DigiFit Olten

Konzept

Version 1.4

Sicherheitskonzept für die Einführung von Microsoft 365

Datum	22.05.2025
Autoren	Teilprojekt Organisation, DigiFit Olten
Programmtitel	DigiFit Olten
Herausgeber	IT-Strategie Board

Inhaltsverzeichnis

Versionskontrolle

1.0	Grundlage Zirkulationsbeschluss IT-Strategie Board	Neaf Weber Jost	18.07.2024
1.1	Änderungen aufgrund Retourmeldungen IT-Strategie Board - Kapitel 1.1, Präzisierung - Kapitel 2.1, Präzisierung - Kapitel 2.2, Präzisierungen Mit Änderungen durch IT-Strategie Board genehmigt.	Jost	09.08.2024
1.2	Korrektur Kapitel 3.1 Datenklassen Besonders schützenswerte Personaldaten durch korrekten Begriff "Besonders schützenswerte Personendaten" ersetzt	Jost	21.10.2024
1.3	Verabschiedung durch IT-Strategie-Board		22.05.2025
1.4	- Textliche Anpassung Kapitel "Definition der zu sichernden Daten" nach Realisierung Backup-Lösung - Textliche Anpassung Hybrides Setup	Jost	02.04.2026

1 Einleitung

1.1 Ziel und Zweck des Datenschutzkonzepts

Das vorliegende Datenschutzkonzept verfolgt das primäre Ziel, einen klaren und umfassenden Rahmen für die Einführung und Nutzung von Microsoft 365 in unserer Organisation zu schaffen. Dabei liegt der Schwerpunkt auf der Implementierung und Aufrechterhaltung von effektiven organisatorischen und technischen Massnahmen, um den Schutz und die Sicherheit personenbezogener und sensibler Daten bei der Nutzung von M365 zu gewährleisten.

1.2 Ausgangslage und Anforderungen an Microsoft 365

Die aktuelle IT-Struktur der Stadt Olten ist charakterisiert durch die vorwiegende Speicherung und Bearbeitung der Daten im lokalen Rechenzentrum der Stadt Olten. Der Grossteil der Daten wird in Fachapplikationen oder in Dateiablagen (Netzlaufwerke) verwaltet. Die E-Mail-Kommunikation wird über Exchange On-Premise abgewickelt. Es fehlt jedoch eine integrierte Lösung für Kollaboration und Kommunikation, was die Möglichkeiten der vernetzten Zusammenarbeit und des Informationsaustausches einschränkt.

Um diesen Anforderungen gerecht zu werden, hat sich die Stadt Olten entschieden, Microsoft 365 als cloudbasierte Plattform für Kollaboration und Kommunikation einzuführen. Microsoft 365 bietet Dienste und Anwendungen wie Microsoft Teams, Exchange, SharePoint Online und OneDrive, die das Arbeiten im Team, die Verwaltung von Dokumenten, die Terminplanung, Videokonferenzen und Chat-Kommunikation erleichtern. Die Einführung von Microsoft 365 soll die digitale Transformation unterstützen sowie die Effizienz und Flexibilität fördern.

Die Nutzung von Microsoft 365 bringt jedoch auch datenschutzrechtliche Herausforderungen mit sich, da personenbezogene und sensible Daten in einer Cloud-Umgebung verarbeitet werden könnten, die sich ausserhalb der direkten Kontrolle der Stadt Olten befindet. Um die Einhaltung der geltenden Datenschutzgesetze und -richtlinien zu gewährleisten, muss daher sorgfältig geprüft werden, welche Daten in Microsoft 365 bearbeitet werden dürfen und wie diese geschützt werden sollen.

2 Rahmenbedingungen und Verantwortlichkeiten

2.1 Geltende Datenschutzgesetze und -richtlinien

Die folgenden wesentlichen Datenschutzgesetze und -richtlinien sind für die Implementierung und den Betrieb von Microsoft 365 bei der Stadt Olten relevant. Sie stellen sicher, dass der Umgang mit personenbezogenen und sensiblen Daten den aktuellen rechtlichen Anforderungen entspricht.

- Datenschutzgesetz des Kanton Solothurn InfoDG; BGS 114.1[1]
- Informations- und Datenschutzverordnung des Kanton Solothurns InfoDV; BGS 114.2[2]
- Weisungen und Empfehlungen des Datenschutzverantwortlichen der Stadt Olten

2.2 Verantwortlichkeiten

Die kontinuierliche Sicherstellung der Datensicherheit und des Datenschutzes bei der Nutzung von Microsoft 365 erfordert definierte Verantwortlichkeiten. Dies gewährleistet, dass alle relevanten Aspekte der Datensicherheit und des Datenschutzes laufend wahrgenommen werden.

