr 2027 markiert den entscheidenden Wendepunkt der Strategieperiode. Mit dem geplanten Abschluss der Rathaus-Netzwerksanierung Ende 2027 entfällt die seit 1995 bestehende infrastrukturelle Begrenzung. Unmittelbar nach Vorliegen der neuen Infrastruktur ist die ergebnisoffene Bewertung des Desktop-Betriebsmodells durchzuführen – zwischen den drei Optionen Citrix-Fortführung, Hybridmodell und erweitertem Fat-Client-Betrieb. Die Ergebnisse sind der Verwaltungsführung als Entscheidungsvorlage vorzulegen.

Parallel startet 2027 der DMS-Pilot in ausgewählten Organisationseinheiten. Der Pilot dient der Validierung der gewählten Lösung unter realen Betriebsbedingungen und ist Voraussetzung für die flächendeckende Einführung ab 2028. Soweit Open-Source-Querschnittsdienste aus der Pilotbewertung 2026 als produktionsreif bewertet wurden, erfolgt ihre Einführung ebenfalls in 2027.

3.3 Jahr 2028 – Umsetzung und erste Überprüfung

Im Jahr 2028 steht die operative Umsetzung der strategischen Entscheidungen aus 2027 im Vordergrund. Mit Auslaufen der IGEL-Lizenzen Ende 2028 ist eine Folgeentscheidung für das Secure-Endpoint-Modell zu treffen: Verlängerung des IGEL-Betriebs, Wechsel auf Linux-basierte gehärtete Endpunkte oder ein kombiniertes Modell. Diese Entscheidung ist in Abhängigkeit von der Betriebsmodellentscheidung Citrix, Hybrid oder Fat Client zu treffen und darf nicht isoliert bewertet werden.

Die flächendeckende DMS-Einführung soll 2028 abgeschlossen werden, sofern der Pilot 2027 erfolgreich verläuft. Ebenfalls in 2028 ist erstmalig eine strukturierte Überprüfung der Zielerreichung aller sechs Leitziele der Strategie durchzuführen. Die Ergebnisse sind zu dokumentieren; bei wesentlichen Abweichungen ist eine Fortschreibung einzelner Strategieelemente zu veranlassen.

3.4 Jahre 2029–2031 – Konsolidierung und Vorbereitung Folgestrategie

In der abschließenden Phase der Strategieperiode stehen Konsolidierung, Weiterentwicklung und Vorbereitung der Folgestrategie im Mittelpunkt. Das gewählte Betriebsmodell wird stabilisiert; das Open-Source-Portfolio wird auf Basis der bis 2028 gewonnenen Erfahrungen gezielt weiterentwickelt. Die jährlichen Umsetzungsberichte an die Verwaltungsführung werden in diesem Zeitraum zum etablierten Steuerungsinstrument.

Spätestens im Jahr 2030 ist mit der Vorbereitung einer Fortschreibung der IT-Gesamtstrategie ab 2031 zu beginnen. Grundlage hierfür sind der aktuelle Umsetzungsstand, die technologische Marktentwicklung sowie die geltenden rechtlichen und organisatorischen Rahmenbedingungen der kommunalen IT.

Die IT-Gesamtstrategie verfolgt für den Zeitraum 2026 bis 2031 sechs übergeordnete Ziele. Erstens ist die Betriebsstabilität aller kritischen Systeme sicherzustellen. Zweitens ist die digitale Souveränität der Stadt durch reduzierte Herstellerabhängigkeiten und den bevorzugten Einsatz offener Standards zu stärken. Drittens ist die Informationssicherheit systematisch an den Maßstäben des BSI-Grundschutzes auszurichten.

Viertens sind Digitalisierung und medienbrucharme Verwaltungsverfahren weiterzuentwickeln, einschließlich der OZG-orientierten Prozessdigitalisierung; hierbei bleibt

die Zusammenarbeit mit kommunalen Dienstleistern und Verbundstrukturen wesentlich. Fünftens sind Wirtschaftlichkeit und Skalierbarkeit aller IT-Entscheidungen anhand eines belastbaren Total-Cost-of-Ownership-Ansatzes zu bewerten. Sechstens ist das Endpunkt- und Desktop-Betriebsmodell technologieneutral zu steuern, sodass nach Abschluss der Gebäudesanierung eine erneute, ergebnisoffene Bewertung des künftig zweckmäßigen Betriebsmodells erfolgen kann.

4. Architekturprinzipien

Netzwerkarchitektur und Segmentierung

Die Netzwerkinfrastruktur der Stadt Schmallingenberg wird in eigener Verantwortung betrieben; externe Dienstleister werden für spezialisierte Aufgaben unterstützend hinzugezogen. Die strategische und operative Steuerung der Netzwerkinfrastruktur verbleibt beim IT-Sachgebiet. Dieses Modell sichert die unmittelbare Reaktionsfähigkeit bei Störungen und wahrt die Kontrolle über eine sicherheitskritische Kernkomponente der IT-Infrastruktur.

Ein verbindliches Netzwerksegmentierungskonzept ist erarbeitet und befindet sich in der schrittweisen Umsetzung. Teilbereiche sind bereits segmentiert; so ist das VoIP-Netz im Rathaus bereits als eigenständiges Segment realisiert, und die Außenstellen der Stadt sind netzwerktechnisch getrennt angebunden. Die vollständige Umsetzung des Segmentierungskonzepts ist im Strategiezeitraum fortzuführen und abzuschließen. Ziel ist eine Netzwerkarchitektur, die kritische Systeme, Nutzersegmente, Fachverfahrensumgebungen und ggf. ein Gastnetz voneinander trennt und damit die laterale Ausbreitung von Schadsoftware im Angriffsfall strukturell erschwert. Die Netzwerksanierung des Rathauses schafft hierfür ab Ende 2027 die vollständige technische Grundlage.

Datensicherung und Wiederherstellung

Die Datensicherung erfolgt auf Basis von Veeam Backup & Replication nach einer dokumentierten Backup-Strategie, die den anerkannten Best Practices für eine ransomware-resistente Sicherungsarchitektur folgt. Kernbestandteil ist die Umsetzung des Immutable-Backup-Prinzips, bei dem Sicherungskopien für einen definierten Zeitraum unveränderlich gespeichert werden und damit auch bei einem erfolgreichen Ransomware-Angriff auf die primäre Infrastruktur nicht verschlüsselt oder gelöscht werden können. Die zugehörige Backup-Richtlinie ist verbindlich und regelt Sicherungszyklen, Aufbewahrungsfristen, Verantwortlichkeiten und Wiederherstellungsprozesse.

