Regierungsrat des Kantons Schwyz

kantonschwyz

Beschluss Nr. 227/2026
Schwyz, 24. März 2026 / jh
Versandt am: 31. März 2026

Einführung von Microsoft 365
Beschluss

1. Übersicht

Die kantonale Verwaltung plant die Einführung von Microsoft 365, um die Verwaltung moderner, effizienter und nutzerorientierter zu gestalten. Dies ist ein strategisch wichtiger Schritt zur Modernisierung und Digitalisierung der Arbeitsabläufe und Zusammenarbeit. In RRB Nr. 148/2025 wurde die Beschaffung von Dienstleistungen u. a. zur Konzeption der Einführung von Microsoft 365 bewilligt. Ein Entscheid zugunsten von Microsoft 365 wurde damals nicht getroffen. Zwischenzeitlich liegen diese Konzepte vor: Die Nutzung von Microsoft 365 wurde rechtlich durch eine spezialisierte und zu diesem Zweck beauftragte Anwaltskanzlei geprüft und entspricht den kantonalen und nationalen Vorgaben zum Datenschutz und zur Informationssicherheit. Besonders schützenswerte Personendaten und vertrauliche Informationen dürfen in Microsoft 365 verarbeitet werden, geheime Informationen bleiben lokal gespeichert. Die Risiken bezüglich eines unberechtigten Zugriffes durch den Cloud-Anbieter oder die Herausgabe an ausländische Behörden werden durch technische, organisatorische und vertragliche Massnahmen minimiert. Die Gesamtrisikobetrachtung zeigt unter Beachtung dieser Massnahmen, dass Microsoft 365 das Sicherheitsniveau und die Verfügbarkeit der Kommunikations- und Kollaborationsbasisdienste im Vergleich zur bisherigen Lösung deutlich erhöht. Zu den Chancen zählen eine gesteigerte Produktivität, die Einführung moderner Arbeitskonzepte wie die Zusammenarbeit mit externen Partnern und die Nutzung von Online-Meetings, eine verbesserte Cybersicherheit, eine erhöhte Arbeitgeberattraktivität sowie kontinuierliche Innovationen und die nachhaltige Zukunftssicherung der IT-Infrastruktur. Durch den Einsatz von Microsoft 365 bieten sich für die kantonale Verwaltung wesentliche Vorteile, die den Einsatz von Alternativen im Open Source-Bereich überwiegen. Zu den Vorteilen gehören neue, dringend benötigte Funktionalitäten, niedrigere Einführungskosten, da die Bedienung der Anwendungen der vertrauten Umgebung entspricht, schnelle Verfügbarkeit, geringerer Personalaufwand und viele erfolgreiche Umsetzungen.

Die Einführung erfordert zusätzliche personelle Ressourcen (3 FTE) und externe Unterstützung. Die Kosten für die Einführung und den Betrieb wurden bereits bewilligt, die unterjährige Erhö-

hung des Stellenplans erfolgt vorliegend. Das Amt für Informatik (AFI) wird beauftragt, die Integration unter Berücksichtigung der rechtlichen Vorgaben, den technologischen Rahmenbedingungen und organisatorischen Massnahmen in die bestehende IT etappenweise einzuführen. Die Umsetzung erfolgt in mehreren Phasen über rund zwei Jahre und umfasst die Migration von E-Mail und Telefonie sowie die Einführung von Kollaborationsplattformen (Teams), Backup/Restore sowie die Schulung der Mitarbeiter.

2. Ausgangslage

Das AFI hat mit der Genehmigung der IT-Strategie (vgl. RRB Nr. 923/2022) den Auftrag erhalten, in den strategischen Handlungsfeldern als innovativer Partner für Schub zu sorgen, damit sich der Kanton Schwyz nutzerzentriert weiterentwickelt. Mit der Einführung von Microsoft 365 sollen u. a. die Handlungsfelder «New Work und mobiles Arbeiten unterstützen», «Anforderungsorientierte Services anbieten», «Projekte geordnet abwickeln» weiter ausgebaut werden. Im Kontext dieser Rahmenbedingungen hat das AFI in Zusammenarbeit mit den Departementen und der Staatskanzlei eine Evaluation einer modernen und zeitgemässen Office-, Kommunikations- und Kollaborationslösung mittels Microsoft 365 durchgeführt. Basierend auf einem «Request for Information» im Sommer 2023 wurden sechs Anwendungsbeispiele (Use Cases) für Microsoft 365, ergänzende Dienstleistungen und das Microsoft 365 Backup und Restore ausgeschrieben. Die gewonnenen Erkenntnisse flossen im Anschluss in den weiteren Projektverlauf ein.

An einer ausserordentlichen Sitzung im Sommer 2024 hat der Regierungsrat entschieden, dass das AFI die strategische Ausrichtung von Microsoft 365 konzipieren und aufzeigen soll. Mit der Beschaffung wurden externe Dienstleistungen vergeben, um Microsoft 365 konzeptionell zielführend im Kanton zu implementieren, nahtlos in die bestehenden sowie zukünftigen Lösungen einzugliedern, die Sicherheit zu gewährleisten und die Ämter dabei zu unterstützen, die neuen Möglichkeiten in ihre Arbeitsprozesse einzubinden. Die Einführung von Microsoft 365 in der Verwaltung und deren Prozesse ist ein komplexes Unterfangen, das inhaltlich fundiert aufbereitet, ordentlich geplant und konsequent umgesetzt werden muss, damit der vorgesehene Mehrwert entstehen kann.

Die Einführung der Microsoft 365 Plattform im Kanton ist indes auch nahezu alternativlos, da sie im öffentlichen und privaten Umfeld bereits breite Anwendung findet und für die organisationsübergreifende Interaktion benötigt wird. Gemäss öffentlichen Quellen haben bereits über 20 Kantone die Einführung von Microsoft 365 geplant oder vorgenommen. Auch der Bund und etliche Gemeinden haben Microsoft 365 in Bezug auf ihre individuellen Anforderungen adaptiert erfolgreich eingeführt.

3. Einsatzgebiete

Mit der Einführung von Microsoft 365 werden sowohl neue Anwendungsbereiche erschlossen als auch bestehende Arbeitsprozesse optimiert, standardisiert und vereinfacht. Aufgrund des verwaltungsweiten Einsatzes sind die informatischen Ressourcen gemäss § 4 Bst. c der Verordnung über die Informationstechnologie vom 1. September 2015 (ITV, SRSZ 143.113) als Basisdienste einzustufen. Die Bereitstellung dieser Dienste gewährleistet eine effiziente, sichere und rechtskonforme Durchführung digitaler Arbeitsvorgänge. Darüber hinaus wird sichergestellt, dass etwaige Kompetenzlücken der Verwaltungsmitarbeiter durch gezielte Weiterbildungsmassnahmen geschlossen werden. In einer Teilrevision der IT-Verordnung (ITV) wird ein neuer Anhang geschaffen, in welchem dargestellt wird, welche Applikation für welches Einsatzgebiet verwendet werden soll.

Es sollen folgende Einsatzgebiete erschlossen oder angepasst und modernisiert werden.

3.1 Einsatzgebiet: Kommunikation und Kollaboration

Microsoft Teams ersetzt die bisherige Telefonielösung und übernimmt künftig die sprachbasierte Kommunikation, wobei die heutige Lösung von Avaya in reduziertem Umfang für Spezialfälle (wie z. B. Lifttelefone, Callcenter etc.) erhalten bleibt. Chats ermöglichen einen schnellen, schriftlichen Austausch, reduzieren insbesondere den internen E-Mailverkehr und erleichtern das Teilen von Dokumenten via Link. Videokonferenzen und Bildschirmfreigaben fördern die Zusammenarbeit auf Distanz durch zusätzliche nonverbale Kommunikation. Insgesamt dienen diese Kommunikationsformen der effizienten Abstimmung, Zusammenarbeit und schnellen Entscheidungsfindung innerhalb der Verwaltung und mit externen Partnern in Projekten. Ebenfalls kann Microsoft Teams zur strukturierten Sitzungsführung und Zusammenarbeit innerhalb von Amtsleitungen, Abteilungen und Fachgruppen verwendet werden. Darüber hinaus bietet Microsoft Teams die Möglichkeit, virtuelle Räume für die Kollaboration mit externen Partnern einzurichten. In diesen Räumen können gemeinsam Dokumente ausgetauscht und eine effiziente Zusammenarbeit gewährleistet werden.

Im Zuge der geplanten Einführung von Microsoft Teams ist eine Umstellung auf Exchange Modern Hybrid erforderlich. Diese Hybridform bezieht sich ausschliesslich auf das E-Mail-System und bedeutet nicht, dass die gesamte Microsoft-365- oder Server-Infrastruktur beliebig im Hybridbetrieb geführt werden kann. Beim Exchange Modern Hybrid bleiben alle produktiven Postfachinhalte – also E-Mails, Kontakte und Termine – weiterhin vollständig im eigenen Rechenzentrum des AFI gespeichert. In der Cloud werden lediglich die für die Zusammenarbeit notwendigen Basisinformationen wie Name, E-Mail-Adresse und Frei-/Gebucht-Informationen für Kalenderabfragen synchronisiert. Durch diese klar definierte und technisch abgesicherte Teil-Synchronisation können die vollständigen Funktionen von Microsoft Teams genutzt werden, ohne dass Postfachinhalte das lokale Rechenzentrum verlassen. Die Umstellung schafft zugleich die Voraussetzung, zusätzliche Sicherheits- und Schutzfunktionen für das E-Mail-System bereitzustellen. Diese dienen dazu, Nachrichten und Daten noch besser gegen Viren, Betrugsversuche und unbefugte Zugriffe zu schützen und unterstützen die langfristige IT-Strategie des AFI.