Rolle	Aufgaben
IT-Strategie Board	– Kontrolle und Freigabe von Vorschriften für Business-Anwendungen – Definition und Kommunikation von Sicherheitsvorschriften – Vermitteln und überprüfen der Einhaltungen von Weisungen und Bearbeitungsvorschriften – Sensibilisierung von Führungskräften bezüglich Sicherheitsvorschriften – Den Risikobericht auf dem Laufenden halten – Erstellung einer Exit-Strategie im Bedarfsfall – Anpassungen / Erweiterungen am Datenklassifizierungs-Konzept – Steuerung von externen Partnern
Sourcing-Board	– Spezifische Vorschriften für Business-Anwendungen zuhanden des IT-Strategie Board vorschlagen (z.B. Einführung Intranet oder Telefonie) – Datenschutzrechtliche Beurteilung von Cloud-Lösungen und Empfehlungen zuhanden des IT-Strategie Board
Externe Partner	– Beobachten und Beurteilung von Weiterentwicklung / Veränderungen von M365 – Überprüfen der Subunternehmenliste – Überprüfung, ob Microsoft ihren vertraglichen Pflichten nachkommt – Regelmässige Überprüfung der definierten Risiken

[1] Informations- und Datenschutzgesetz (InfoDG) des Kanton Solothurns
[2] Informations- und Datenschutzverordnung (InfoDV) des Kanton Solothurns

3 Datenklassifizierung und -schutz

3.1 Datenklassen

3.1.1 Arten von Daten

Die Stadt Olten verwaltet verschiedene Arten von Daten, die durch die Nutzung von Microsoft 365 betroffen sein können und daher einer entsprechenden Klassifizierung bedürfen. Diese Datenarten umfassen:

Arten von Daten	Beschreibung
Sachdaten	Informationen, die sich nicht auf bestimmte oder bestimmbare Personen beziehen
Personendaten (InfoDG § 6)	Personendaten (Daten) sind Angaben, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person (betroffene Person) beziehen Beispiele: Name, Vorname, Adresse
Besonders schützenswerte Personendaten	Informationen, die gemäss Datenschutzgesetzt (DSG), Kapitel 2, Abschnitt 1, § 5c[3] als besonders schützenswert deklariert sind. Es wurde die Formulierung aus dem DSG übernommen, da davon auszugehen ist, dass diese im InfoDG entsprechend angepasst wird. Beispiel: – Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten – Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie – genetische Daten – biometrische Daten – Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen – Daten über Massnahmen der sozialen Hilfe
Besondere Amtsgeheimnisse	Informationen, die einem besonderen Amtsgeheimnis unterstehen Beispiele: Steuerdaten, Sozialhilfedaten, Opferhilfedaten
Berufsgeheimnis	Informationen, die einem Berufsgeheimnis unterstehen Beispiele: Gesundheitsdaten bei einer Ärztin oder einem Arzt

3.1.2 Definition Datenklassen

Daten und Informationen werden zwei Datenklassen zugeordnet. Diese Klassifizierung ermöglicht eine gezielte und effektive Handhabung der unterschiedlichen Datentypen, um den Datenschutz und die Datensicherheit gemäss den gesetzlichen Vorgaben zu gewährleisten.

[3] Quelle: Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) (admin.ch)

Datenklasse	Arten von Daten
Besonders schützenswerte Daten	– Besonders schützenswerte Personendaten – Besondere Amtsgeheimnisse – Berufsgeheimnisse
Sach- und Personendaten	– Sachdaten – Personendaten

3.1.3 Anwendung der Datenklassen

Die folgende Tabelle zeigt welche Arten von Daten mit welchen Microsoft-Applikationen bearbeitet werden dürfen.

	Microsoft Applikationen							
	Office 365 Apps	Office 365 Online	Exchange Mailserver		MS Teams		Share Point	One Drive
Datenklassen	Word, Excel, Power-Point etc. lokal*	Word, Excel, PowerPoint in der Cloud*	Lokal, on prem	Online	Audio- oder Videobe-sprechungen ohne Aufzeichnung	Übrige Funktionen		
Besonders schützenswerte Daten	✓	✗	✓	✗	✓	✗	✗	✗
Sach- und Personendaten	✓	✓	✓	✓	✓	✓	✓	✓

✓ Nutzung möglich

✗ Keine Nutzung

- Aufzählung nicht abschliessend

Zusammengefasst dürfen besonders schützenswerte Daten nicht in der M365 Cloud bearbeitet werden, um den Datenschutzanforderungen gerecht zu werden. Die Bearbeitung von Personen- und Sachdaten ist in der M365 Cloud jedoch zulässig. Personen- und Sachdaten müssen nicht verschlüsselt werden. Der Datenzugriff wird mittels Berechtigungen geregelt.

