Richtlinie über die Nutzung von Microsoft 365 an kantonalen Berufs- und Weiterbildungszentren und Mittelschulen (Nutzungsrichtlinie M365 Sek II)

vom 12. November 2024

1 Allgemeines

1.1 Worum geht es?

Diese Richtlinie regelt die Nutzung der cloudbasierten Plattform Microsoft 365 und seiner Dienste (M365) an den kantonalen Berufs- und Weiterbildungszentren (nachstehend Berufsfachschulen) und Mittelschulen (Sek II)[1] (nachfolgend M365 Sek II).

Sie legt verbindliche Verhaltensregeln für einen sicheren und sorgfältigen Umgang bei der Bearbeitung von Daten mit M365 Sek II fest, um den Datenschutz und die Informationssicherheit zu gewährleisten.

Diese Richtlinie gilt ausschliesslich für die Nutzung von M365 Sek II. Für andere Informatiksysteme sind weiterhin die Verordnung über die Informatiksicherheit (sGS 142.21) und die Dienstanweisung über Einsatz und Verwendung von Informatikmitteln massgebend.

1.2 Für wen gilt diese Richtlinie?

Diese Richtlinie findet Anwendung für kantonale Mitarbeitende, die M365 Sek II geschäftlich nutzen. Dies umfasst Mitarbeitende:

- der kantonalen Berufsfachschulen inkl. Weiterbildungsabteilungen und Mittelschulen inkl. Interstaatliche Maturitätsschule für Erwachsene;
- des Amtes für Berufsbildung und des Amtes für Mittelschulen im Rahmen ihrer schulischen Zusammenarbeit
- der Informatik-Abteilung.

Für die übrigen geschäftlichen Tätigkeiten nutzen die Mitarbeitenden des Amtes für Berufsbildung und des Amtes für Mittelschulen den kantonalen M365-Tenant und richten sich nach der Nutzungsrichtlinie über die Nutzung von M365 vom 25. Juni 2024.

Weiter gilt die Richtlinie für externe Personen (Gäste und kantonale Angestellte), die auf Einladung oder im Auftrag der kantonalen Berufsfachschulen und Mittelschulen sowie des Amtes für Berufsbildung und des Amtes für Mittelschulen tätig werden. Mit der Einladung zu M365 Sek II müssen diese externen Personen die vorliegende Nutzungsrichtlinie zur Kenntnis nehmen, bevor sie Zugriff erhalten.

---

1 Dies umfasst die Dienste unter dem M365-Tenant «Kt. SG BLD».

1.3 Wer ist verantwortlich?

Für den Betrieb von M365 Sek II und die Gewährleistung der Sicherheitsmassnahmen für den Grundschutz des Gesamtsystems verantwortlich ist der Dienst für Finanzen und Informatik des Bildungsdepartementes (Abteilung Informatik-Cluster).

Die Verantwortung über die mit M365 Sek II bearbeiteten Daten kommt weiterhin dem inhaltlich zuständigen öffentlichen Organ zu, d.h. der zuständigen Berufsfachschule oder Mittelschule bzw. dem zuständigen Amt. Das zuständige öffentliche Organ stellt sicher, dass seine Mitarbeitenden diese Richtlinie und die geltenden rechtlichen Vorgaben kennen und beachten.[2]

Wer Daten auf M365 Sek II bearbeitet oder bearbeiten lässt, ist für die Einhaltung des Datenschutzes und der Informationssicherheit im Rahmen dieser Datenbearbeitung verantwortlich.[3]

2 Microsoft 365

2.1 Wofür wird M365 eingesetzt?

Mit M365 werden den Nutzenden verschiedene Dienste für die interne und externe Zusammenarbeit sowie für die Erstellung und Bearbeitung von Dokumenten aus der Cloud zur Verfügung gestellt.