Die Backup-Architektur ist als dauerhaft kritische Infrastrukturkomponente zu behandeln. Änderungen an der Sicherungsarchitektur bedürfen einer dokumentierten Freigabe durch das IT-Sachgebiet. Die Wiederherstellbarkeit der Sicherungen ist in regelmäßigen Abständen durch praktische Restore-Tests zu verifizieren; die Ergebnisse sind zu dokumentieren. Im Kontext des unter R-01 (s. Seite 13) beschriebenen Ausfallrisikos des primären Serverraums ist ergänzend zu prüfen, ob eine extern vorgehaltene oder räumlich getrennte Sicherungskopie die Wiederanlaufzeit im Katastrophenfall weiter reduzieren kann.

Monitoring und Betriebsüberwachung

Die kontinuierliche Überwachung der IT-Infrastruktur erfolgt durch den Einsatz eines externen Security Operations Center des Anbieters Arctic Wolf. Das SOC überwacht sicherheitsrelevante Ereignisse in Echtzeit, erkennt Anomalien und ermöglicht eine zeitnahe Reaktion auf Sicherheitsvorfälle. Darüber hinaus übernimmt das SOC das aktive Schwachstellenmanagement: Bekannte Schwachstellen in der eingesetzten Infrastruktur werden kontinuierlich erfasst, bewertet und priorisiert; die Behebung erfolgt in Abstimmung mit dem IT-Sachgebiet nach einem definierten Prozess. Dieser Ansatz ergänzt die internen Betriebskapazitäten des IT-Sachgebiets um eine spezialisierte Sicherheitsüberwachung und ein strukturiertes Vulnerability Management.

Ergänzend befindet sich ein netzwerk- und systembasiertes Infrastruktur-Monitoring auf Basis von PRTG im Aufbau. PRTG dient der Überwachung von Verfügbarkeit, Auslastung und Erreichbarkeit von Netzwerkkomponenten, Servern und Diensten und bildet die operative Grundlage für die unter den Erfolgskennzahlen definierten Verfügbarkeitsmessungen. Mittel- bis langfristig sind SOC-Monitoring und Infrastruktur-Monitoring als komplementäre, aufeinander abgestimmte Schichten zu betreiben: PRTG für den operativen Betriebsüberblick, Arctic Wolf für die sicherheitsorientierte Ereignisauswertung.

Die künftige IT-Architektur folgt verbindlichen Grundsätzen. Kernsysteme mit hoher Kritikalität, insbesondere Verzeichnisdienste, zentrale Datei- und Anwendungsdienste sowie fachverfahrensnahe Basiskomponenten, verbleiben grundsätzlich in kommunaler Hoheit auf eigener oder kommunal kontrollierter Infrastruktur. Dies dient der Verfügbarkeit, der Kontrollierbarkeit und der Wahrung der Datenhoheit.

Für neue oder ersetzbare Dienste ist vorrangig zu prüfen, ob Open-Source-Lösungen mit offenen Schnittstellen eingesetzt werden können. Dies betrifft insbesondere Collaboration-, Dateiablage-, Monitoring-, Automatisierungs- und Sicherheitswerkzeuge. Offene Standards und dokumentierte Schnittstellen sind bei Neuanschaffungen verbindliche Bewertungskriterien. Cloud-Dienste kommen nur dann in Betracht, wenn sie datenschutzrechtlich, organisatorisch und strategisch mit dem Ziel kommunaler digitaler Souveränität vereinbar sind.

5. Herstellerstrategie und digitale Souveränität

Die Stadt Schmallenberg verfolgt keine vollständige technische Autarkie, wohl aber eine kontrollierte Reduzierung kritischer Herstellerabhängigkeiten. Dieser Ansatz entspricht dem fachlichen Verständnis digitaler Souveränität in der öffentlichen Verwaltung, wonach Abhängigkeiten aktiv gesteuert und dort begrenzt werden sollen, wo funktional gleichwertige und wirtschaftlich tragfähige Alternativen verfügbar sind.

Vor diesem Hintergrund wird die bestehende Microsoft-Infrastruktur für Kernfunktionen weiterhin on premises betrieben. Eine strategische Verlagerung dieser Kernfunktionen in Microsoft-Cloud-Dienste ist nicht vorgesehen. Stattdessen wird ein Modell verfolgt, bei dem Microsoft-basierte Kernsysteme im eigenen Verantwortungsbereich stabil betrieben werden, während neue oder ablösbare Querschnittsdienste vorrangig mit Open-Source-Komponenten umgesetzt werden. Dies schafft schrittweise Handlungsspielräume und reduziert Lock-in-Effekte, ohne kurzfristig funktionskritische Umstellungen zu erzwingen.

Die Portfoliosteuerung erfolgt anhand einer Dreiteilung in nicht ersetzbare Kernsysteme, teilersetzbare Querschnittsdienste und neu zu besetzende Dienste. Nicht ersetzbare Kernsysteme verbleiben vorerst auf bewährten Plattformen. Teilersetzbare Dienste wie Dateiablage, Collaboration, Passwortmanagement oder Monitoring werden auf Migrationsfähigkeit geprüft. Neu zu besetzende Dienste sollen grundsätzlich anhand des Prinzips „Open Source zuerst“ bewertet werden. Diese Vorgehensweise ist für eine Kommune der Größenordnung Schmallenbergs belastbarer als ein Totalumbau der Gesamtlandschaft in kurzer Zeit.

6. Desktop-Betriebsmodell und Secure Endpoints

Die seit 1995 bestehende strukturelle Begrenzung der Arbeitsplatzverkabelung auf 100 Mbit/s war ein maßgeblicher Grund dafür, dass ein klassischer Fat-Client-Betrieb im Rathaus über Jahre nicht wirtschaftlich und technisch nur eingeschränkt sinnvoll war. Unter diesen Bedingungen war die Entscheidung für einen zentral bereitgestellten Citrix Published Desktop mit Secure Endpoints sachgerecht. Citrix Virtual Apps and Desktops ist für zentralisierte Bereitstellung von Desktops und Anwendungen ausgelegt und unterstützt die Auslieferung standardisierter Arbeitsumgebungen unabhängig vom konkreten Endgerät.

Dieses Modell ermöglicht einen Arbeitsplatz, der funktional „mitwandert“: Der persönliche Desktop folgt dem Nutzer unabhängig vom konkret genutzten Gerät oder Standort innerhalb der Verwaltungsgebäude. Dies ist insbesondere in einer Phase fortlaufender Sanierung und temporärer Umzüge organisatorisch vorteilhaft. Gleichzeitig werden lokale Datenhaltung und komplexe Client-Verwaltung weitgehend vermieden, was Sicherheits- und Betriebsaufwände reduziert.