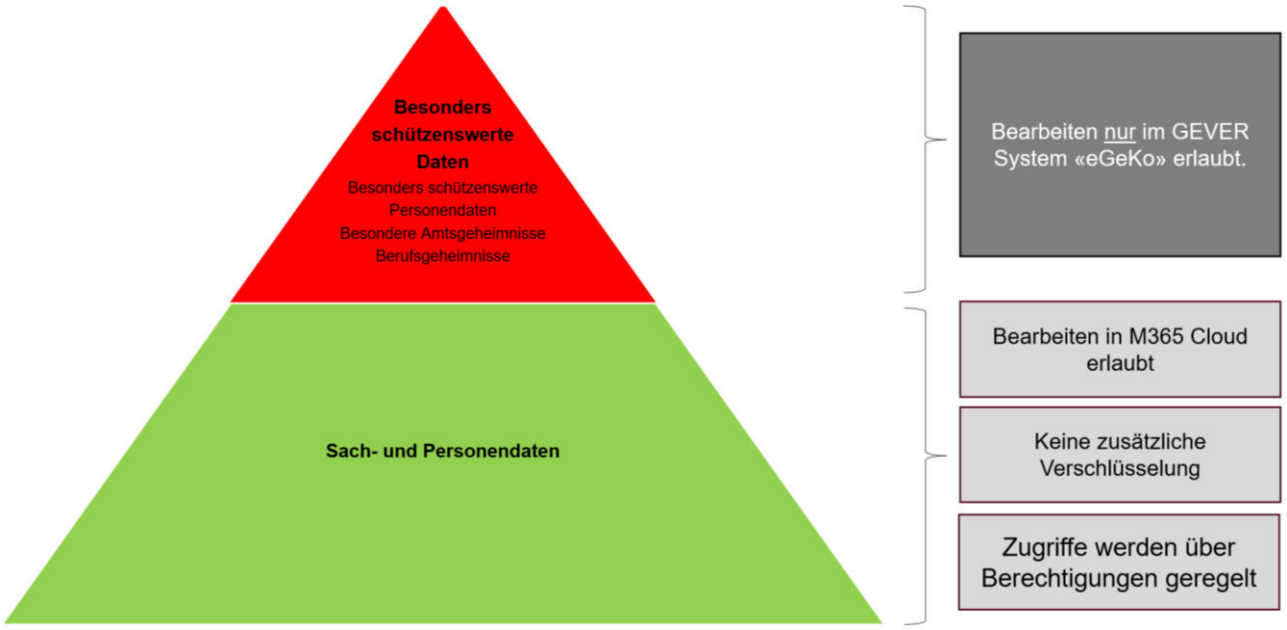

Abbildung 1: Darstellung Datenklasse der Stadt Olten

3.1.4 Implementierung der Datenklassen

Technische Massnahmen:
- Es wird keine technische Implementierung der Datenklassen (z.B. mittel Azure Information Protection) zur Verfügung gestellt
- Exchange-Postfächer, welche besonders schützenswerte Daten enthalten oder über die entsprechende Daten versendet oder empfangen werden, werden weiterhin On-Premise betrieben.

Organisatorische Massnahmen:
Für die korrekte Handhabung der Datenklassen sollen organisatorische Massnahmen aufgesetzt werden, welche die Mitarbeitenden zum Thema Datenschutz laufend sensibilisiert. Mögliche organisatorische Massnahmen sind:
- Klare Anweisungen über korrekte Ablage von Daten
- Erstellung und Durchführung von Schulungs- und Informationsmaterialien für die Mitarbeitenden
- Erstellung und Durchführung von Tests und Übungen zur Überprüfung des Sicherheitsbewusstseins
- Erstellung und Durchführung von Feedback- und Verbesserungsmassnahmen