Die Daten in M365 Sek II dürfen langfristig bearbeitet und gespeichert werden. Personenbezogene Daten müssen nach Austritt der betroffenen Person aus der Schule innerhalb von drei Monaten unwiderruflich gelöscht oder archiviert werden[4]. Als geheim oder vertraulich klassifizierte Daten müssen umgehend gelöscht oder archiviert werden, sobald sie nicht mehr benötigt werden. Für die Archivierung gelten die Bestimmungen nach Ziff. 4.

---

2 Art. 4 des Datenschutzgesetzes (sGS 142.1; abgekürzt DSG); in Bezug auf Weiterbildungsabteilungen gilt das eidgenössische Datenschutzgesetz (SR 235.1; nachfolgend eidg. DSG).

3 Art. 3 DSG und Art. 6 f. eidg. DSG.

4 Betreffend Löschung siehe Ziff. 2.4.

2.2 Welche Dienste stehen mit M365 zur Verfügung?

Es stehen insbesondere folgende M365Dienste zur Verfügung:

- Office-365-Anwendungen:
  - Word: Programm zur Textverarbeitung
  - Excel: Programm für Tabellenkalkulationen
  - PowerPoint: Programm für Präsentationen
  - OneNote: Programm zur Erstellung und Organisation von Notizen
  - Exchange Online (Outlook): Kommunikationsinfrastruktur (E-Mail und Kalender)
  - OneDrive: Speicherlösung für nutzerbezogene Daten wie Chatverläufe oder E-Mail-Archiv
  - SharePoint: Speicherlösung für Teams, OneDrive, Planner, Forms, Stream, Project

- Teams: Kollaborationsanwendung mit folgenden Funktionen:
  - Einzel- und Gruppen-Chat
  - Erstellung von Beiträgen in Kanälen
  - Anrufe, Video- und Audiokonferenzen
  - Dokumenten- und Kalenderfreigabe
  - Anzeige der Verfügbarkeit (Anwesenheitsstatus) der Nutzenden
  - Planung und Organisation mittels Aufgaben, Listen, Plänen und Umfragen

2.3 Wo sind die M365-Dienste aufrufbar?

M365-Dienste werden über lokal installierte Office-Anwendungen sowie über Web-Applikationen (https://www.microsoft365.com/) genutzt.

Der Zugang ist durch wenigstens zwei Faktoren gesichert: Login (Nutzername und Passwort) in Kombination mit einem zweiten Faktor, z.B. Microsoft Authenticator.

Mit mobilen Geräten (Smartphones und Tablets) ist der Zugang zu M365 Sek II über spezifische Anwendungen möglich. Die Autorisierung hierfür erfolgt nebst Angabe der Login-Daten (Nutzername und Passwort) über eine Multi-Faktor-Authentifizierung. Geräte, welche die Sicherheitsanforderungen des Bildungsdepartementes nicht erfüllen, können von der Nutzung ausgeschlossen werden.

2.4 Teams

Innerhalb von Teams gibt es verschiedene Teams für die Zusammenarbeit (nachstehend Teams-Raum). Jede Nutzerin oder jeder Nutzer kann grundsätzlich selbständig (im Einklang mit allfälligen, für sie geltenden Vorgaben der jeweiligen Berufsfachschule oder Mittelschule bzw. des Amtes für Mittelschulen oder des Amtes für Berufsbildung) einen Teams-Raum einrichten. Dabei muss sie oder er wenigstens eine Person als Besitzerin oder Besitzer festlegen.

Die Besitzerin oder der Besitzer hat folgende Pflichten:

- Sie oder er vergibt die Zugänge auf den Teams-Raum. Dabei ist das «Need-to-know-Prinzip» zu beachten: Personen erhalten nur Zugang, wenn dies für die Erfüllung ihrer Aufgaben erforderlich ist.
- Sie oder er legt die Rollen der Mitglieder des Teams-Raums fest («Besitzerin oder Besitzer», «Mitglied», «Gast»). Dabei ist wenigstens eine weitere Person als stellvertretende Besitzerin oder stellvertretender Besitzer des Teams-Raums zu bestimmen.
- Sie oder er klassifiziert den Teams-Raum gemäss dem Schutzbedarf der darin bearbeiteten Daten mit einem Label (siehe nachstehend Ziff. 3.2.1).