Als Secure-Endpoint-Plattform wurde bislang insbesondere IGEL OS eingesetzt. Die Stadt Schmallingenberg wurde 2025 in diesem Zusammenhang für den IGEL Now and Next Award nominiert, was den gewählten Ansatz als fachlich beachtenswert ausweist. Perspektivisch wird ergänzend geprüft, ob Linux-basierte, gehärtete Secure-Endpunkte auf Basis von Linux Mint oder vergleichbaren Distributionen als lizenz- und souveränitätsfreundliche Alternative etabliert werden können. Maßgeblich ist dabei nicht die Produktbezeichnung, sondern die Fähigkeit, einen abgesicherten, administrativ beherrschbaren und persistenzarmen Endpunktbetrieb sicherzustellen.

Mit dem ab 1. Juli 2026 geltenden Anspruch der Mitarbeitenden auf einen Tag Homeoffice pro Woche – soweit arbeitstechnisch abbildbar – entsteht ein konkreter operativer Bedarf, der die strategische Endpunktentscheidung zeitlich vorzieht. Die bislang für den Zeitraum nach Abschluss der Rathaus-Sanierung vorgesehene ergebnisoffene Prüfung des Betriebsmodells wird daher durch ein parallel laufendes, praxisbasiertes Pilotvorhaben ergänzt: Im Rahmen eines laufenden Proof of Concept wird ein standardisiertes Notebook-Modell auf Basis von Linux Mint mit Dockingstation, YubiKey und zentralem Management über NinjaOne erprobt. Die Einführung orientiert sich zunächst am Kreis der Mitarbeitenden, für die Homeoffice-Zugänge beantragt werden; end-of-life-bedingte Ersatzbeschaffungen für auslaufende IGEL-Arbeitsplätze werden soweit möglich am gleichen Zielbild ausgerichtet.

Das Pilotvorhaben ist als bedarfsorientierter Einstieg konzipiert, der Erkenntnisse für die spätere strategische Gesamtentscheidung zum Betriebsmodell liefert. Fachverfahren und die zentrale Windows-Arbeitsumgebung werden auch in diesem Modell weiterhin über Citrix bereitgestellt; das Notebook fungiert als standardisierte, sichere Zugangskomponente. Nach Abschluss der Rathaus-Sanierung ist in geeigneten Bereichen ergänzend die Einrichtung von Shared Workplaces vorgesehen. Das standardisierte Notebook mit Dockingstation bildet hierfür die technische Grundlage, da Mitarbeitende ihren persönlichen Arbeitsplatz physisch mitführen und an beliebigen Dockingstationen aufnehmen können, ohne dass eine feste Gerätezuordnung je Arbeitsplatz erforderlich ist. Dies reduziert den Hardwarebedarf und unterstützt flexible Raumnutzungskonzepte nach der Sanierung. Die Detailplanung und Ergebnisse des Pilotprojekts sind in einem gesonderten Positionspapier zur strategischen Neuausrichtung der IT-Arbeitsplätze dokumentiert, das dem Verwaltungsvorstand zur Beschlussfassung vorgelegt wird.

7. Infrastrukturbedingte Zurückstellung von Softwareentscheidungen

Die strukturell unzureichende Arbeitsplatzverkabelung wirkte sich nicht nur auf das Desktop-Betriebsmodell aus, sondern auch auf die fachliche Priorisierung von Softwareeinführungen. Insbesondere die Einführung eines Dokumentenmanagementsystems wurde bislang zurückgestellt, weil die notwendige technische Grundlage für einen wirtschaftlichen und performanten Produktivbetrieb im Rathaus nicht hinreichend gegeben war. Die Zurückstellung war daher infrastrukturell verursacht und strategisch nachvollziehbar.

Mit Abschluss der baulichen und netztechnischen Sanierung entfällt dieser Hinderungsgrund. Die Strategie sieht deshalb vor, alle bislang aus Infrastrukturgründen verschobenen Softwarevorhaben systematisch zu inventarisieren, neu zu priorisieren und der Verwaltungsleitung in einer abgestimmten Entscheidungsfolge vorzulegen. Das Dokumentenmanagementsystem ist hierbei als prioritäres Folgeprojekt zu behandeln, weil es sowohl für die Prozessdigitalisierung als auch für Aktenführung, Recherche,

Nachvollziehbarkeit und medienbrucharme Vorgangsbearbeitung von zentraler Bedeutung ist.

Zielbild nach Abschluss der Sanierung

8. Ressourcenplanung

8.1 Personelle Ressourcen

Das IT-Sachgebiet der Stadt Schmallenberg ist mit vier Vollzeitstellen besetzt und im Hauptamt organisatorisch verankert. Diese Personalausstattung deckt den laufenden Betrieb, die Benutzerbetreuung, die strategische Steuerung sowie die Koordination externer Dienstleister ab. Angesichts des Aufgabenumfangs – Betrieb einer vollständigen kommunalen IT-Infrastruktur einschließlich Netzwerk, Server, Virtualisierungs Umgebung, Endpunkte, Fachverfahren und Informationssicherheit – ist die Personalausstattung als knapp, aber funktionsfähig zu bewerten.

Für den Strategiezeitraum 2026–2031 ist die Personalausstattung zu sichern. Ein Ausfall oder eine unbesetzte Stelle hätte bei dieser Größenordnung unmittelbare Auswirkungen auf Betriebsstabilität und Umsetzungskapazität. Vakanzen sind daher unverzüglich und vorrangig zu besetzen. Darüber hinaus ist für alle vier Stellen ein strukturiertes Wissensmanagement sicherzustellen, das kritisches Betriebswissen dokumentiert und nicht ausschließlich personengebunden vorhält. Dies betrifft insbesondere Systemdokumentationen, Konfigurationsstandards, Vertrags- und Lizenzübersichten sowie Eskalationswege zu externen Dienstleistern.

Im Strategiezeitraum sind außerdem gezielte Qualifizierungsmaßnahmen vorzusehen. Schwerpunkte ergeben sich aus den strategischen Vorhaben: Informationssicherheit, Open-Source-Administration, DMS-Einführungskompetenz sowie – je nach Betriebsmodellentscheidung – veränderte Anforderungen an Client-Management und Netzwerkbetrieb.