3.2 Datensicherung und -wiederherstellung

3.2.1 Definition der zu sichernden Daten

Die Dateien in der Microsoft-365-Umgebung werden täglich bei einem Drittanbieter gesichert. Die Datensicherungen sind verschlüsselt gespeichert. Auf die Daten kann ausschliesslich die Informatikabteilung zugreifen, und nur sie ist berechtigt, eine Wiederherstellung durchzuführen. Zudem ist sichergestellt, dass eine Wiederherstellung auch auf einer Umgebung ausserhalb von Microsoft 365 möglich ist. Es werden folgende Anwendungsdaten gesichert:

- **Exchange:**
  - Postfächer
  - Öffentliche Ordner
  - Kalenderelemente

  - Kontakte
  - Aufgaben
  - Journal-Einträge

- **SharePoint Online:**
  - Websitesammlungen
  - Listen
  - Bibliotheken
  - Notizen

- **Microsoft Teams:**
  - Team-Kanäle
  - Private Chats
  - Dateien
  - Besprechungsaufzeichnungen

Folgende Anwendungen werden nicht gesichert:
- **OneDrive for Business (persönliche Ablage)**

3.2.2 Wiederherstellungsoptionen

Weitere Informationen folgen nach Wahl eines geeigneten Backup Tools.

3.3 Datenlöschung und -archivierung

In diesem Kapitel werden die Verfahren und Prozesse beschrieben, die für die sichere Löschung und Archivierung von Daten in Microsoft-Systemen verwendet werden.

3.3.1 Datenlöschung

Die Verantwortung für die Löschung von Daten liegt bei den Benutzern. Dieser Ansatz stellt sicher, dass jeder Einzelne eine aktive Rolle im Datenmanagement spielt und fördert ein umfassendes Bewusstsein für den Wert und die Sensibilität der Informationen, mit denen gearbeitet wird.

- **Benutzerverantwortung:**
  Es ist die Aufgabe jedes Benutzers, seine eigenen Daten regelmässig auf ihre Notwendigkeit und Aktualität hin zu überprüfen. Nicht mehr benötigte oder veraltete Informationen sollten von den Benutzern selbst identifiziert und entsprechend gelöscht werden. Dies betrifft alle Arten von Daten, darunter Dokumente, E-Mails und andere digitale Inhalte.

- **Verzicht auf technische Automatisierung:**
  In Microsoft 365 ist es möglich, automatische Aufbewahrungsrichtlinien für Dokumente festzulegen. [redacted] Ein generelles Löschen nach einer bestimmten Dauer ist oft nicht ratsam, da gewisse Daten eine längere Gültigkeit haben. Daher sind Aufbewahrungsrichtlinien auf bestimmte Anwendungsfälle auszurichten. Daher werden keine technischen, automatisierten Löschverfahren implementiert.

- **Organisatorische Massnahmen durch Benutzer:**
  Benutzer müssen eigenständig organisatorische Massnahmen ergreifen, um die Löschung von Daten, die nicht mehr benötigt werden, sicherzustellen. Dies beinhaltet das Befolgen interner

Richtlinien und bewährter Verfahren für ein effektives Datenmanagement.

- **Regelmässige Überprüfung**:
  Eine regelmässige Selbstüberprüfung der eigenen Daten auf Aktualität und Relevanz wird von allen Benutzern erwartet. Veraltete oder unnötige Daten sind zu löschen.

3.3.2 Datenarchivierung

Obwohl Microsoft 365 zahlreiche Funktionen für das Datenmanagement bietet, ist zu beachten, dass keine spezifischen Funktionen für die langfristige Datenarchivierung direkt zur Verfügung gestellt werden.

- **Backup-Verfahren:**
  Zur Sicherung der Datenintegrität und -verfügbarkeit werden regelmässig Backups durchgeführt. Diese Sicherungen dienen als kurz- bis mittelfristige Lösung zur Datenwiederherstellung im Falle eines Datenverlustes oder einer Beschädigung. Die Aufbewahrungsfristen dieser Backups sind detailliert im aktuellen Backup-Konzept der Stadt Olten festgelegt und orientieren sich an den organisatorischen Anforderungen sowie an den gesetzlichen Vorgaben.

- **Geschäftsrelevante und archivierungspflichtige Daten:**
  Für Daten, die einer Archivierungspflicht unterliegen, setzt die Stadt Olten weiterhin auf die bestehenden Verfahren. Diese Daten werden, abhängig von ihrer Beschaffenheit und den Anforderungen der Fachabteilungen, entweder elektronisch in den Fachapplikationen, in der Gever-Lösung oder in Papierform archiviert.