3.2 Informationsverwaltung

Um eine sichere und verlustfreie Übertragung von Daten und Informationen zum Abschluss eines Projekts zu gewährleisten und anschliessend die Archivierung im Staatsarchiv zu ermöglichen, wird bei Bedarf eine Verbindung zwischen einem spezifischen CMI Axioma-Geschäft und Microsoft 365 Team eingerichtet. Dadurch können die Informationen aus Microsoft 365 automatisiert in CMI Axioma übertragen werden. Hierfür werden geeignete Nutzungsempfehlungen sowie eine benutzerfreundliche Lösung mit definierbaren Einschränkungen implementiert, um zu steuern, welche Dokumente ausgetauscht werden dürfen. Ziel ist es, optimale Sicherheit und effiziente Zusammenarbeit sicherzustellen. Die Implementierung eines Backup- und Wiederherstellungskonzepts gewährleistet den Schutz vor Datenverlust, die Einhaltung gesetzlicher Vorgaben sowie die Sicherstellung der Informationsverfügbarkeit auch in Krisensituationen. Dabei werden insbesondere die Verfügbarkeit, Integrität und Nachvollziehbarkeit der Informationen sichergestellt. Microsoft 365 bietet mit der Power Plattform (z. B. Power Automate) erweiterte Möglichkeiten zur Prozessautomatisierung. Damit sollen gezielt ausgewählte Abläufe automatisiert werden – im Unterschied zum Projekt «Smart Services» (vgl. RRB Nr. 24/2026), das sich auf die Verwaltung, Bearbeitung und Einbindung von Formularen in den digitalen Schalter und innerhalb der kantonalen Verwaltung konzentriert.

3.3 Microsoft 365 in der Verwaltung

Die technologische Entwicklung und der Umstieg auf Microsoft 365 sind auch bereits in anderen Institutionen der öffentlichen Verwaltung im Kanton Schwyz umgesetzt.

Microsoft 365 wurde bereits an den Kantonsschulen Ausserschwyz, Kollegium Schwyz und den Berufsschulen, sowie beim HZI und HZA eingeführt. Die bisherigen Erfahrungen sind durchwegs positiv und der Austausch (best practices) ist etabliert. Die Ausgleichskasse des Kantons hat bereits begonnen, Microsoft 365 einzuführen. Es sind einige Dienste produktiv und im Laufe des Jahres 2026 sollen weitere Anwendungen aus Microsoft 365 folgen. Ebenfalls arbeiten einzelne Gemeinden bereits mit Microsoft 365 oder werden dieses in Kürze einführen.

Im Kanton Luzern wird Microsoft 365 seit einiger Zeit an den kantonalen Schulen eingesetzt. In der pädagogischen Umgebung (SLUZ) werden die Microsoft 365-Anwendungen täglich für den Unterricht verwendet und sind für die Lehrpersonen unverzichtbar. Microsoft 365 wird ebenfalls in kantonsnahen Organisationen wie z. B. bei Wirtschaft Arbeit Soziales (WAS), dem Kantonsspital Luzern (LUKS), der Luzerner Psychiatrie (LUPS), der Hochschule Luzern (HSLU) sowie bei der Stadt Luzern eingesetzt.

Die Freigabe zur Nutzung von Microsoft 365 ist beim Bund, in grösseren Kantonen wie Bern, Zürich, Basel-Stadt, St. Gallen oder Ob- und Nidwalden, welche dieselbe Datenschutzstelle haben, sowie in den Städten Zürich oder Bern bereits erfolgt.

4. Rechtliche Grundlagen

Mit Microsoft 365 werden Anwendungen wie Teams, Exchange, SharePoint und OneDrive künftig in Schweizer Microsoft-Rechenzentren betrieben und Informationen ebenda gespeichert. Dies stellt eine Auslagerung von kantonalen IT-Dienstleistungen nach § 30 ITV dar, welche unter Berücksichtigung der entstehenden Risiken grundsätzlich zulässig ist, sofern die gesetzlichen Vorschriften, insbesondere über den Datenschutz und die Informationssicherheit sowie den Finanzhaushalt eingehalten werden. Aufgrund der Betroffenheit von Basisdiensten ist die Auslagerung durch den Regierungsrat zu genehmigen (§ 31 Abs. 1 Bst. a ITV).

Das Projekt sieht vor, dass ausschliesslich Informationen mit den Klassifizierungen «öffentlich», «intern» und «vertraulich» in Microsoft 365 verarbeitet und gespeichert werden. Als «geheim» klassifizierte Informationen werden nicht in Microsoft 365 verarbeitet oder gespeichert. Informationen, die nicht mehr aktiv bearbeitet werden, sind gemäss den aktuell geltenden Vorschriften lokal in den hierfür vorgesehen Fachanwendungen aufzubewahren. Mit dem vorliegenden Projekt werden weder Fachanwendungen noch CMI Axioma oder die Datenablage Laufwerk I:\ ausgelagert.

Die geplante Einführung und Umsetzung von Microsoft 365-Diensten für zentrale Office-, Kommunikations- und Kollaborationslösungen ist rechtlich zulässig und erfüllt diesbezüglich die anwendbaren kantonalen Vorgaben. Diese Form der Bedarfsverwaltung dient nach § 4 Abs. 1 des Gesetzes über die Organisation des Regierungsrates und der kantonalen Verwaltung vom 27. November 1986 (RVOG, SRSZ 143.110) der effizienten und zweckmässigen Aufgabenerfüllung innerhalb der Verwaltung. Für das Wirkungsfeld der Beschaffung und Nutzung von Basisdiensten in der kantonalen Verwaltung wirkt weiter die ITV als spezialgesetzliche Vollzugsverordnung koordinierend. Der verwaltungsinterne Einsatz der M365-Dienste stellt Dienstleistungen im Bereich IT dar, für die das AFI zuständig ist. Die Auslagerung von digitalen Leistungen an beauftragte Dritte ist über die §§ 4 Bst. e, 30 und 31 ITV explizit geregelt. Da die M365-Dienste als digitale Leistungen zudem nicht unmittelbar der Ausübung hoheitlicher Befugnisse dienen oder eine Form der Eingriffsverwaltung darstellen, braucht es keine (formell-) gesetzliche Grundlage für die Auslagerung oder ihren Einsatz (vgl. Machbarkeitsbericht, Ziffer A.1).

Die Bearbeitung von Personendaten, einschliesslich besonders schützenswerter Personendaten, richtet sich nach den, für die jeweilige öffentliche Aufgabenerfüllung einschlägigen rechtlichen Grundlagen und dem Gesetz über die Öffentlichkeit der Verwaltung und den Datenschutz vom

23. Mai 2007 (ÖDSG, SRSZ 140.410) sowie der Verordnung zum Öffentlichkeits- und Datenschutzgesetz vom 28. Oktober 2008 (ÖDSV, SRSZ 140.411).

Eine schriftliche Vereinbarung nach § 30 Abs. 2 ITV, über das von der Digitalen Verwaltung Schweiz (DVS) mit Microsoft verhandelte Vertragswerk, gewährleistet umfassende datenschutzrechtliche Garantien, Weisungsrechte und Kontrollmöglichkeiten für den Kanton. Microsoft verpflichtet sich darin zur Einhaltung der schweizerischen Datenschutzrechte (inklusive kantonaler Datenschutzbestimmungen) und sichert zu, Daten nur nach Weisung und im Interesse des Kantons zu bearbeiten. Das Amtsgeheimnis, wie es seinen Niederschlag in § 35 des Personal- und Besoldungsgesetzes vom 26. Juni 1991 (PG, SRSZ 145.110) und Art. 320 des Schweizerischen Strafgesetzbuches vom 21. Dezember 1937 (StGB, SR 311.0) findet, ist kategorisch von der informationssicherheitsrechtlichen Klassifizierungsstufe «geheim» nach § 16a ITV zu unterscheiden. Es erfüllt eine Doppelfunktion und schützt sowohl das berechtigte Geheimhaltungsinteresse, der mit dem Staat kommunizierenden Privaten sowie genuin staatliche Interessen zur Vertraulichkeit behördlicher Tätigkeiten. Deshalb können auch als intern klassifizierte Informationen nach § 16a ITV unter das Amtsgeheimnis fallen.