8.2 Externe Dienstleister und Verbundstrukturen

Die Südwestfalen-IT nimmt als kommunaler IT-Dienstleister eine zentrale Rolle in der IT-Versorgung der Stadt Schmallenberg ein. Leistungen der Südwestfalen-IT sind als fester Bestandteil der IT-Versorgung zu verstehen und bei der Ressourcenbetrachtung entsprechend einzuordnen. Die strategische Steuerungsverantwortung verbleibt jedoch vollständig bei der Stadtverwaltung; die Beauftragung externer Leistungen ist ein Instrument der Leistungserbringung, nicht der strategischen Führung.

Darüber hinaus werden für spezialisierte Aufgaben, insbesondere Informationssicherheit, Infrastrukturprojekte und Fachverfahrensbetreuung, externe Dienstleister beauftragt. Diese Beauftragungen sind wirtschaftlich zu steuern, vertraglich klar abzugrenzen und im IT-Portfolioregister zu dokumentieren. Eine strategisch unkontrollierte Ausweitung externer Abhängigkeiten ist zu vermeiden; die Entscheidung zwischen Eigenleistung, Verbunddienstleister und freiem Drittdienstleister ist bei jedem wesentlichen Vorhaben explizit zu treffen und zu begründen.

8.3 Finanzielle Ressourcen

Der IT-Haushalt der Stadt Schmallenberg gliedert sich in einen konsumtiven und einen investiven Anteil. Der konsumtive Anteil umfasst laufende Aufwendungen für Softwarelizenzen, Wartungsverträge, Dienstleistungen und Betriebsmittel; der investive Anteil deckt Infrastrukturinvestitionen, Hardwarebeschaffungen und größere Einführungsprojekte ab. Beide Anteile bewegen sich in einer für eine Kommune dieser Größenordnung vertretbaren, jedoch nicht großzügigen Größenordnung.

Für den Strategiezeitraum ist sicherzustellen, dass strategisch notwendige Vorhaben rechtzeitig in die Haushaltsplanung eingebracht werden. Dies betrifft insbesondere die DMS-

Einführung, die für das Haushaltsjahr 2027 als investives Vorhaben anzumelden ist, sobald die Entscheidungsvorlage auf Basis der Markterkundung vorliegt. Ebenso sind die aus der Betriebsmodellentscheidung 2027 resultierenden investiven Bedarfe, etwa für Endgeräte, Netzwerkkomponenten oder Lizenzen, frühzeitig zu ermitteln und für den Haushalt 2028 anzumelden.

Alle wesentlichen IT-Investitionsentscheidungen sind anhand einer Fünfjahres-Gesamtkostenbetrachtung Total Cost of Ownership zu bewerten, die neben Anschaffungskosten auch Betriebs-, Wartungs-, Schulungs- und Ablösekosten einschließt. Einzelne Beschaffungskosten ohne TCO-Betrachtung sind als Entscheidungsgrundlage nicht ausreichend.

8.4 Fördermöglichkeiten

Im Bereich der Digitalisierungsförderung für Kommunen bestehen grundsätzlich Möglichkeiten zur Ko-Finanzierung strategischer IT-Vorhaben, insbesondere im Kontext der OZG-Umsetzung, der Informationssicherheit und der digitalen Infrastruktur. Eine systematische Prüfung verfügbarer Förderprogramme des Bundes und des Landes Nordrhein-Westfalen ist für den Strategiezeitraum vorzusehen. Fördermittel sind dabei als ergänzendes Finanzierungsinstrument zu verstehen und ersetzen keine belastbare Haushaltsplanung. Vorhaben dürfen nicht allein von einer unsicheren Fördererwartung abhängig gemacht werden.

9. Erfolgskennzahlen und Steuerungsgrößen

Die Umsetzung der IT-Gesamtstrategie ist nicht allein durch die Durchführung von Maßnahmen, sondern durch deren nachweisbare Wirkung zu bewerten. Für die wesentlichen Leitziele werden daher Steuerungsgrößen definiert, anhand derer das IT-Sachgebiet den Umsetzungsstand jährlich im Rahmen des Umsetzungsberichts an die Verwaltungsführung dokumentiert. Die nachfolgenden Kennzahlen sind erstmalig festgelegt; Zielwerte sind als Orientierungsgrößen zu verstehen und können auf Basis der ersten Erhebungsjahre fortgeschrieben werden.

9.1 Leitziel 1 – Betriebsstabilität

Maßgebliche Steuerungsgröße ist die Verfügbarkeit kritischer Systeme, insbesondere der Citrix-Umgebung, der zentralen Dateidienste sowie der Netzwerkinfrastruktur. Als erstmals definierter Orientierungswert gilt eine Verfügbarkeit von mindestens 99,0 Prozent im Jahresmittel, gemessen an Werktagen während der regulären Betriebszeiten. Ergänzend wird die mittlere Entstörungszeit, also die Zeit von Störungsmeldung bis Wiederherstellung, als Qualitätsgröße erfasst. Basis der Messung ist das im IT-Sachgebiet eingesetzte Ticketsystem TOPdesk; alle betriebsrelevanten Störungen sind dort vollständig zu erfassen. Als Zielgröße für die mittlere Entstörungszeit bei kritischen Systemen gilt ein Richtwert von maximal vier Stunden im Regelbetrieb.

9.2 Leitziel 2 – Digitale Souveränität

Steuerungsgröße ist der Anteil der Dienste mit offenen Standards und dokumentierten Schnittstellen an neu eingeführten oder erneuerten Systemen. Ergänzend wird der Fortschritt der Kategorisierung des Systemportfolios nach „nicht ersetzbar“, „teilersetzbar“ und „neu zu besetzen“ als Vollständigkeitskennzahl erfasst; Ziel ist die vollständige Kategorisierung bis Ende 2026. Die Anzahl aktiv gesteuerter Herstellerabhängigkeiten in der Kategorie „kritisch“ ist jährlich auszuweisen und soll über den Strategiezeitraum nicht ansteigen.

9.3 Leitziel 3 – Informationssicherheit

Grundlage ist der im Rahmen des B-Hard-Projekts durchgeführte Sicherheitscheck, dessen Ergebnisse als Ausgangsbasis dienen. Steuerungsgröße ist der Umsetzungsgrad offener Maßnahmen aus dem B-Hard-Sicherheitscheck, ausgewiesen als Anteil erledigter gegenüber ursprünglich identifizierter Maßnahmen. Ziel ist die vollständige Abarbeitung aller

als kritisch eingestuften Maßnahmen bis Ende 2026 sowie aller verbleibenden Maßnahmen bis Ende 2027. Darüber hinaus ist die Anzahl sicherheitsrelevanter Incidents, klassifiziert nach Schweregrad, jährlich aus TOPdesk auszuwerten und der Verwaltungsführung zu berichten.