- **Archivierung von Microsoft Teams Arbeitsräumen:**
  Microsoft Teams bietet eine spezifische Funktion zum Archivieren von Arbeitsräumen (Teams), die es ermöglicht, Teams-Räume als archiviert zu kennzeichnen. Es ist jedoch wichtig zu verstehen, dass diese Archivierungsfunktion nicht der Langzeitarchivierung dient, die eine dauerhafte Aufbewahrung und den Schutz der Daten gemäss gesetzlichen oder unternehmensspezifischen Vorgaben garantiert. Daten in Microsoft Teams, die einer Archivierungspflicht unterliegen, müssen gemäss den vorgängig beschriebenen Verfahren archiviert werden.

- **Weitere Massnahmen:**
  Neben den traditionellen Archivierungsmethoden prüft die Stadt Olten kontinuierlich die Einführung zusätzlicher Massnahmen und Technologien, um die Langzeitarchivierung und den Schutz archivierungspflichtiger Daten zu optimieren. Dies beinhaltet die Evaluierung von spezialisierten Archivierungslösungen, die eine effizientere, sicherere und gesetzeskonforme Archivierung ermöglichen.

3.4 Lockbox für den eingeschränkten Zugriff durch Microsoft-Mitarbeitende

Damit ein Zugriff durch Microsoft (z.B. zur Behebung von technischen Problemen) nicht unkontrolliert stattfindet, besteht die Möglichkeit die «Customer Lockbox[4]» einzurichten. Diese stellt einen Genehmigungsprozess sicher, welcher durchlaufen werden muss, bevor ein Zugriff durch Microsoft erfolgt. Erst mit der kundenseitigen Genehmigung wird der Zugriff zeitlich begrenzt und geloggt gewährt. Ohne “Customer Lockbox” kommt bei einem Zugriff auf Kundendaten durch

[4] Weiterführende Informationen zu Lookbox

Microsoft in jedem Fall der Microsoft “Lockbox” Prozess zum Tragen, d.h. die vorgesetzte Stelle eines Microsoft-Mitarbeitenden muss den Zugriff freigeben, der wiederum zeitlich begrenzt (just-in-time) und protokolliert stattfindet. Solche Zugriffsprotokolle sind durch den Kunden jederzeit einsehbar.
[redacted]

Technische Massnahmen:
[redacted]

4 Kommunikationssicherheit

4.1 Verwendung von Exchange

4.1.1 Hybrides Setup

Die Stadt Olten betreibt ein hybrides Setup von Exchange, um die Vorteile sowohl der lokalen als auch der cloudbasierten Exchange-Umgebung zu nutzen. Ein hybrides Exchange-Setup bedeutet, dass ein Teil der Exchange-Postfächer und -Dienste weiterhin On-Premises (lokal) betrieben wird, während ein anderer Teil in der Microsoft 365 Cloud gehostet wird. Diese Konfiguration ermöglicht eine nahtlose Integration und Zusammenarbeit zwischen den beiden Umgebungen, wodurch eine flexible und skalierbare Lösung geschaffen wird.

4.1.2 Verwaltung von Postfächern

Allen Mitarbeitenden der Stadt Olten wird ein Exchange-Postfach mit 2GB Speicherplatz zur Verfügung gestellt. Die Exchange Postfächer werden wie folgt angelegt:

Exchange online:
Persönliche Postfächer werden in der Exchange online Umgebung angelegt. Ausnahmen sind unter Exchange On-Premise aufgeführt.
Über diese Postfächer dürfen **keine** besonders schützenswerten Daten versendet werden. Diese Einschränkung gilt explizit auch für E-Mail-Empfänger mit einer @olten.ch-Adresse.

Exchange On-Premise:
Exchange Postfächer, welche besonders schützenswerte Daten enthalten oder über die besonders schützenswerte Daten versendet oder empfangen werden, müssen weiterhin On-Premise geführt werden. Dies bis angemessene technische und organisatorische Richtlinien etabliert sind, um den Schutz der besonders schützenswerten Daten sicherzustellen.
Betroffen sind die Postfächer:
- der Direktion Soziales
- der Sozialregion
- der Direktion Finanzen und Dienste

4.2 Verschlüsselung von E-Mails und Anhängen

Es gilt der Grundsatz, dass besonders schützenswerte Daten nicht per E-Mail versendet werden dürfen. Dies ist insbesondere für persönliche Postfächer relevant, da diese in Exchange Online gehostet werden und somit in der M365 Cloud gespeichert sind.