Tatbestandsmässig setzt eine Verletzung des Amtsgeheimnisses (im Sinne von Art. 320 Ziff. 1 StGB) voraus, dass eine nicht offenkundige und nicht allgemein zugängliche Tatsache, an deren Geheimhaltung ein berechtigtes Interesse besteht, einem Unbefugten offenbart wird (BGer 142 IV 65 E. 3.1.1). Das Bundesgericht hat in BGer 6B_825/2019 weiter präzisiert, dass ein Geheimnis offenbart, wer es einem Unbefugten zur Kenntnis bringt oder ihm die Kenntnisnahme zumindest ermöglicht. Durch die vertragliche Einbindung von Microsoft als Hilfsperson wird sichergestellt, dass selbst in den seltenen Fällen eines technisch notwendigen Zugriffs keine strafbare Offenbarung geheimer Tatsachen erfolgt (vgl. § 20 Abs. 1 ÖDSG analog). Weiter ist im Bereich des sogenannten Confidential Computings, bei dem die Informationen in hardwarebasierten und speziell isolierten Bereichen mit einer End-zu-End Verschlüsselung getrennt vom restlichen System bearbeitet werden, der Klartextzugriff durch Systemadministratoren nicht ermöglicht. Die Datenspeicherung erfolgt zudem in Schweizer Rechenzentren. Für allfällige grenzüberschreitende Datenflüsse ausserhalb der EU/EFTA, die im Normalbetrieb nicht vorgesehen sind, bieten die vertraglichen Regelungen (u. a. EU-Standardvertragsklauseln) und das Swiss-U.S. Data Privacy Framework einen angemessenen Schutz im Sinne von § 18 ÖDSG. Normalbetrieb meint hierbei, dass das Cloud-Angebot wie geplant von der Anbieterin betrieben wird. Dies steht im Gegensatz zu den ausserordentlichen Situationen, die dem Normalbetrieb gerade nicht zuzurechnen sind (z. B. Konkurs der Anbieterin, Behördenzugriff auf das Cloud-Angebot, Zugriffe von Kriminellen auf das Cloud-Angebot).

Als Querschnittsinfrastruktur für die gesamte kantonale Verwaltung ist M365 zudem im Kontext aller besonderen Geheimnispflichten zu beurteilen, die bei verschiedenen Verwaltungseinheiten gesetzlich verankert sind, namentlich das Steuergeheimnis (§ 130 des Steuergesetzes vom 9. Februar 2000 [StG, SRSZ 172.200]), das Sozialhilfegeheimnis, das Geheimnis der Opferhilfeberatungsstellen (Art. 11 des Bundesgesetzes über die Hilfe an Opfer von Straftaten vom 23. März 2007 [OHG, SR 312.5]) sowie das Berufsgeheimnis bei kantonal betriebenen Gesundheitseinrichtungen (Art. 321 StGB). Für alle diese Bereiche gilt gleichermassen, dass die Klassifizierungsstufe «geheim» nach § 16a ITV nicht mit dem jeweiligen gesetzlichen Geheimnisschutz deckungsgleich ist.

Im Ergebnis kann auf der Grundlage des DVS-Vertragswerks, der vertraglich verankerten Geheimhaltungspflichten sowie der Massnahmen gegen Klartextzugriffe vertretbar argumentiert werden, dass im vorgesehenen Betrieb weder eine vollendete Amtsgeheimnisverletzung noch ein strafrechtlich vorwerfbarer Eventualvorsatz vorliegen, sofern Klartextzugriffe im Normalbetrieb technisch ausgeschlossen sind und das Risiko ausserordentlicher US-Behördenzugriffe auf kantonale Verwaltungsdaten aufgrund der faktischen Unwahrscheinlichkeit risikobasiert als vertretbar einge-

stuft, technisch durch besondere Verschlüsselungsverfahren des Confidential Computings limitiert und nachvollziehbar dokumentiert wird. Informationen mit besonderem gesetzlichen Geheimnisschutz sowie geheime Unterlagen nach § 16a ITV bleiben von der Bearbeitung in M365-Cloud-Anwendungen ausgeschlossen. Die massgeblichen Abgrenzungskriterien, Zugriffskontrollen und technischen Massnahmen sind im ISDS-Konzept festgelegt und werden dort umfassend beschrieben. Ergänzend kommt auch die umfassende rechtliche Machbarkeitsprüfung durch die Anwaltskanzlei [redacted] vom 13. Dezember 2024 (aktualisiert am 18. Februar 2026) in Zusammenarbeit mit dem Projektteam zum gleichen Ergebnis. Bei der geplanten sachgemässen und risikoorientierten Umsetzung der Nutzung von Microsoft 365 stehen für Informationen bis zur Klassifizierungsstufe «vertraulich» sowie für besonders schützenswerte Personendaten keine gesetzlichen Schranken entgegen.

Aus dem Bereich des Datenschutzes wird vielfach die Auffassung vertreten, dass die Auslagerung von (besonders schützenswerten) Personendaten in die Microsoft-Cloud nur zulässig sei, wenn ein Klartextzugriff des Anbieters technisch vollständig verhindert wird. Darüber hinaus werden gleichsam Bedenken hinsichtlich der Herausgabe von Informationen an ausländische Behörden geäussert sowie zur Sicherstellung der Geheimniswahrung und der starken Herstellerabhängigkeit. Diese Auffassung wird vom Regierungsrat entsprechend der vorliegenden Argumentation und der geplanten Risikomitigierung nicht geteilt. Weder das Strafrecht noch das Datenschutzrecht fordern eine absolute «Null-Risiko-Garantie». Die vertragliche Einbindung von Microsoft als Hilfsperson genügt den Anforderungen des Amtsgeheimnisses (Art. 320 StGB) und das Restrisiko einer unautorisierten Herausgabe von Daten an ausländische Behörden wird durch die seitens Microsoft sowie seitens des Kantons implementierten Schutzmassnahmen auf ein Mindestmass reduziert. Die Ausgestaltung der Massnahmen und deren Einschätzung ist dem handelnden öffentlichen Organ überlassen, zumal dieses auch für die Datenbearbeitung durch Dritte verantwortlich bleibt (§ 20 Abs. 3 ÖDSG). Die strategische Beurteilung der Anbieterabhängigkeit obliegt zudem ohnehin der politischen Führung (vgl. nachfolgend Ziffer 5).

Werden die gesetzlichen aufgeführten Grundlagen, die ganz allgemein den Schutz von Daten zum Ziel haben, den heute technologischen fortgeschrittenen Möglichkeiten gegenübergestellt, so kann klar festgestellt werden, dass die technischen Mittel von Microsoft 365 dieses Schutzziel erfüllen und die vom Kanton verwalteten Daten vor der grössten Gefahr, einem erfolgreichen Cyberangriff, schützen kann.

5. Chancen und Risiken durch die Microsoft 365 Nutzung

Da Microsoft 365 Informationen und Daten in Rechenzentren von Microsoft speichert, müssen die Datenhoheit, die Datenschutzkonformität, die Ausfallsicherheit, potenzielle Angriffsflächen und die Bindung ans Unternehmen Microsoft im Sinne einer Risikoabwägung geprüft werden. Ebenso sind die Chancen des Einsatzes von Microsoft 365 zur Zielerreichung innerhalb der Verwaltung zu dokumentieren.

5.1 Chancen durch die Einführung von Microsoft 365

Die Einführung von Microsoft 365 eröffnet der Kantonsverwaltung zahlreiche Chancen, die über die reine Modernisierung des Arbeitsplatzes hinausgehen.

- Benutzerfreundlichkeit: Intuitive und einheitliche Oberfläche, einfache Bedienung und schnelle Einarbeitung ermöglichen effizientes Arbeiten und unkomplizierte Nutzung neuer Funktionen.
- Gemeinsame Dokumentenbearbeitung: Echtzeit-Co-Authoring verhindert Versionschaos, spart Zeit und ermöglicht, Aufgaben direkt aus Dokumenten heraus zuzuweisen.

- Effiziente Kommunikation: Chat-Funktionen und Anwesenheitsanzeigen fördern schnelle Abstimmung im Team und reduzieren den E-Mail-Verkehr erheblich.
- Zentrale Kommunikationsplattform: Alle Informationen, Kommunikation und Telefonie sind in Teams gebündelt – inklusive professioneller Telefoniefunktionen wie Voicemail, Anrufweiterleitung und Sprachdialogsystem.
- Vereinfachte Zusammenarbeit: Informationen und Dokumente stehen zentral zur Verfügung, auch für externe Partner. Planungstools wie Planner und To Do sind integriert.
- Moderne Online-Meetings: Direktes Einrichten und Durchführen von Meetings dank Teams-Kalender, hochwertige Audio-/Videoqualität, Bildschirmfreigabe und Transkriptionen.
- Zentrale Aufgabenverwaltung: Übersichtliche Aufgabenlisten für Einzelne, Teams und Ämter, klare Verantwortlichkeiten und transparente Fortschrittskontrolle.
- Digitalisierte Prozesse: Automatisierung wiederkehrender Aufgaben und Workflows wie Datenerfassung oder Genehmigungen, wodurch Wartezeiten und manuelle Tätigkeiten reduziert werden.
- Schliessen von bestehenden Fähigkeitslücken: Mit Microsoft Teams wird die Zusammenarbeit sowohl intern als auch mit externen Partnern deutlich erleichtert. Bestehende Herausforderungen, z. B. bei der Telefonieanlage oder beim Dokumentenaustausch mit Externen, werden gelöst.
- Hohe Verfügbarkeit und Sicherheit: Minimale Wartungsfenster, zuverlässige Nutzung aller Dienste sowie automatische Sicherheits- und Funktionsupdates.
- Mobilität und Geräteunabhängigkeit: Einfacher Zugriff auf E-Mails, Dokumente und Termine von überall und auf verschiedenen Geräten (Notebook und Smartphone) sorgt für flexible und nahtlose Arbeitsabläufe.
- Cybersicherheit und Zukunftsfähigkeit: Die neuesten, von Microsoft laufend implementierten Technologien im Bereich Cybersicherheit sorgen für einen hohen Schutzgrad und passen sich rascher an neue Bedrohungen an. Dadurch bleibt die IT-Infrastruktur stets aktuell und technologisch zukunftsfähig.
- Attraktivität als Arbeitgeber: Moderne Anwendungen steigern die Arbeitgeberattraktivität, da viele Mitarbeiter diese von früheren Arbeitgebern, aus dem privaten Umfeld oder aus der Ausbildung kennen und erwarten. Die Verwaltung positioniert sich als fortschrittlicher und attraktiver Arbeitgeber.
- Innovation und kontinuierliche Verbesserung: Microsoft 365 bietet regelmässige Updates und neue Funktionen, sodass die Verwaltung von kontinuierlicher Innovation profitiert und zusätzliche Effizienzpotenziale eröffnet werden.