9.4 Leitziel 4 – Digitalisierung

Als beispielhafte Steuerungsgröße für die DMS-Einführung gilt der Anteil der Organisationseinheiten, die aktiv im DMS arbeiten, gemessen an der Gesamtzahl der für die Einführung vorgesehenen Einheiten. Diese Kennzahl ist ab dem Pilotstart 2027 zu erheben. Ergänzend wird die Anzahl digitalisierter Verwaltungsprozesse, also OZG-relevanter Leistungen mit medienbruchfreier Bearbeitung, jährlich fortgeschrieben.

9.5 Leitziel 5 – Wirtschaftlichkeit

Steuerungsgröße ist die Durchführung einer TCO-Betrachtung bei allen Investitionsentscheidungen oberhalb eines intern festzulegenden Schwellenwertes. Dies wird als Prozessmerkmal im IT-Portfolioregister dokumentiert. Ergänzend wird die Einhaltung der Haushaltsansätze für IT-Vorhaben als Abweichungsgröße jährlich ausgewiesen.

9.6 Leitziel 6 – Technologieneutrale Steuerung

Steuerungsgröße ist die termingerechte Vorlage der Betriebsmodellentscheidung an die Verwaltungsführung, Zieltermin nach Abschluss der Sanierung, spätestens Ende 2027. Diese Kennzahl ist binär – die Entscheidungsvorlage liegt vor oder nicht.

9.7 Berichtswesen

Die vorstehenden Steuerungsgrößen sind Bestandteil des jährlichen IT-Umsetzungsberichts, den das IT-Sachgebiet der Verwaltungsführung vorlegt. Der Bericht dokumentiert den Ist-Stand je Kennzahl, benennt Abweichungen vom Zielwert, erläutert deren Ursachen und schlägt gegebenenfalls Anpassungsmaßnahmen vor. Eine externe Berichtspflicht gegenüber dem Rat besteht nicht; die Steuerung erfolgt ausschließlich auf Ebene der Verwaltungsführung.

Mit dem Abschluss der Sanierung entsteht erstmals seit Errichtung des Rathauses eine technische Ausgangslage, auf deren Basis die bisherigen Grundsatzentscheidungen neu bewertet werden können. Dies betrifft insbesondere das künftige Desktop-Betriebsmodell, die Einführung bislang zurückgestellter Softwarelösungen sowie die generelle Frage, an welchen Stellen zentrale Bereitstellungsmodelle auch künftig Vorteile gegenüber dezentralen Clients bieten.

Die Strategie legt hierfür ausdrücklich keine Vorfestlegung fest. Vielmehr ist nach Abschluss der Sanierung eine ergebnisoffene Prüfung zwischen mindestens drei Zielmodellen vorzunehmen: erstens die Fortführung des zentralisierten Citrix-Modells, zweitens ein Hybridmodell mit zentralen und dezentralen Endpunkten je nach Arbeitsplatzprofil, drittens eine weitergehende Rückkehr zu leistungsfähigeren Fat-Client-Konzepten, soweit Fachverfahren, Sicherheitsanforderungen und Wirtschaftlichkeit dies tragen. Grundlage der Entscheidung sind eine belastbare Fünfjahresbetrachtung der Gesamtkosten, eine Sicherheitsbewertung, die Fachverfahrenskompatibilität und die praktische Eignung für die Verwaltungsorganisation.

Governance und Steuerung

10. Fachverfahren-Strategie

10.1 Überblick und Bestandsaufnahme

Die Stadt Schmallenberg betreibt ein breites Portfolio an Fachverfahren, das sowohl gehostete als auch lokal betriebene Lösungen umfasst. Die Fachverfahren decken alle wesentlichen kommunalen Aufgabenbereiche ab und werden organisatorisch durch

dezentrale Fachadministratoren in den jeweiligen Ämtern betreut. Die IT-Abteilung verantwortet die technische Infrastruktur sowie die zentrale Einspielung von Updates bei lokal betriebenen Verfahren; die inhaltliche Fachverantwortung verbleibt bei den zuständigen Organisationseinheiten.

Zu den gehosteten Fachverfahren zählen ab dem 1. Juli 2026 der Sitzungsdienst SD.Net des Anbieters Sternberg, sowie LOGA, VOIS-Meso, Autista, VOIS-Geso, AKDN Sozial und Votemanager. Lokal betriebene Fachverfahren umfassen ProSozBau, FlowChief, LogoData, MachFinanz+ und Avviso. Eigenentwicklungen existieren nicht; alle eingesetzten Lösungen sind Produkte externer Hersteller.

10.2 Sonderstellung des Finanzwesens

Eine strategisch bedeutsame Besonderheit der IT-Landschaft Schmallingenbergs ist das seit 2006 im Einsatz befindliche Finanzverfahren MachFinanz+, das autark und lokal betrieben wird. Dieses System funktioniert nach langjähriger Betriebserfahrung stabil und zuverlässig und bildet das Herzstück der kommunalen Finanzverwaltung. Es unterscheidet sich damit wesentlich vom Standard anderer Kommunen in der Region, die das Finanzverfahren Infoma über die Südwestfalen-IT betreiben.

Diese Eigenständigkeit ist strategisch als Vorteil zu bewerten: Sie reduziert die Abhängigkeit von der Südwestfalen-IT im besonders kritischen Bereich des Finanzwesens und sichert die Handlungsfähigkeit der Finanzverwaltung auch bei Störungen externer Dienstleister. Die Fortführung des autarken Betriebs von MachFinanz+ ist im Strategiezeitraum als Grundsatzentscheidung beizubehalten, solange das System stabil betrieben werden kann und keine zwingenden rechtlichen oder fachlichen Gründe eine Ablösung erfordern. Eine Migration auf andere Plattformen ist strategisch nicht vorgesehen.

10.3 Strategische Neuausrichtung bei der Dienstleisterauswahl

Der Sicherheitsvorfall bei der Südwestfalen-IT im Oktober 2023, in dessen Folge Fachverfahren über einen längeren Zeitraum nicht oder nur eingeschränkt verfügbar waren, hat die Bewertung externer Abhängigkeiten maßgeblich beeinflusst. Die Stadt Schmallingenberg hat daraus die Konsequenz gezogen, neue Fachverfahren zurückhaltend über die Südwestfalen-IT zu beauftragen und alternative Anbieter und Rechenzentren aktiv in die Beschaffungsüberlegungen einzubeziehen.