Postfächer mit besonders schützenswerten Daten hingegen bleiben weiterhin On-Premises verfügbar, sodass besonders schützenswerte Daten aus diesen Postfächern versendet werden können. Für eine sichere Übertragung solcher Daten wird weiterhin die bestehende Lösung IncaMail verwendet.

4.3 Schutz vor Phishing und Spam

Microsoft bietet mit Advanced Threat Protection (ATP) eine umfassende Lösung zum Schutz vor Phishing und Spam. Diese Lösung nutzt fortschrittliche Technologien wie maschinelles Lernen und Verhaltensanalysen, um verdächtige E-Mails zu erkennen und zu blockieren, bevor sie die Posteingänge der Benutzer erreichen. [redacted]

5 Identitäts- und Zugriffsmanagement

5.1 Entra ID für die Benutzerverwaltung und -authentifizierung

Entra ID, ehemals Azure Active Directory, ist ein cloudbasierter Identitäts- und Zugriffsverwaltungsdienst von Microsoft, der die Benutzerverwaltung und -authentifizierung in der Microsoft 365 Umgebung unterstützt. Durch die Verwendung von Entra ID können Benutzer nahtlos und sicher auf verschiedene Microsoft 365-Dienste zugreifen. Ein entscheidender Bestandteil für den Betrieb von Microsoft 365 ist die Synchronisierung zwischen dem lokalen Active Directory und Entra ID. Diese Synchronisation stellt sicher, dass Benutzerdaten konsistent und aktuell sind und ermöglicht eine einheitliche Verwaltung von Benutzeridentitäten sowohl in der lokalen als auch in der Cloud-Umgebung.

5.2 Multi-Faktor-Authentifizierung für den Zugriff auf Microsoft 365

Die Multi-Faktor-Authentifizierung (MFA) bietet eine zusätzliche Sicherheitsebene für den Zugriff auf Microsoft 365, indem sie neben dem Passwort einen zweiten Identitätsnachweis erfordert. Dies verringert das Risiko von unbefugtem Zugriff erheblich, selbst wenn Passwörter kompromittiert werden.

Der Zugriff auf Microsoft 365 wird mit folgendem Identitätsnachweis gewährt:

Standort	Gerät	Identitätsnachweis
Netzwerk der Stadt Olten	Verwaltetes Gerät	Benutzername und Passwort
Ausserhalb des Netzwerk Stadt Olten	Verwaltetes Gerät	Benutzername und Passwort Authenticator App
Innerhalb und ausserhalb des Netzwerk Stadt Olten	Nicht verwaltetes Gerät	Benutzername und Passwort Authenticator App

5.3 Conditional Access für die Anwendung von Sicherheitsrichtlinien

Mit dem Conditional Access, auf Deutsch „bedingter Zugriff“, können Richtlinien erstellt und definiert werden, die auf Anmeldeereignisse reagieren und andere Aktionen anfordern, bevor einem Benutzer Zugriff auf eine Anwendung oder einen Dienst gewährt wird.

Richtlinien für den bedingten Zugriff können granular und spezifisch sein und die Benutzer befähigen, überall und jederzeit produktiv zu sein, aber gleichzeitig eine Organisation schützen.

5.3.1 Zugriffe von bestimmten Standorten

Mit Conditional Access können Zugriffe basierend auf geografischen Standorten eingeschränkt werden, um damit die Sicherheit zu erhöhen. Dies schützt sensible Daten vor unbefugtem Zugriff und stellt sicher, dass nur autorisierte Nutzer aus definierten Regionen Zugang erhalten.

Basierend auf der Datenschutzverordnung, Anhang 1 (Art. 8 Abs. 1)[5] verfügen folgende Staaten, Gebiete und internationale Organe über einen angemessenen Datenschutz und werden seitens Stadt Olten als Standort zugelassen:

- Schweiz
- Deutschland
- Österreich
- Belgien
- Dänemark
- Spanien
- Estland
- Finnland
- Frankreich
- Griechenland
- Ungarn
- Island
- Italien
- Lettland
- Lichtenstein
- Litauen
- Luxemburg
- Malta
- Norwegen
- Niederlande
- Polen
- Portugal
- Tschechien
- Slowakei
- Slowenien
- Schweden

Der Zugang auf die M365 Umgebung wird von allen nicht aufgelisteten Gebieten blockiert.