5.2 Technische, organisatorische und datenschutzspezifische Risikoabwägung

Es ist von zentraler Bedeutung, die technischen, organisatorischen und datenschutzspezifischen Risiken für das konkrete Einsatzgebiet zu kennen und zu minimieren.

Sämtliche Risiken im Zusammenhang mit der Nutzung von Microsoft 365 wurden systematisch in einem Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) dokumentiert, erläutert und bewertet. Es adressiert die Nutzung von Microsoft 365 bis und mit der Informationsklassifizierungskategorie «vertraulich» sowie besonders schützenswerte Personendaten. Die wesentlichen Risiken bei der Nutzung von Microsoft 365 oder den entsprechenden Lösungen im eigenen Rechenzentrum sind folgende:

Risiko von Datenverlust (und Datenabfluss):

Ein Datenverlust kann über einen unbefugten Zugriff auf das Rechenzentrum, durch die Exfiltration von Informationen durch Dritte (Cyberangriff), unerlaubten Datenaustausch ins Ausland, aufgrund von Sicherheitsverletzungen auf IT-Infrastrukturebene, Fehlverhalten von Benutzern und nicht zuletzt durch einen technischen Fehler im Rechenzentrum entstehen.

In Microsoft 365	Heute in eigenem Rechenzentrum (Fokus Teamwork, Mail, Kommunikation)
Microsoft betreibt hochsichere, mehrfach abgesicherte Rechenzentren mit physischem und digitalem Zugangsschutz. Verdächtige Aktivitäten werden rund um die Uhr überwacht. Neben der hochverfügbaren Datenhaltung durch Microsoft zum Schutz vor versehentlichem oder böswilligem Datenverlust werden externe Backuplösungen zur Wiederherstellung von gelöschten oder verschlüsselten Daten eingesetzt. Das Risiko eines Datenverlustes ist bei Microsoft 365 kleiner als beim lokalen Rechenzentrum wegen der integrierten Versionierung, dem automatischen Speichern und dem Papierkorb. Microsoft spricht davon, dass sie 34 000 Vollzeitäquivalente an Ingenieuren für Sicherheitsprojekte abgestellt haben (Quelle: Microsoft Digital Defense Report 2024, https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024).	[redacted]

Risiko eines Serviceausfalls (Verfügbarkeit):

Ein vollständiger oder teilweiser Ausfall von zentralen Diensten wie E-Mail, Telefonie und Teams kann zu Betriebsunterbrüchen, Produktivitätsverlusten oder finanziellen Schäden führen.

In Microsoft 365	Heute in eigenem Rechenzentrum (Fokus Teamwork, Mail, Kommunikation)
Microsoft garantiert für Microsoft 365 eine Verfügbarkeit von mindestens 99.90 %. Tatsächlich liegt sie noch höher. Unterbrüche durch Wartungsarbeiten gibt es keine. Zur Risikominimierung wurden in verschiedenen Departementen im Rahmen des Business Continuity Managements (BCM) leicht umsetzbare Massnahmen implementiert, [redacted]. Ein vorbereitetes BCM-Konzept sorgt allgemein dafür, dass die Organisation bei Störungen handlungsfähig bleibt – durch Notfallpläne, Wiederherstellungsplanung und Steuerung der Risiken.	Das Rechenzentrum ist teilweise redundant aufgebaut und bietet entsprechende Verfügbarkeit. Wartungsunterbrechungen sind Teil des Betriebs. Zur Risikominimierung wurden in verschiedenen Departementen im Rahmen des BCM leicht umsetzbare Massnahmen implementiert, [redacted].

Risiko von Lock-In Effekt:

Die Nutzung von Microsoft 365 birgt das Risiko eines Lock-In-Effekts, da zentrale digitale Funktionen wie Kommunikation, Datenverarbeitung und Kollaboration stark an einen Anbieter gebunden sind. Dies kann auch die digitale Souveränität einschränken, weil Kontrolle über Datenflüsse, Speicherorte und technologische Entscheidungsfreiheit verloren geht.

In Microsoft 365	Heute in eigenem Rechenzentrum (Fokus Teamwork, Mail, Kommunikation)
Das Risiko eines Lock-In-Effekts ist erkannt und wird im Projekt durch vertragliche, technische und organisatorische Vorkehrungen wie z. B. On-Prem-Backups in die AFI-Umgebung sowie durch eine definierte Rückführungsstrategie gemäss § 30 Abs. 3 ITV adressiert. Eine vollumfängliche Gewährleistung der Funktionsfähigkeit der kantonalen Verwaltung ohne Microsoft 365 kann in der Büroautomation kurzfristig nicht garantiert werden. Es existieren aktuell keine realistischen Alternativen zu den Microsoft-Lösungen in diesem Bereich, welche alle Anforderungen erfüllen. (Quelle: DVS Second Source – Studie https://www.digitale-verwaltung-schweiz.ch/application/files/4417/5084/6123/Studie-SecondSourceDVSV1.0.pdf). Eine Umstellung wäre mit erheblichen Zeit-, Kosten- und Schulungsaufwänden verbunden und müsste im Rahmen eines mehrjährigen Projekts erfolgen. Wenn Open Source wirklich eine geeignete Lösung darstellen würde, würden mehr kostenorientierte Unternehmen aus dem privaten Sektor darauf zurückgreifen.	Das AFI stellt die gängigen Office-Applikationen wie Word, Excel, PowerPoint zur Verfügung und betreibt über 50 Fachanwendungen mit Microsoft-Office-Integration oder enger Anbindung an Microsoft-Technologien und ist somit schon heute abhängig von Microsoft. Wer unabhängig von Microsoft sein will, muss auf deren Produkte verzichten. Open-Source-Office-Lösungen wie LibreOffice stehen kostenfrei zum Download zur Verfügung, erfordern jedoch eine umfassende Anpassung der IT-Betriebsmodelle sowie der etablierten Nutzung durch die Anwender. Die Abhängigkeit verschiebt sich von einem kommerziellen Anbieter wie Microsoft hin zu einer offenen Community, die von Non-Profit-Organisationen unterstützt wird. Leistungen, die bei Microsoft als Service angeboten werden, müssen bei Open-Source-Lösungen entweder durch externe Partnerunternehmen bereitgestellt oder eigenverantwortlich aufgebaut, betrieben und abgesichert werden. Alternative Kollaborationsplattformen wie Nextcloud bieten bestimmte Funktionalitäten, sind jedoch im öffentlichen Sektor bislang wenig etabliert und weisen Abhängigkeiten hinsichtlich des internen Betriebs auf. Open-Source-Lösungen werden im öffentlichen Sektor selten als vollwertiger Ersatz für die weit verbreitete Microsoft-Office-Palette genutzt. Das liegt nicht nur daran, dass das notwendige technische Know-how fehlt, sondern auch daran, dass eine solche Umstellung den Austausch mit der Umgebung erheblich einschränken könnte. In vielen Bereichen wäre der Kanton dadurch auf sich allein gestellt. Bei neuen Lösungen prüft das AFI jeweils, ob geeignete Open-Source-Anwendungen verfügbar sind.

Risiko von Kontrollverlust:

Dieses Risiko könnte entstehen, wenn die Kantonsverwaltung die Kontrolle über die Sicherheit, Verfügbarkeit und den Zugriff auf die Systeme und Daten der jeweiligen Lösung verlieren und dadurch die Richtlinien über die Nutzung von Daten nicht mehr durchsetzen könnte. Unabhängig von der Wahl des Betreibers bleibt die Verantwortung für den Einsatz sowie die damit verbundenen Informationen und Daten immer bei der kantonalen Verwaltung (Dateneigner).