Diese Haltung entspricht dem in dieser Strategie verankerten Ziel der kontrollierten Reduzierung kritischer Abhängigkeiten. Sie bedeutet nicht den vollständigen Verzicht auf Leistungen der Südwestfalen-IT; laufende Verfahren werden weitergeführt. Bei jeder Neuanschaffung oder Ablösung eines Fachverfahrens ist künftig explizit zu prüfen, ob ein Angebot der Südwestfalen-IT, ein alternatives kommunales Rechenzentrum oder ein Direktanbieter den Anforderungen an Verfügbarkeit, Datenschutz, Wirtschaftlichkeit und Unabhängigkeit am besten entspricht.

10.4 Steuerungsgrundsätze für Fachverfahren

- **Bestandssicherung vor Ablösung:** Stabil laufende Fachverfahren werden nicht ohne zwingenden Grund abgelöst. Ablösevorhaben werden nur eingeleitet, wenn rechtliche Anforderungen, fehlender Herstellersupport oder wirtschaftliche Gründe dies erfordern.
- **Dezentrale Fachverantwortung, zentrale technische Verantwortung:** Die Konfiguration und fachliche Nutzung der Verfahren obliegt den Fachadministratoren in den Ämtern. Die IT-Abteilung verantwortet die technische Betriebsvoraussetzung, die Update-Versorgung bei lokal betriebenen Systemen sowie die Koordination mit externen Rechenzentren.
- **Dokumentation im IT-Portfolioregister:** Alle Fachverfahren sind im IT-Portfolioregister zu erfassen, einschließlich Hersteller, Betriebsmodell, Vertragspartner, Laufzeiten und Ablöserelevanz.

- **Dienstleisterdiversifizierung:** Bei Neubeauftragungen ist die Wahl des Rechenzentrums oder Anbieters explizit zu begründen. Eine Konzentration auf einen einzelnen Dienstleister ist zu vermeiden.
- **DMS als Querschnittskomponente:** Das Dokumentenmanagementsystem ist nicht als isoliertes Fachverfahren, sondern als Querschnittsinfrastruktur zu planen, die mit bestehenden Fachverfahren integriert werden muss. Die Schnittstellenfähigkeit zu den relevanten Bestandssystemen ist ein verbindliches Bewertungskriterium bei der Produktauswahl.

11. Risikokatalog

Die IT-Gesamtstrategie ist unter Berücksichtigung der wesentlichen Risiken zu planen und umzusetzen, die den IT-Betrieb, die Umsetzung strategischer Vorhaben oder die Handlungsfähigkeit der Verwaltung beeinträchtigen können. Der nachfolgende Risikokatalog erhebt keinen Anspruch auf Vollständigkeit im Sinne einer formalen Risikoanalyse nach BSI-Grundsatz; er benennt die strategisch relevanten Risiken, bewertet ihre Priorität und benennt die jeweils vorgesehene Steuerungsmaßnahme. Der Katalog ist Bestandteil des jährlichen IT-Umsetzungsberichts und bei wesentlichen Veränderungen der Risikolage fortzuschreiben.

Die Risikobewertung erfolgt anhand einer dreistufigen Prioritätseinstufung: **Hoch** bezeichnet Risiken mit potenziell gravierenden Auswirkungen auf den Verwaltungsbetrieb oder die Handlungsfähigkeit der Stadt; **Mittel** bezeichnet Risiken mit spürbaren, aber beherrschbaren Auswirkungen; **Niedrig** bezeichnet Risiken, die bei Eintreten handhabbar sind und keine wesentliche Betriebsunterbrechung verursachen.

Nr.	Risiko	Beschreibung	Priorität	Gegenmaßnahme
R-01	Totalausfall Serverraum / IT-Safe	Bei vollständiger Zerstörung oder dauerhafter Nichtverfügbarkeit des primären Serverraums durch höhere Gewalt existiert zwar eine Datensicherung in der nahegelegenen Stadthalle, jedoch kein betriebsbereites Ausweichsystem, das den Regelbetrieb unmittelbar weiterführen könnte. Der Neuaufbau würde zu einer erheblichen Betriebsunterbrechung führen.	Hoch	Im Strategiezeitraum ist zu prüfen, ob ein Notfallsystem mit Minimal-Serverbetrieb am Ausweichstandort etabliert werden kann. Bis dahin ist ein dokumentiertes IT-Notfallkonzept zu erstellen, das Wiederanlaufprozesse, Verantwortlichkeiten und Kommunikationswege beschreibt.
R-02	Ausfall oder eingeschränkte Verfügbarkeit externer IT-Dienstleister	Die Stadt Schmallingenberg ist für wesentliche Fachverfahren und Basiskomponenten auf externe Dienstleister angewiesen. Störungen oder Ausfälle auf Seiten	Hoch	Abhängigkeiten von externen Dienstleistern sind im IT-Portfolioregister vollständig zu dokumentieren. Für kritische Fachverfahren sind Notfallprozesse und Übergangslösungen zu definieren. Vertragliche Regelungen zur Verfügbarkeit

		dieser Partner können dazu führen, dass Fachverfahren über einen längeren Zeitraum nicht verfügbar sind und die Aufgabenerfüllung der Verwaltung erheblich eingeschränkt wird.		und Entstörung sind regelmäßig zu prüfen.
R-03	Personalausfall im IT-Sachgebiet	Bei einer Stellenstärke von vier Vollzeitstellen führt der gleichzeitige oder länger andauernde Ausfall einer oder mehrerer Personen zu einer unmittelbaren Kapazitätseinschränkung. Kritisches Betriebswissen ist bei kleinen IT-Einheiten erfahrungsgemäß stark personengebunden.	Hoch	Personalausfälle werden durch Serviceverträge mit externen Dienstleistern kompensiert. Ergänzend ist ein strukturiertes Wissensmanagement aufzubauen, das den Einsatz externer Unterstützung ohne Einarbeitungsverluste ermöglicht.
R-04	Verzögerung der Rathaus-Netzwerksanierung	Die Sanierung der Netzwerkinfrastruktur ist zentraler Enabler für mehrere strategische Folgeentscheidungen. Eine wesentliche Verzögerung über Ende 2027 hinaus würde den gesamten Maßnahmenrahmen verschieben und laufende Lizenz- und Vertragslaufzeiten zusätzlich belasten.	Mittel	Enge Abstimmung mit den bauverantwortlichen Stellen der Verwaltung; regelmäßige Statusabfrage des Sanierungsfortschritts. Bei absehbarer Verzögerung ist der Maßnahmenrahmen frühzeitig anzupassen und der Verwaltungsführung zu berichten.
R-05	Fehlentscheidung beim Betriebsmodellwechsel	Die nach Abschluss der Sanierung zu treffende Entscheidung über das Desktop-Betriebsmodell hat langfristige wirtschaftliche und technische Konsequenzen. Eine unzureichend fundierte Entscheidung birgt das Risiko kostspieliger Korrekturen.	Mittel	Die Entscheidungsvorlage ist auf Basis einer vollständigen Fünfjahres-TCO-Betrachtung, einer Sicherheitsbewertung und einer Fachverfahrenskompatibilitätsprüfung zu erstellen.
R-06	Scheitern oder Verzögerung der DMS-Einführung	Die DMS-Einführung ist ein komplexes Organisationsprojekt, das über die rein	Mittel	Sorgfältige Markterkundung und Pilotphase 2027 vor flächendeckender Einführung.