5.4 Privileged Identity Management

Entra ID Privileged Identity Management (PIM) bietet eine erweiterte Verwaltung und Kontrolle über privilegierte Zugriffsrechte in Microsoft 365. Mit PIM können Administratoren den Zugriff auf wichtige Ressourcen zeitlich begrenzen, Multi-Faktor-Authentifizierung erzwingen und detaillierte Überwachungs- und Berichtsfunktionen nutzen, um sicherzustellen, dass nur autorisierte Benutzer temporär erhöhte Rechte erhalten. Diese Sicherheitsmassnahmen reduzieren das Risiko von unbefugtem Zugriff und Missbrauch von privilegierten Konten.

[5] Quelle: AS 2022 568 - Verordnung vom 31.August 2022 über... | Fedlex (admin.ch)

6 Geräte- und Anwendungssicherheit

6.1 Definition und Anwendung von Richtlinien für den Gastzugriff auf Microsoft 365

Externe Gäste können in die Microsoft 365 Umgebung der Stadt Olten eingeladen werden, um eine einfache und effiziente Zusammenarbeit mit externen Partnern zu ermöglichen.

Die Verantwortung für das On- und Offboarding externer Gäste liegt bei den Team-Besitzern. Mit einer Einladung in einen Teams-Arbeitsraum erhalten externe Gäste Zugriff auf Beiträge, Dokumente, Aufgaben und weitere Verknüpfungen zu Anwendungen innerhalb des Arbeitsraums.

Durch technische Unterstützung können Benutzerinnen und Benutzer den Überblick über externe Gäste in Microsoft Teams und Microsoft 365 Gruppen einfach verwalten. Ein digitalisierter Onboarding-Prozess ermöglicht die einfache und sichere Aufnahme externer Gäste ins System, einschliesslich der Unterzeichnung erforderlicher Dokumente. Automatisierte Lebenszyklen fordern Benutzerinnen und Benutzer regelmässig auf, die Gäste zu überprüfen. Falls diese Überprüfung nicht erfolgt, werden die Gäste sicher entfernt. Um dies zu gewährleisten, wird das Tool [redacted] eingesetzt.

Dateien können auch ohne Einladung in einen Teams-Arbeitsraum mit externen Gästen geteilt werden. Die Verwaltung dieser Zugriffe liegt in der Verantwortung der jeweiligen Benutzerinnen und Benutzer.

7 Datenschutz und Compliance

7.1 Data Loss Prevention für die Verhinderung von Datenverlusten

Data Loss Prevention (DLP) in Microsoft 365 ist eine leistungsstarke Funktion, die entwickelt wurde, um den ungewollten Verlust sensibler Daten zu verhindern. DLP ermöglicht es, Inhalte in E-Mails und Dateien automatisch zu erkennen, zu überwachen und zu schützen, indem Richtlinien angewendet werden, die den Umgang mit sensiblen Informationen regeln. Dies hilft, Verstösse gegen Datenschutzrichtlinien zu vermeiden und sicherzustellen, dass vertrauliche Daten nicht versehentlich oder absichtlich nach aussen gelangen.

[redacted]

7.2 eDiscovery für die Suche und den Export von Daten

eDiscovery (electronic Discovery) in Microsoft 365 ist eine Funktion, die es ermöglicht, Daten effizient zu durchsuchen, zu identifizieren und zu exportieren, um rechtlichen Anforderungen und Compliance-Vorschriften gerecht zu werden. Mit eDiscovery können Organisationen relevante

Daten aus E-Mails, Dokumenten und anderen Office 365-Diensten finden und bereitstellen, was besonders bei Rechtsstreitigkeiten, Untersuchungen und Audits wichtig ist.

[redacted]

7.3 Audit Log für die Überwachung von Aktivitäten

Microsoft 365 Audit Log dient zur Überwachung und Nachverfolgung von Benutzeraktivitäten innerhalb der Microsoft 365 Umgebung. Mit Audit Log können Organisationen detaillierte Protokolle über verschiedene Aktivitäten, wie Anmeldungen, Dateiänderungen und administrative Aktionen, erfassen und analysieren. Diese Funktion unterstützt die Einhaltung von Compliance-Richtlinien und hilft bei der schnellen Identifikation und Untersuchung von sicherheitsrelevanten Vorfällen.

[redacted]

Microsoft 365 bietet umfassende Überwachungsfunktionen zur Verfolgung organisatorischer Aktivitäten, wie in der folgenden Tabelle dargestellt.