In Microsoft 365	Heute in eigenem Rechenzentrum (Fokus Teamwork, Mail, Kommunikation)
Das Risiko eines Kontrollverlusts ist durch die vertraglich und technisch verankerten Steuerungs- und Sicherungsmechanismen	Der Betrieb der jeweiligen Lösungen im eigenen Rechenzentrum ermöglicht eine direkte Kontrolle, ist jedoch gleichzeitig mit einer

begrenzt. Der Kanton definiert eigenständig Zugriffsrechte, Datenflüsse und Speicherorte. Der Zugriff durch den Anbieter ist nur nach vorgängiger Genehmigung durch den Kanton möglich. Ergänzend gewährleisten transparente Audit- und Protokollierungsfunktionen, dass sämtliche relevanten Aktivitäten nachvollziehbar bleiben und die Einhaltung der kantonalen Richtlinien in allen Betriebsphasen durchgesetzt werden kann.
Als Antwort auf die veränderten politischen Rahmenbedingungen und geopolitischen Unsicherheiten hat Microsoft u. a. vertragliche Zusicherungen zugunsten von Regierungskunden in der EU und EFTA eingeführt, welche die Anfechtung von staatlichen Anordnungen zur Aussetzung von Onlinediensten regelt.

grösseren Verantwortung und erhöhten Risiken durch das kontinuierliche Nachführen von Sicherheitsmassnahmen verbunden. Sämtliche Anforderungen in den Bereichen Sicherheit, Compliance sowie Betriebsrisiken müssen eigenverantwortlich sichergestellt werden. Eine Abhängigkeit von Hard- und Software sowie die Übertragung von Kontrollfunktionen auf externe Dienstleister lässt sich auch beim Betrieb im eigenen Rechenzentrum nicht vollständig eliminieren. Die Umsetzung einer Open Source Strategie für die Office-Umgebung würde Jahre dauern, da Fachkräfte fehlen, und das Risiko der Abhängigkeit läge künftig im eigenen Betrieb.

Risiko der Herausgabe von Daten an US-Behörden aufgrund des US CLOUD Act:

Zur Aufklärung oder Verfolgung schwerer Straftaten erlauben verschiedene nationale Gesetze und insbesondere der US Stored Communications Act Strafverfolgungsbehörden die Herausgabe von Daten von Unternehmen, die diese in ihrem Besitz haben oder kontrollieren, und zwar selbst dann, wenn die Daten ausserhalb des fraglichen Staates aufbewahrt werden (so klärend festgehalten im sog. US CLOUD Act [Clarifying Lawful Overseas Use of Data Act]). In den USA benötigen die Strafverfolgungsbehörden hierzu eine richterliche Anordnung, die das Vorliegen eines verbrecherischen Sachverhalts bestätigt. Microsoft könnte in den USA auf diesem Weg verpflichtet werden, Daten, welche der Kanton Schwyz in einem Schweizer Rechenzentrum von Microsoft speichert, herauszugeben.

In Microsoft 365

Die empirischen Daten zeigen, dass seit Inkrafttreten des US CLOUD Act im Jahr 2018 im Kontext von Microsoft 365 keine Herausgaben aus EU/EFTA-Staaten an US-Strafverfolgungsbehörden erfolgt sind, die Kunden des öffentlichen Sektors betrafen. Die Eintrittswahrscheinlichkeit ist nach allem was heute bekannt ist, in tatsächlicher Hinsicht sehr gering. Die im Projekt verankerten umfassenden Massnahmen wie bspw. Datenhaltung ausschliesslich in der Schweiz und Verarbeitung jederzeit innerhalb Europas, umfassende Transport- und Ruhend-Verschlüsselung, umfangreiche vertragliche Zusicherungen und Abwehrmechanismen, Schweizer Recht und Gerichtsbarkeit etc. führen in der Gesamtheit zu einem faktisch sehr hohen Schutzniveau gegen unautorisierte Herausgaben von Daten an ausländische Behörden. Von einer rechtswidrigen Datenherausgabe muss unter den gegebenen Umständen nicht ausgegangen werden.

Heute in eigenem Rechenzentrum (Fokus Teamwork, Mail, Kommunikation)

Eine Herausgabe unter dem US CLOUD Act stellt beim Betrieb eines eigenen Rechenzentrums ein sehr kleines Risiko dar. Da jedoch meist Produkte von US-Anbietern verwendet werden, bleibt ein minimales Restrisiko bestehen.

5.3 Gesamtheitliche Einschätzung der Risiken und Chancen

Zusammenfassend lässt sich feststellen, dass die Einführung von Microsoft 365 im Vergleich zur heutigen Situation zu einer signifikanten Verbesserung des Gesamtrisikoprofils führt.

Insbesondere in den Bereichen Verfügbarkeit, Schutz vor Cybervorfällen und Datenverlust wird das Sicherheitsniveau durch die Nutzung der modernen, hochsicheren Infrastruktur von Microsoft markant erhöht. Die isolierte Betrachtung einzelner Risiken, die sich durch den Wechsel in Microsoft 365 leicht erhöhen, wie das theoretische Risiko einer Herausgabe von Daten in einem Strafverfahren unter dem US CLOUD Act, würde die Gesamtlage verzerren. Dieses spezifische Risiko wird durch umfassende vertragliche, technische und organisatorische Massnahmen wirksam mitigiert und als gering eingeschätzt. Demgegenüber steht eine deutliche Reduktion der Wahrscheinlichkeit und des potenziellen Schadensausmasses bei einer Vielzahl von weitaus realistischeren Bedrohungen. Die Entscheidung für Microsoft 365 stellt somit eine bewusste und fundierte Wahl für ein insgesamt höheres Schutzniveau und eine robustere IT-Infrastruktur dar. Davon sollen selbstredend grundsätzlich alle durch den Kanton im Rahmen des digitalen Arbeitsplatzes verarbeiteten Daten profitieren. Es ist wichtig zu erwähnen, dass der grösste Teil der Daten weiterhin in den bestehenden Fachanwendungen und in CMI Axioma lokal auf den kantonseigenen Systemen gespeichert bleibt.

Microsoft 365 ist derzeit marktführend und ausschliesslich über Microsoft verfügbar. Trotz dieser Anbieterbindung profitiert die Kantonsverwaltung von kontinuierlicher Innovation und professionellem, hochsicherem Betrieb, ohne dabei die Kontrolle über zentrale Aspekte oder die Datenhoheit zu verlieren. Insgesamt bietet Microsoft 365 vielfältige Chancen, um die digitale Zusammenarbeit und Modernisierung der Verwaltung nachhaltig zu stärken.

5.4 Abgrenzung der Nutzung von Microsoft 365

5.4.1 Grundsätzlicher Umgang mit unterschiedlichen Informationsklassifikationen

Der sachgerechte Umgang mit Personendaten und weiteren schutzbedürftigen Informationen ist von zentraler Bedeutung. Er ist bereits heute – unabhängig vom Einsatz von Microsoft 365 – im Arbeitsalltag der einzelnen Verwaltungseinheiten sicherzustellen und konsequent umzusetzen. Für die Nutzung von Microsoft 365 gelten für die vorgesehenen Use Cases die folgenden verbindlichen Vorgaben:

	§16a ITV				§4 ÖDSG	
Schutzstufe						
Use Case	**öffentlich**	**intern**	**vertraulich**	**geheim**	**Personendaten**	**Besonders schützenswerte Personendaten[1]**
Exchange Modern Hybrid	✓	✓	✓ 🔒	×	✓	✓ 🔒
Teamwork und Projektmanagement	✓	✓	✓	×	✓	✓
Kommunikation (exkl. E-Mail)	✓	✓	✓	×	✓	✓

✓: erlaubt, 🔒 nur verschlüsselter Versand, ×: verboten,

[1]: wenn Fachanwendungen vorhanden sind, müssen diese genutzt werden

Zur Sensibilisierung der Mitarbeiter des Kantons für die unterschiedlichen Schutzstufen wird im Rahmen der Einführung der jeweiligen Use Cases durch den Kantonalen Informationssicherheitsbeauftragten (KISB) gemeinsam mit den Dateneignern (in der Regel den Amtsvorstehern) eine

strukturierte Sichtung der relevanten Datenprozesse vorgenommen. Diese werden hinsichtlich ihrer Eignung und Zulässigkeit für die Bearbeitung in Microsoft 365 beurteilt. Gestützt auf diese Beurteilung erfolgt eine gezielte Schulung der Mitarbeiter zur korrekten Klassifizierung und Bearbeitung der Informationen und Daten bei der Nutzung von Microsoft 365. Sofern eine automatisierte Klassifizierung möglich und zweckmässig ist, wird diese eingesetzt.

5.4.2 Umgang mit geheimen Informationen im Kontext von Microsoft 365

Informationen werden je nach möglicher Beeinträchtigung öffentlicher Aufgaben bei unbefugter Kenntnisnahme in die Schutzstufen öffentlich, intern, vertraulich und geheim eingeteilt (siehe § 16a ITV). Für als «geheim» klassifizierte Informationen, die nur in Ausnahmefällen vorkommen, da ihre Offenlegung schwerwiegende Folgen für die öffentliche Sicherheit oder staatliche Interessen hätte, gelten erhöhte Sicherheitsanforderungen und zusätzliche Risiken. Daher wird festgelegt, dass solche Informationen derzeit nicht in Microsoft 365 verarbeitet werden dürfen. Ein vollständiger Umstieg auf Microsoft 365 ist somit aktuell nicht vorgesehen, was durch den parallelen Betrieb zu zusätzlichem Aufwand führt. Mittels Informationsklassifizierung kann technisch verhindert werden, dass als «geheim» klassifizierte Daten zu Microsoft 365 gelangen können.