		technische Implementierung hinausgeht. Unzureichendes Änderungsmanagement, fehlende Nutzerakzeptanz oder eine ungeeignete Produktwahl können zu Verzögerungen oder einem Teilscheitern führen.		Einbindung der Fachbereiche von Beginn an.
R-07	Zunehmende Cyberbedrohungslage	Kommunen sind zunehmend Ziel von Cyberangriffen, insbesondere Ransomware. Die Bedrohungslage ist strukturell und unabhängig von der Größe der Kommune als dauerhaft erhöht einzustufen.	Hoch	Systematische Umsetzung der Maßnahmen aus dem B-Hard-Sicherheitscheck; Fortführung des SOC-gestützten Monitorings; regelmäßige Sensibilisierung der Mitarbeitenden; Backup-Strategie mit getrennter und unveränderlicher Datensicherung.
R-08	Lizenz- und Compliance-Risiken	Bei proprietären Softwareprodukten besteht das Risiko von Lizenzänderungen, Preiserhöhungen oder veränderten Nutzungsbedingungen, die kurzfristig Mehrkosten oder Handlungszwang erzeugen.	Mittel	Lizenz- und Vertragsübersicht im IT-Portfolioregister pflegen; Laufzeiten und Kündigungsfristen dokumentieren; strategische Ablösepfade für kritische Abhängigkeiten vorbereiten.
R-09	Wissensverlust durch Fluktuation oder Ruhestand	Auch wenn aktuell keine konkreten Vakanzen absehbar sind, besteht bei einem kleinen IT-Team grundsätzlich das Risiko, dass langjährig aufgebautes Erfahrungswissen durch Stellenwechsel oder Ruhestand verloren geht.	Niedrig	Strukturiertes Wissensmanagement und frühzeitige Nachfolgeplanung bei absehbaren Veränderungen in der Stellenbesetzung.

12. Datenschutz und Notfallplanung

12.1 Datenschutz

Die datenschutzrechtlichen Anforderungen der DSGVO sowie des Datenschutzgesetzes Nordrhein-Westfalen sind für den IT-Betrieb der Stadt Schmallenberg verbindlicher Rahmen. Der behördliche Datenschutzbeauftragte ist extern beim Hochsauerlandkreis bestellt; die Koordination zwischen Verwaltung und Datenschutzbeauftragtem erfolgt über eine im Hauptamt bestellte Verbindungsperson. Dieses Modell sichert die organisatorische Einbindung des Datenschutzes in die Verwaltungsabläufe und entspricht der gängigen Praxis in Kommunen dieser Größenordnung.

Das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO ist vorhanden und bildet die dokumentarische Grundlage für die datenschutzrechtliche Bewertung eingesetzter Systeme und Verfahren. Im Strategiezeitraum ist sicherzustellen, dass das Verzeichnis bei der Einführung neuer oder der Ablösung bestehender IT-Systeme aktuell gehalten wird. Die Einbindung der Verbindungsperson und des Datenschutzbeauftragten bei wesentlichen IT-Entscheidungen, insbesondere bei der DMS-Einführung, der Betriebsmodellentscheidung und der Bewertung von Cloud-Diensten, ist als verbindlicher Prozessschritt zu verankern.

Für alle neu eingeführten oder wesentlich veränderten Systeme ist eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO zu prüfen; bei hohem Risiko für die Rechte und Freiheiten natürlicher Personen ist sie durchzuführen. Die Verantwortlichkeit für diese Prüfung liegt beim IT-Sachgebiet in Abstimmung mit der Verbindungsperson.

12.2 Notfallplanung und Business Continuity

Die Stadt Schmallenberg verfügt über ein IT-Notfallhandbuch in Grundzügen, das Notfallkontakte, Eskalationswege und einen Wiederanlaufplan enthält. Diese Unterlagen sind im internen IT-Wiki dokumentiert und damit für das IT-Sachgebiet zugänglich. Dies ist als belastbare Ausgangsbasis zu bewerten; gleichwohl besteht im Strategiezeitraum Weiterentwicklungsbedarf in Bezug auf Vollständigkeit, Aktualität und praktische Erprobung.

Im Jahr 2025 wurde eine Stromausfall-Übung durchgeführt, die den Wiederanlauf der IT-Infrastruktur unter realen Bedingungen erprobt hat. Diese Übung ist als wertvolle Erfahrungsgrundlage zu nutzen; die gewonnenen Erkenntnisse sind in das Notfallhandbuch einzuarbeiten, sofern dies noch nicht erfolgt ist. Im Strategiezeitraum ist eine regelmäßige Erprobung von Notfallszenarien, mindestens alle zwei Jahre, als fester Bestandteil des IT-Betriebs zu etablieren. Dabei sind sowohl technische Szenarien wie Restore-Test und Systemausfall als auch organisatorische Szenarien wie Ausfall externer Dienstleister und Sicherheitsvorfall zu berücksichtigen.

Das Notfallhandbuch ist im Strategiezeitraum zu einem vollständigen IT-Notfallkonzept weiterzuentwickeln. Dieses soll mindestens folgende Bestandteile umfassen: eine Übersicht kritischer Systeme und ihrer Wiederanlaufpriorität, definierte Zielzeiten für Wiederherstellung und zulässigen Datenverlust bei kritischen Systemen, dokumentierte Eskalationswege zu internen Verantwortlichen und externen Dienstleistern sowie Kommunikationsprozesse gegenüber der Verwaltungsführung im Schadensfall. Die Federführung liegt beim IT-Sachgebiet; die Verwaltungsführung ist über den Stand der Notfallvorsorge im jährlichen Umsetzungsbericht zu informieren.

Ein besonderes Augenmerk gilt dem im Risikokatalog beschriebenen Szenario des Totalausfalls des primären Serverraums sowie dem Ausfall externer Dienstleister. Für beide Szenarien sind die Wiederanlaufprozesse im Notfallkonzept konkret zu beschreiben, einschließlich der Nutzung des Ausweichstandorts Stadthalle und der dort vorgehaltenen Datensicherung.