- Sie oder er installiert die für die Aufgabenerfüllung erforderlichen und zugelassenen M365-Anwendungen im Teams-Raum.
- Sie oder er strukturiert den Inhalt des Teams-Raums und sorgt für die ordnungsgemässe Archivierung der Daten (siehe Ziff. 4) sowie für die unmittelbare und unwiderrufliche Löschung des Raums, soweit dessen Inhalte nicht mehr für die Aufgabenerfüllung benötigt werden.

In einem Teams-Raum können zusätzlich Kanäle erstellt werden. Die dem Teams-Raum unterliegenden Kanäle übernehmen die Klassifizierung des Teams-Raums.

3 Grundsätze der Datenbearbeitung

3.1 Welche Daten dürfen mit M365 bearbeitet werden?

Mit M365 dürfen grundsätzlich alle Arten von Daten bearbeitet werden. Dabei müssen aber zusätzliche Massnahmen beachtet werden, um nicht für die Öffentlichkeit bestimmte Daten zu schützen (siehe nachstehend Ziff. 3.2).

Um eine angemessene Sicherheit zu gewährleisten, müssen in M365 bearbeitete Daten nach ihrem Schutzbedarf strukturiert werden. Hierfür müssen Nutzende die von ihnen bearbeiteten Daten über die *Zuweisung eines Labels* in verschiedenen Bearbeitungsvorgängen klassifizieren.

Je nach Label greifen unterschiedliche technische und organisatorische Massnahmen. Damit können der Zugriff und die Verbreitung von Informationen gesteuert und es kann verhindert werden, dass Unbefugte Kenntnis von Daten erlangen. Die durch das Label erfolgte visuelle Kennzeichnung trägt zudem zu einem sorgfältigeren Umgang mit Daten bei.

3.2 Schutzmassnahmen

3.2.1 Datenklassifizierung mit Labels

Für M365 Sek II bestehen die vier Labels «geheim», «vertraulich», «intern» und «öffentlich»:

	geheim	vertraulich	intern	öffentlich
Definition	Daten, deren Kenntnisnahme durch Unbefugte öffentliche oder schützenswerte private Interessen *schwerwiegend* beeinträchtigen kann.	Daten, deren Kenntnisnahme durch Unbefugte öffentliche oder schützenswerte private Interessen beeinträchtigen kann.	Daten mit grundsätzlich verwaltungs- und schulinternem Charakter.	Daten mit öffentlichem Charakter.
Merkmal	Diese Daten sind nur einem kleinen, klar beschränkten Personenkreis zugänglich.	Diese Daten sind nur einem beschränkten Personenkreis zugänglich (innerhalb der Berufsfachschule oder Mittelschule oder von ihr beauftragten Dritten).	Diese Daten sind grundsätzlich nur der Verwaltung und von ihr beauftragten Dritten zugänglich. Sie können aber auf Anfrage öffentlich zugänglich gemacht werden.	Diese Daten werden von Amtes wegen veröffentlicht, da sie von allgemeinem Interesse sind, oder sie sind bereits allgemein rechtmässig zugänglich.
Rechtsgrundlagen	– Art. 1 Bst. b, d und d^{bis} DSG – Art. 320 und 321 StGB – Art. 67 PersG i.V.m. Art. 3 StVG – Art. 6 und 7 OeffG	– Art. 320 StGB – Art. 67 PersG i.V.m. Art. 3 StVG – Art. 6 und 7 OeffG	Art. 5 OeffG	Art. 4 OeffG
Beispiele	– besonders schützenswerte Personendaten (z.B. religiöse Ansichten, Gesundheit, strafrechtliche Verfahren) – Persönlichkeitsprofile – Profiling – Schlussprüfungen – Disziplinarverfahren – Krankheitsmeldungen mit Angabe von Gründen – Schulpsychologische Berichte o.ä.	– Zeugnisse und Leistungsnachweise – Verträge – Angebote – Offerten – Krankheitsmeldungen ohne Angabe von Gründen – Informationen, die dem Amtsgeheimnis unterstehen (z.B. hängige politische und amtliche Geschäfte; E-Mail mit Angaben zur unangemessenen Bekleidung von Schülerinnen und Schülern)	– Informationen an die Mitarbeitenden – Dienstanweisungen – Unterrichtsunterlagen	– Website – Medienmitteilungen – Newsletter – Social-Media-Beiträge