5.4.3 Keine Fachanwendungen betroffen

Von der Einführung von Microsoft 365 ausgenommen sind die rund 600 Fachanwendungen, wie CARI, NEST, Abacus, Tribuna, CMI Axioma und die Aufbewahrung in CMI Axioma (GEVER). Ihre Daten werden weiterhin auf der bisherigen AFI-Infrastruktur verarbeitet und gespeichert. Sie behalten ihre zentrale Rolle für die Durchführung amtsspezifischer Aufgaben. Das Öffnen von Daten aus den Fachanwendungen heraus geschieht weiterhin lokal auf dem Client mit einer lokalen Installation von Microsoft Office (diese wird auch über Microsoft 365 lizenziert, ist jedoch lokal installiert). Derzeit ist lediglich die sichere Umsetzung von Schnittstellen zwischen CMI Axioma und Microsoft Teams vorgesehen, wobei nur eine kleine Auswahl der Daten aus CMI Axioma in Microsoft 365 bearbeitet wird. Dazu werden die Daten in Teams exportiert und später wieder in CMI Axioma importiert. Es werden keine Informationen mit der Klassifikation «geheim» ex- und importiert.

5.4.4 Kein Archivierungssystem

Microsoft 365 ist kein Ablagesystem zur Aktenführung, sondern ein Arbeitsmittel für die Zusammenarbeit. Geschäftsrelevante Informationen und Daten müssen weiterhin in Fachanwendungen oder im CMI Axioma abgelegt werden. Dokumente, welche in Projekten o. ä. erstellt werden, werden in Microsoft 365 erstellt und bearbeitet. Sobald diese Dokumente finalisiert sind, werden diese über eine Schnittstelle in CMI Axioma mit dem zugeordneten Geschäft synchronisiert und dem für die Aktenführung relevanten Dokumentenlebenszyklus hinzugefügt. Wenn die Geschäfte abgeschlossen sind und die Dokumente nicht mehr aktiv benötigt werden, werden diese automatisch in Microsoft 365 gelöscht. Diese sind anschliessend in CMI Axioma als ruhende Ablage auffindbar.

5.5 Folgen bei Verzicht auf Einführung von Microsoft 365

Ein vollständiger Verzicht auf die Einführung von Microsoft 365 hat erhebliche Auswirkungen auf die Digitalisierungsvorhaben und auf die Betriebsprozesse:

- Weiterhin nur reduzierte Möglichkeiten zur digitalen Zusammenarbeit: Die teamübergreifende Zusammenarbeit innerhalb der Verwaltung und mit externen Partnern wird primär durch Cloud-Dienste unterstützt. Beim Verzicht auf den Einsatz von Microsoft 365 und insbeson-

dere der Applikation Teams müssten alternative Anwendungen eingesetzt werden, die oft geringere Funktionalitäten besitzen und weniger tief in die bestehende Infrastruktur integriert sind. Diese heute bestehende Fähigkeitslücke könnte nicht geschlossen werden.
- Begrenzte Zukunftsfähigkeit: Microsoft und andere Lösungsanbieter verfolgen eine klare Cloud-Strategie und entwickeln viele Funktionen ausschliesslich für die Cloud weiter. Auch die Preisgestaltung fördert zunehmend den Umstieg. Zukünftig werden vermehrt nur noch cloudbasierte Lösungen angeboten, wie dies bereits heute oft bei KI-Lösungen der Fall ist.
- Schatten-IT: Fehlt eine zentrale Plattform wie Microsoft 365, kann dies dazu führen, dass Mitarbeiter nicht autorisierte Webanwendungen zur Erledigung ihrer Aufgaben, beispielsweise für die Dateiablage, die externe Kommunikation oder das Projektmanagement nutzen. Die Verwendung solcher Anwendungen kann zu mehrfachen Lizenzkosten, versteckten Abonnements sowie erhöhten Betriebsausgaben führen und birgt das hohe Datenschutzrisiko, dass Daten in nicht konformen Cloud-Umgebungen verarbeitet werden.
- Eingeschränkte Digitalisierungspotenziale: Ohne Zugriff auf Microsoft 365-Cloud-Dienste entfallen zahlreiche Optionen zur Optimierung von Büroprozessen und zur Automatisierung von Abläufen.
- Nachteile bei der Cybersicherheit: Sicherheitslösungen werden zunehmend als Cloud-Dienste bereitgestellt. Das Sicherheitsniveau, das über die Cloud erreicht werden kann, lässt sich im lokalen Betrieb mittelfristig nicht mehr vollständig abbilden.
- Sinkende Arbeitgeberattraktivität: Cloud-Lösungen sind im privaten Sektor weit verbreitet. Viele Mitarbeiter erwarten auch im beruflichen Umfeld (gleiche) moderne Anwendungen und möchten von deren dynamischer Weiterentwicklung profitieren.

6. Massnahmen zur Risikominimierung

Zur Minimierung der im Kapitel 5 erwähnten Risiken werden verschiedene technische, organisatorische und vertragliche Massnahmen (TOM) umgesetzt. Die sicherheitsrelevanten Konfigurationen für Microsoft 365 werden im Rahmen der Einführung definiert, laufend überprüft und bei Bedarf angepasst. So wird ein hoher Grundschutz entsprechend dem besonderen Schutzbedarf gewährleistet.

6.1 Technische Massnahmen

Zu den technischen Massnahmen gehören:

1. Nutzung neuer Sicherheitsfunktionen: Eine strikte Nutzung der in Microsoft 365 integrierten Sicherheitsfunktionen wie Mehrfaktor-Authentifizierung und rollenbasierter Zugriff zur Reduktion von Angriffsflächen.
2. Backup & Restore: Als Backup- und Wiederherstellungssysteme für Microsoft 365 werden die vorhandenen On-Premise-Systeme (lokal betrieben) auf der Infrastruktur des AFI genutzt. So wird sichergestellt, dass Cloud-Daten lokal auf der kantonalen Infrastruktur gesichert und vor unrechtmässigem oder versehentlichem Verlust geschützt sind.
3. «Evergreen»-Ansatz (Dienste werden automatisch mit Sicherheitsupdates versorgt): Services zur kontinuierlichen Schliessung von Sicherheitslücken und automatisierten Verbesserung der Software.
4. Regelbasierter Zugriff: Arbeitsbereiche oder Nutzerrechte werden je nach Standort, Gerät oder Zeitraum begrenzt.
5. Verhinderung von Datenverlusten: Systematische Überwachung von Massentransaktionen zur Erkennung und Verhinderung von Datenverlust oder Datenabzug.
6. Kontrollvorgang für Zugriffe von Microsoft (Customer Lockbox): Die Daten werden georedundant und verschlüsselt in Schweizer Rechenzentren gespeichert. Die zusätzlich vereinbarte

Massnahme «Customer Lockbox» stellt sicher, dass Microsoft-Supporttechniker nur mit ausdrücklicher Genehmigung der Kantonsverwaltung auf Daten zugreifen können. Jeder Zugriff wird protokolliert und Veränderungen werden aufgezeichnet.

6.2 Organisatorische Massnahmen

Organisatorische Massnahmen zur Risikominderung und zur Begleitung des Wandels der Arbeitsweise in der Verwaltung sind zentral. In der kantonalen Verwaltung sind vorderhand folgende Massnahmen vorgesehen:

1. Nutzungsempfehlung Microsoft 365: Die Nutzungsempfehlung Microsoft 365 wird vom AFI geführt und aktualisiert. Sie definiert verbindliche Regeln für den sicheren Umgang mit Microsoft 365. Es wird unter anderem geregelt, wie Informationen nach Schutzbedarf zu klassifizieren sind. Informationen werden in Microsoft 365 nur temporär verarbeitet, aber nicht dauerhaft gespeichert (kein Archiv). Geschäftsrelevante Informationen müssen weiterhin in Fachanwendungen oder CMI Axioma abgelegt werden, um eine korrekte Aktenführung und spätere Archivierung sicherzustellen. Nach Abschluss eines Geschäfts werden die Daten aus Microsoft 365 gelöscht.
2. Ausbildung: Mitarbeiter werden vor der Einführung von Microsoft 365 umfassend geschult, um eine sichere Anwendung zu gewährleisten, den Nutzen der neuen Technologien voll auszuschöpfen und die digitalen Kompetenzen in der Verwaltung zu stärken. Zusätzlich erhalten ausgewählte Superuser eine vertiefte Ausbildung und übernehmen als sogenannte «Champions» eine unterstützende Rolle im Veränderungsprozess der jeweiligen Verwaltungseinheit.
3. Governance: Die internen Prozesse werden dokumentiert und Zuständigkeiten definiert. Es finden regelmässig Informationskampagnen zur Cybersicherheit statt.
4. Schweiz- und Behörden-spezifische Verträge: Der zwischen der Digitalen Verwaltung Schweiz (DVS) und Microsoft abgeschlossene Rahmenvertrag, unter welchem Microsoft 365 erworben wird, ist speziell auf die Bedürfnisse der öffentlichen Verwaltung in der Schweiz zugeschnitten. Er enthält spezifische Zusatzvereinbarungen, die u. a. explizit das Amts- und Berufsgeheimnis berücksichtigen, Microsoft verpflichten bei behördlichen Anfragen aus Drittstaaten ausserhalb der EU/EFTA das EU-/EFTA-Recht (inklusive dem Schweizer Recht) ausnahmslos zu beachten und für vertragliche Auseinandersetzungen gelten bezüglich anwendbarem Recht und Gerichtsstand mit Microsoft eigens verhandelte Regelungen, die eine angemessene rechtliche Absicherung für Kunden in der Schweiz bieten.
5. Informationsklassifizierung: Die Klassifizierung von Informationen wird entsprechend der IT-Verordnung verlangt (§ 16a ITV). Informationen, die in einer Ablage von Microsoft Teams gespeichert werden, können automatisch klassifiziert werden, sodass eine manuelle Zuordnung durch den Nutzer nicht erforderlich ist. Neue Office-Dateien werden standardmässig als «vertraulich» eingestuft, um einen angemessenen Schutz sensibler Inhalte zu gewährleisten, bis die tatsächliche Vertraulichkeit feststeht. Für Informationen der höchsten Klassifizierungsstufe «geheim», die ausschliesslich in Ausnahmefällen angewendet wird, gelten erweiterte Sicherheitsmassnahmen sowie zusätzliche Risikobewertungen. Microsoft 365 stellt zudem sicher, dass als «geheim» eingestufte Dokumente nicht in der Cloud bearbeitet und gespeichert werden.
6. Qualifiziertes IT-Personal: Eigene top-ausgebildete AFI-Mitarbeiter sind wesentlich, um die Microsoft 365-Sicherheitsmechanismen und Funktionen zu aktivieren und aktuell zu halten. Eine klare Rollendefinition hilft, Verantwortlichkeiten zu trennen, Sicherheitsrisiken zu minimieren und die Plattform effizient zu betreiben.
7. Zertifizierungen und Prüfberichte: Regelmässige Einforderung und Evaluation der externen Kontroll- und Prüfberichte zu Datenschutz und Informationssicherheit.
8. Anhang ITV: Mit dem Anhang an die ITV wird geregelt, welche Applikationen zum Basisdienst des Kantons gehören und für welche Aufgaben welche Applikationen zu verwenden sind. Dazu ist eine separate Teilrevision der ITV notwendig.

Nachfolgende schematische Darstellung stellt die Risiken den zugehörigen technischen und organisatorischen Massnahmen gegenüber:

	Risiken				
Massnahmen	Datenverlust	Serviceausfall	Lock-In-Effekt	Kontrollverlust	Herausgabe von Daten an Behörden
Technische Massnahmen					
Nutzung neue Sicherheitsfunktionen	●				
Backup & Restore	●	●	●		
«Evergreen»-Ansatz	●	●			
Regelbasierter Zugriff	●				
Verlustverhinderung von Daten (DLP)	●			●	
Regelmässige Zertifizierung und Prüfberichte		●		●	●
Kontrollvorgang für Zugriffe von Microsoft (Customer Lockbox)				●	
Organisatorische Massnahmen					
Nutzungsrichtlinie Microsoft 365	●			●	●
Ausbildung	●				●
Governance			●		
Schweiz- und Behörden-spezifische Verträge				●	●
Datenklassifizierung	●			●	●
Qualifiziertes IT-Personal		●		●	

Gewisse Restrisiken bleiben bei jedem Betrieb einer IT-Infrastruktur. Aus rechtlicher Sicht erfüllt die geplante Einführung von Microsoft 365 die einschlägigen Anforderungen des ÖDSG und der strafrechtlichen Geheimnisschutzvorschriften. Aus technischer Sicht stärkt sie die Widerstands- und Zukunftsfähigkeit der kantonalen IT-Landschaft in einer Bedrohungslage, die sich dynamisch und global entwickelt. Vor diesem Hintergrund sollte der Blick auf den strategischen Gesamtmehrwert des Vorhabens gerichtet werden: Microsoft 365 als Hebel für eine moderne, sichere und leistungsfähige Verwaltung, die den Herausforderungen der Digitalisierung langfristig gewachsen ist, anstatt Einzelrisiken isoliert überzubewerten.

7. Umsetzung

Der Entwurf der Umsetzungsplanung geht von einer Einführungsdauer von rund zwei Jahren aus. Die Umsetzung wird durch das AFI in Zusammenarbeit mit der Firma UPGREAT sichergestellt und sieht folgenden, groben Vorgehensplan vor.

Phase 0 – Entscheid Regierungsrat	Q1 2026
Phase 1 – Vorbereitung / Konzepte	Q2 2026
Phase 2 – Umsetzung «Basis Use Cases» «E-Mail»: Nutzung einer Modern Hybrid-Lösung mit maximalem Funktionsumfang und hoher Sicherheit. «Archivierung CMI Axioma»: Microsoft 365 und CMI Axioma archivieren Projektdaten automatisiert nach Status und Amtsvorgaben. «Backup & Restore»: Implementation einer ISDS-konformen Backup- und Restorelösung mit Speicherziel im Rechenzentrum des	Q3 2026

AFI.
Ausbildung Benutzer, Service Desk

Phase 3 – Umsetzung Use Case «Teamwork und Projektmanagement» Microsoft 365 stärkt die Teamarbeit und steigert die Effizienz durch moderne, vernetzte Arbeitsweisen (siehe Kapitel 3)	Q4 2026
Phase 4 – Umsetzung Use Case «Kommunikation (exklusive E-Mail)» Die Verwaltung modernisiert ihre Telefonie, indem sie grossteils auf Microsoft Teams als Kommunikations- und Telefonielösung setzt (siehe Kapitel 4).	Q1 2027
Projektabschluss	Q4 2027

Um einen reibungslosen Rollout der Use Cases sicherzustellen und den Zeitplan einzuhalten, werden die betroffenen Ämter frühzeitig durch die Projektleitung informiert. Die notwendigen Vorbereitungen werden gemeinsam koordiniert. Dabei ist die aktive Mitwirkung aller Mitarbeiter entscheidend für den Erfolg.

8. Mitberichtsverfahren

Das Finanzdepartement hat zum vorliegenden Regierungsratsbeschluss ein Mitberichtsverfahren durchgeführt. [redacted]

[redacted]

[redacted]

[redacted]

9. Mitteleinsatz für die Umsetzung und den Betrieb von Microsoft 365

Mit der Einführung von Microsoft 365 wird die bestehende Systemlandschaft grundlegend erweitert und für die einzelnen Verwaltungseinheiten ein grosser Mehrwert erzielt. Das neue Betriebsmodell der Servicebewirtschaftung, zahlreiche Vorgaben sowie der parallele Betrieb mit der lokalen IT-Infrastruktur stellen hohe Anforderungen an die Umsetzung von Microsoft 365. Eine Realisierung mit den bestehenden Ressourcen ist nicht möglich. Zur fundierten Einschätzung der notwendigen Aufwände und Kosten für die Projektumsetzung sowie den späteren Betrieb wurden in Zusammenarbeit mit externen Microsoft-365-Experten die relevanten Arbeitsgebiete evaluiert.

Der erhöhte Betriebsaufwand entsteht in den folgenden thematischen Schwerpunkten:

1. Kontinuierliche Systemänderungen (Evergreen-Modell): Im Rahmen des Evergreen-Modells veröffentlicht Microsoft monatlich rund 300–400 Funktions- und Sicherheitsupdates. Die Bewertung, Priorisierung und koordinierte Einführung dieser Updates und neuen Funktionen in den laufenden Betrieb erfordern zusätzliche personelle Ressourcen mit entsprechendem Fachwissen und Expertise.
2. Technische Implementierung: Die technische Implementierung, einschliesslich der Migration von Daten, der Einrichtung der hybriden Systemlandschaft und der Konfiguration der Microsoft 365 Dienste, erhöht den Betriebsaufwand, da zusätzliche Systeme überwacht und Schnittstellen gepflegt werden müssen.
3. Anwenderunterstützung und Schulung: Die Einführung neuer Werkzeuge wie Microsoft Teams, SharePoint und OneDrive führt zu einem erhöhten Bedarf an Supportleistungen. Neben dem laufenden First- und Second-Level-Support sind auch die Erstellung, Pflege und Aktualisierung von Hilfsmitteln, Schulungsunterlagen und Nutzungsempfehlungen erforderlich. Neue Mitarbeiter müssen systematisch in die Nutzung der KVS-Umgebung eingeführt werden. Zusätzlich müssen bedarfsspezifisch Teamräume in Teams für Ämter und Departemente erstellt, verwaltet und bei Bedarf wieder entfernt werden. Dabei ist eine enge Abstimmung mit den jeweiligen Organisationseinheiten notwendig. Ebenso wird Unterstützung bei der Archivierung nach CMI Axioma benötigt, um die gesetzeskonforme Ablage und Nachvollziehbarkeit sicherzustellen.
4. Governance und Betriebsprozesse: Ein geordneter Betrieb setzt die Entwicklung, Durchsetzung und kontinuierliche Anpassung von Governance-Vorgaben voraus. Ohne diese Steuerungsmechanismen drohen eine ineffiziente Nutzung, Schatten-IT und erhöhte Sicherheitsrisiken.