Die IT-Gesamtstrategie ist als Führungs- und Steuerungsdokument der Verwaltungsleitung zu verstehen. Die operative Umsetzung obliegt dem IT-Sachgebiet, die strategische Priorisierung und Freigabe wesentlicher Richtungsentscheidungen verbleibt jedoch bei der

Verwaltungsführung. Dies betrifft insbesondere Architekturgrundsätze, Herstellerstrategie, größere Infrastrukturentscheidungen und das Zielbild für das Endpunktmodell.

Die Umsetzung der Strategie ist in einem IT-Portfolioregister zu hinterlegen. Darin sind laufende Vorhaben, zurückgestellte Maßnahmen, technische Hinderungsgründe, Zieltermine, Verantwortlichkeiten und Abhängigkeiten nachvollziehbar zu dokumentieren. Für strategisch wesentliche Themen ist mindestens jährlich ein strukturierter Umsetzungsbericht vorzulegen. Dadurch wird sichergestellt, dass technische Entwicklungen, Marktentwicklungen und Ergebnisse der Gebäudesanierung geordnet in die Fortschreibung der Strategie einfließen.

13. Wirtschaftlichkeit und Entscheidungsgrenzen

13.1 Schwellenwerte für strategische IT-Entscheidungen

Der im Kapitel „Governance und Steuerung“ verankerte Grundsatz, wesentliche IT-Richtungsentscheidungen der Verwaltungsführung als Entscheidungsvorlage vorzulegen, ist verbindlich anzuwenden für:

- alle IT-Vorhaben mit einem Gesamtvolumen (Investition und Betrieb über fünf Jahre) von mindestens 50.000 Euro sowie
- alle Vorhaben von strategischer Relevanz, unabhängig vom finanziellen Umfang.

13.2 Definition strategischer Relevanz

Ein IT-Vorhaben gilt als strategisch relevant, wenn mindestens eines der folgenden Kriterien erfüllt ist:

- Einführung oder Ablösung eines verwaltungskernrelevanten Fachverfahrens (z. B. Finanzverfahren, Ratsinformationssystem, Zeiterfassung)
- grundlegende Änderung von Arbeitsabläufen oder Organisationsstrukturen
- wesentliche Auswirkungen auf Informationssicherheit, Datenschutz oder Verfügbarkeit
- Einführung neuer plattform- oder architekturprägender Technologien
- Aufbau neuer oder erhebliche Änderung bestehender Abhängigkeiten von externen Dienstleistern oder Herstellern

Die Einstufung eines Vorhabens als strategisch relevant erfolgt durch das IT-Sachgebiet in Abstimmung mit der Hauptamtsleitung.

13.3 Wirtschaftlichkeitsanforderungen

Für alle Vorhaben, die unter diese Regelung fallen, ist eine strukturierte Wirtschaftlichkeitsbetrachtung durchzuführen. Diese umfasst mindestens:

- eine Fünfjahres-Gesamtkostenbetrachtung (Total Cost of Ownership) einschließlich Beschaffung, Betrieb, Wartung, Schulung und Ablösung
- eine Darstellung von mindestens zwei Handlungsoptionen (z. B. Beibehaltung gegenüber Neubeschaffung)
- eine Bewertung nicht-monetärer Faktoren, insbesondere Informationssicherheit, organisatorische Auswirkungen sowie Abhängigkeiten von Herstellern oder Dienstleistern

Die Wirtschaftlichkeitsbetrachtung ist Bestandteil der Entscheidungsvorlage und revisionssicher zu dokumentieren.

14. Maßnahmenrahmen 2026–2031

Im ersten Umsetzungsabschnitt ist ein vollständiges IT-Portfolioregister aufzubauen oder fortzuschreiben. Parallel sind die bestehenden Herstellerabhängigkeiten strukturiert zu erfassen und den Kategorien „nicht ersetzbar“, „teilersetzbar“ und „neu zu besetzen“ zuzuordnen. Weiterhin ist die Dokumentation aller aus Infrastrukturgründen zurückgestellten Vorhaben, insbesondere des DMS, zu vervollständigen.

Im zweiten Umsetzungsabschnitt sind Open-Source-Optionen für Querschnittsdienste, etwa im Bereich Collaboration, Passwortmanagement und Monitoring, pilotfähig zu bewerten und soweit sinnvoll produktiv einzuführen. Parallel ist das bestehende Citrix-/Secure-Endpoint-Modell bis zum Abschluss der Sanierung stabil weiterzuführen.

Im dritten Umsetzungsabschnitt, nach Vorliegen der sanierten Infrastruktur, erfolgt die Neubewertung des Desktop-Betriebsmodells einschließlich der Prüfung eines Hybridansatzes. Zugleich ist das DMS als priorisiertes Vorhaben entscheidungsreif vorzubereiten. Die Ergebnisse sind der Verwaltungsleitung als integrierte Entscheidungsvorlage vorzulegen.

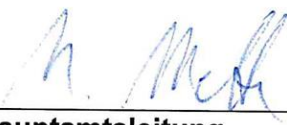
15. Strategische Bewertung

Die vorliegende Strategie ist für eine Kommune der Größenordnung Schmallingenbergs belastbar, weil sie nicht auf modischen Technologiewechseln, sondern auf den konkreten betrieblichen Rahmenbedingungen der Verwaltung aufsetzt. Sie verbindet Stabilität im Bestand mit schrittweiser Modernisierung, berücksichtigt die besondere infrastrukturelle Ausgangslage des Rathauses und vermeidet strategische Fehlentscheidungen, die aus unzureichender technischer Basis heraus entstehen würden.

Zugleich schafft sie einen nachvollziehbaren Handlungsrahmen für die Zeit nach Abschluss der Sanierung. Sie ermöglicht, bis dahin tragfähige Betriebsmodelle fortzuführen, ohne die spätere Neubewertung zu verbauen. Damit ist sie sowohl aus Sicht des IT-Managements als auch aus Sicht einer rechtssicheren, wirtschaftlich ausgerichteten Verwaltungssteuerung konsistent und anschlussfähig.

16. Freigabevermerk

Funktion	Zuständigkeit
Erstellt durch	Hauptamt / Sachgebiet IT
Fachlich geprüft	Mit Informationssicherheitsaufgaben betraute Stelle
Zur Freigabe	Hauptamtsleitung
Freigegeben durch	Bürgermeister der Stadt Schmallingenberg

Datum, Unterschrift	Datum, Unterschrift
11.06.2026	11.06.2026
	
Hauptamtsleitung	Bürgermeister der Stadt Schmallingenberg