Funktion	Überwachung (Standard)	Audit (Premium)
Standardmäßig aktiviert	✔	✔
Tausende von durchsuchbaren Überwachungsereignissen	✔	✔
Audit-Suchtool im Complianceportal	✔	✔
Search-UnifiedAuditLog-Cmdlet	✔	✔
Exportieren von Überwachungsdatensätzen in eine CSV-Datei	✔	✔
Zugriff auf Überwachungsprotokolle über Office 365-Verwaltungsaktivitäts-API [1]	✔	✔
Aufbewahrung von Überwachungsprotokollen für 180 Tage	✔	✔
1-jährige Aufbewahrung des Überwachungsprotokolls		✔
10-jährige Aufbewahrung des Überwachungsprotokolls [2]		✔
Aufbewahrungsrichtlinien für Überwachungsprotokolle		✔
Intelligente Erkenntnisse		✔

Quelle: https://learn.microsoft.com/de-de/purview/audit-solutions-overview

7.4 Compliance Manager für die Einhaltung von Standards und Vorschriften

Der Microsoft 365 Compliance Manager unterstützt, Standards und Vorschriften einzuhalten. Der Compliance Manager bietet Bewertungs- und Nachverfolgungsfunktionen für Compliance-Aktivitäten, indem er detaillierte Einblicke in den Compliance-Status gibt und Massnahmen zur Risikominderung vorschlägt. Dies erleichtert es Organisationen, regulatorische Anforderungen zu erfüllen und ihre Compliance-Bemühungen effizient zu verwalten.

8 Glossar

Das folgende Glossar enthält einige wichtige Begriffe, die in diesem Dokument verwendet werden und deren Bedeutung für das Verständnis des Konzepts erläutert wird.

Begriff	Definition
Datenschutzkonzept	Ein Plan, der die Massnahmen und Richtlinien beschreibt, um den Schutz personenbezogener und sensibler Daten sicherzustellen.
Microsoft 365 (M365)	Eine cloudbasierte Plattform von Microsoft, die verschiedene Dienste und Anwendungen wie Teams, Exchange, SharePoint Online und OneDrive umfasst.
Exchange On-Premise	Ein lokal betriebenes E-Mail- und Kalenderverwaltungssystem von Microsoft.
Data Loss Prevention (DLP)	Eine Funktion, die den Verlust sensibler Daten verhindert, indem sie Inhalte in E-Mails und Dateien überwacht und schützt.
eDiscovery	Eine Funktion in Microsoft 365, die das Durchsuchen, Identifizieren und Exportieren von Daten für rechtliche und Compliance-Zwecke ermöglicht.
Audit Log	Ein Überwachungswerkzeug, das Aktivitäten innerhalb der Microsoft 365 Umgebung protokolliert und analysiert.
Compliance Manager	Ein Tool in Microsoft 365, das Organisationen unterstützt, Standards und Vorschriften einzuhalten, indem es den Compliance-Status bewertet und Massnahmen zur Risikominderung vorschlägt.
Entra ID (ehemals Azure Active Directory)	Ein cloudbasierter Identitäts- und Zugriffsverwaltungsdienst von Microsoft, der die Benutzerverwaltung und -authentifizierung unterstützt.
Multi-Faktor-Authentifizierung (MFA)	Ein Sicherheitsmechanismus, der neben dem Passwort einen zweiten Identitätsnachweis erfordert.
Conditional Access	Eine Sicherheitsfunktion, die Richtlinien erstellt, um den Zugriff auf Anwendungen und Dienste basierend auf bestimmten Bedingungen zu steuern.
Privileged Identity Management (PIM)	Eine Funktion, die die Verwaltung und Kontrolle über privilegierte Zugriffsrechte bietet und den Zugriff auf wichtige Ressourcen zeitlich begrenzt und überwacht.
On-Premises	IT-Infrastruktur und -Anwendungen, die lokal in den Einrichtungen der Organisation betrieben werden, im Gegensatz zu cloudbasierten Lösungen.

Customer Lockbox	Ein Genehmigungsprozess, der sicherstellt, dass der Zugriff von Microsoft-Mitarbeitern auf Kundendaten nur nach Kundengenehmigung und für eine begrenzte Zeit erfolgt.
Microsoft Teams	Eine Kommunikations- und Kollaborationsplattform von Microsoft, die Chat, Videokonferenzen und Datei-Management integriert.
SharePoint Online	Ein cloudbasierter Dienst von Microsoft, der die Verwaltung und Speicherung von Dokumenten und die Zusammenarbeit im Team erleichtert.
OneDrive for Business	Ein cloudbasierter Dienst von Microsoft für die persönliche Dateispeicherung und -freigabe.