5. Sicherheits- und Compliance-Anforderungen: Die Plattform unterliegt fortlaufenden Änderungen durch den Hersteller, die hinsichtlich Datenschutz, Informationssicherheit und gesetzlicher Vorgaben geprüft, umgesetzt und überwacht werden müssen.

9.1 Zusätzlicher Stellenbedarf

Für zahlreiche Projektarbeiten kann externe Unterstützung hinzugezogen werden, die über ausgewiesene Microsoft 365-Kompetenzen und umfassende Projekterfahrung verfügt. Die Integration in das bestehende kantonale IT-Ökosystem – einschliesslich der Systemlandschaft mit CMI Axioma und weiteren Fachanwendungen – erfordert jedoch eine enge Zusammenarbeit mit den internen Spezialisten. Obwohl der zukünftige Betrieb der Microsoft 365-Services in Schweizer Rechenzentren von Microsoft erfolgt, verbleiben Verantwortung und Bewirtschaftung der verwendeten Services beim AFI. Die Betreuung und Überwachung der sich stetig ändernden Gegebenheiten und Funktionalitäten von Cloud-Systemen ist zentral. Wie bei Cloud-Applikationen üblich, hat auch Microsoft die Lieferfrequenz neuer Funktionalitäten deutlich erhöht. Zusätzlich entstehen durch den Parallelbetrieb von lokalen und Cloud-basierten Microsoft-Services substanzielle Mehraufwände. Um diesen Anforderungen gerecht zu werden, müssen entsprechende personelle Kapazitäten intern geschaffen werden. Dies soll dazu beitragen, internes Fachwissen aufzubauen und gleichzeitig die Kosten für externe Dienstleistungen zu reduzieren. Die gesamte Prozesskette – von Eingang einer Störungsmeldung bis zur Behebung eines komplexen Problems – erfordert spezifisches Fachwissen, das innerhalb des AFI vorhanden und abrufbar sein muss.

Die Verwaltungseinheiten befürworten im Mitberichtsverfahren eine breite Einführung der verfügbaren Funktionalitäten und sehen darin einen substanziellen Mehrwert für ihre tägliche Arbeit. Gewünscht wird ein vollumfänglicher interner Betrieb und Support sowie eine kontinuierliche Aus- und Weiterbildung durch dedizierte, interne Fachpersonen. Ergänzend sollen Automatisierungslösungen eingesetzt werden, um Prozesse über Anwendungsgrenzen hinweg zu automatisieren und optimieren. Auf die Einführung von KI-Funktionalitäten und Data-Analytics wird hingegen im Sinne einer schlankeren Umsetzung verzichtet. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

9.1.4 Vergleich zu anderen kantonalen Verwaltungen

[redacted]

[redacted]

[redacted]

[redacted]

9.2 Finanzbedarf

Mit RRB Nr. 148/2025 wurde die Beschaffung von Dienstleistungen zur Einführung von Microsoft 365 von der Firma UPGREAT AG in der kantonalen Verwaltung im Umfang von Fr. 1 417 235.-- bewilligt.

Mit RRB Nr. 799/2025 wurde das Enterprise Agreement mit Microsoft für die Jahre 2026-2028 auf Basis des Digitale Verwaltung Schweiz (DVS)-Rahmenvertrages verlängert. Die Kosten betragen pro Jahr EUR 1 198 965.96. Damit erhält der Kanton Mietlizenzen, die viele Microsoft Produkte beinhalten wie Windows-Betriebssystem (Windows 11); Office-Produktepalette (Word, Excel, PowerPoint, Outlook, Teams); E-Mailsystem (Exchange on Prem und Online); Endpunktschutz (Defender), um Notebooks und Mobiltelefone zu schützen und Log-Daten an das ausgelagerte Security Operation Center (SOC) zu übermitteln; Gerätemanagement und Softwareverwaltung (Intune); Datenanalyse (Power BI); Prozessautomatisierung (Power Automate). Mit einem Verzicht auf die Einführung von Microsoft Teams, Exchange Modern Hybrid und Power Automate können somit keine Lizenzkosten gespart werden, weil für die anderen benötigten Produkte weiterhin diese Stufe von Mietlizenzen benötigt wird.

Die drei angeführten Stellen verursachen jeweils Vollkosten (Lohn, Sozialleistungen, Ausrüstung etc.) von rund Fr. 160 000.-- pro Stelle und somit jährlich insgesamt Fr. 480 000.--. Es wird davon ausgegangen, dass die Erleichterungen oder Effizienzsteigerungen in den Departementen und Ämtern durchaus relevant sein werden. Dieser Nutzen kann indes nicht verlässlich quantifiziert oder gegenübergestellt werden.

Mit der Einführung von Microsoft 365 können auf der virtualisierten Umgebung des AFI bis zu [redacted] Server zurückgebaut werden. Die Lizenzen für Exchange werden wie oben ausgeführt weiterhin benötigt. Es können jedoch die Kosten im Umfang von Fr. 250 000.-- jährlich für [redacted]-Lizenzen reduziert werden. [redacted] Aufgrund der vielen Fachanwendungen werden für die kantonale Verwaltung weiterhin diverse physikalische Server benötigt.

9.3 Ausbildung der Mitarbeiter KVS während der Einführung

Die Superuser werden frühzeitig und vertieft in die praxisnahe Erstellung von Schulungsunterlagen, Nutzungsempfehlungen und weiteren Instrumenten einbezogen. In den Fachanwendungen ist lediglich ein punktueller Anpassungsbedarf durch die neuen Microsoft Office-Versionen zu erwarten. Ausnahmen bilden die erweiterten Integrationsmöglichkeiten mit Microsoft Teams und weiteren Microsoft 365-Apps, auf welche viele Systeme bereits technisch vorbereitet sind. Während der Umstellung und der Integration von Fachsystemen ist mit einem durchschnittlichen Aufwand von rund einem halben Arbeitstag pro Mitarbeiter der Kantonsverwaltung zu rechnen, an dem die Mitarbeiter ausgebildet werden und Telefonie- und Mailsysteme nur eingeschränkt oder gar nicht verfügbar sind. Zur Gewährleistung eines reibungslosen Rollouts werden die betroffenen Verwaltungseinheiten und Mitarbeiter frühzeitig informiert und sind zur aktiven Mitwirkung verpflichtet.

10. Fazit

Der Regierungsrat ist der Ansicht, dass die vielen Vorteile der cloudbasierten Lösung von Microsoft 365 die Nachteile sowie die Restrisiken deutlich überwiegen. Es sind wirksame technische und organisatorische Massnahmen vorgesehen, um die identifizierten Risiken auf ein Mindestmass zu reduzieren. Die verbleibenden Restrisiken können im Sinne einer effizienten Ausrüstung

und damit Leistungserbringung der kantonalen Verwaltung akzeptiert werden. Die damit verbundene Auslagerung bis zur Stufe der vertraulichen Informationen wird entsprechend genehmigt. In der Umsetzung sowie im weiteren Verlauf ist die Risikosituation im Bereich Informationssicherheit und -schutz insbesondere durch das AFI laufend und eng zu verfolgen. Zudem sind Optionen und Handlungsmöglichkeiten zur bestmöglichen Wahrung der digitalen Souveränität weiterhin regelmässig zu prüfen und der Regierungsrat über massgebende Entwicklungen zu orientieren. Zum aktuellen Zeitpunkt kommt der Regierungsrat indes zum Schluss, dass die Effizienzeinbussen, der Umstellungsaufwand und die Herausforderungen in der Interoperabilität deutlich zu gross sind, als dass andere Optionen wie Open-Source-Lösungen ein gleichwertiges Kosten-Nutzen-Verhältnis erreichen könnten.

Beschluss des Regierungsrates

1. Das Amt für Informatik wird beauftragt, Microsoft 365 im Sinne der Erwägungen einzuführen. Der Umsetzungsablauf gemäss Ziffer 7 wird bewilligt.

2. Die damit verbundene Auslagerung von Daten, welche aktiv und in Bearbeitung sind, bis und mit Klassifizierungsstufe «vertraulich» und besonders schützenswerten Personendaten, nach Microsoft 365 wird gemäss § 31 Abs. 1 ITV unter Akzeptanz der Restrisiken bewilligt. Geschäftsrelevante Informationen müssen weiterhin in Fachanwendungen oder CMI Axioma abgelegt werden, um eine korrekte Aktenführung und Archivierung sicherzustellen. Die Mitarbeiter werden im Rahmen des Projektes umfassend geschult.

3. Der Stellenplan des Amts für Informatik wird ab dem Jahr 2026 unterjährig um 3 FTE erhöht.

4. Zustellung: Gerichte.

5. Zustellung elektronisch: Mitglieder des Regierungsrates; Staatskanzlei; Departemente; Ämter.

Im Namen des Regierungsrates:

Regierungsrat Kanton Schwyz

Dr. Mathias E. Brun
Staatsschreiber