Abbildung 1: M365 Sek II-Labels

3.2.2 Wann muss ein Label zugewiesen werden?

Beim Versand von E-Mails muss das strikteste Label eines im Anhang angefügten Dokuments übernommen werden.

Wird einem Dokument, das bereits mit einem Label versehen ist, ein Label mit einem tieferen Schutzbedarf zugewiesen (z.B. «intern» statt «geheim»), muss dies im Dialogfeld begründet werden.

3.2.3 Bedeutung der Labels für die Verwendung der M365-Dienste

Je höher der Schutzbedarf (Label), desto eingeschränkter ist der Nutzerkreis, für den ein Dokument oder Inhalte bestimmt sind. Weiter sind folgende organisatorische Massnahmen bei der Verwendung der M365 Sek II-Dienste zu beachten:

	Bearbeitung von Dokumenten mit M365 Sek II	**Exchange Online** (Outlook / E-Mail)	**Microsoft Teams**
geheim	Label «geheim» zuweisen	– E-Mails mit «geheimen» Daten, die aus M365 Sek II versendet werden, müssen entweder verschlüsselt oder in einem verschlüsselten Anhang versendet werden. Ausnahme: Es wird vorgängig schriftlich das Einverständnis der von den «geheimen» Daten Betroffenen für einen unverschlüsselten Versand eingeholt. – Alternativ kann ein Link zu einem Ablageort, zu dem nur Berechtigte Zugang haben, gesendet werden.	– «Geheime» Daten dürfen nur in «geheimen» Teams-Räumen gespeichert werden. – Gäste werden zu «geheimen» Teams-Räumen nicht zugelassen. – Telefonie, Audio- oder Videokonferenzen mit Teams mit «geheimen» Daten dürfen nicht aufgezeichnet werden. – Das Teilen von «geheimen» Daten über die Chatfunktion ist unzulässig.
vertraulich	Label «vertraulich» zuweisen	keine zusätzlichen Massnahmen	«Vertrauliche» Daten dürfen nur in «geheimen» oder «vertraulichen» Teams-Räumen gespeichert werden.
intern	Label «intern» zuweisen	keine zusätzlichen Massnahmen	«Interne» Daten dürfen nur in «geheimen», «vertraulichen» oder «internen» Teams-Räumen gespeichert werden.
öffentlich	Label «öffentlich» zuweisen	keine zusätzlichen Massnahmen	«Öffentliche» Daten dürfen in allen Teams-Räumen gespeichert werden.

Abbildung 2: Schutzmassnahmen bei der Verwendung der M365-Dienste

Auch für Dateien und Anwendungen, die nicht gelabelt werden können, gilt als Grundsatz: Geheime, vertrauliche und interne Daten dürfen nur befugten Personen zugänglich gemacht werden.

4 Archivierung

Für die Aktenführung und Archivierung sind folgende Erlasse und Vorgaben zu beachten:
- Gesetz über Aktenführung und Archivierung (sGS 147.1)
- Verordnung über Aktenführung und Archivierung (sGS 147.11)
- Fachtechnische Richtlinien
- Vereinbarungen zwischen der Schule und dem Staatsarchiv

Vollzug
Diese Nutzungsrichtlinie wird für Schulen angewendet, bei denen Dienst zur Datenklassierung (Labels) aktiviert wurde.

Bettina Surber
Vorsteherin des Bildungsdepartementes