LUZERN

KANTON LUZERN

Vorlage für ein ISDS Nutzungskonzept der Microsoft 365 Plattform in der Volksschule und den kantonalen Schulen

Basiert auf der Vorlage: Nutzungsregelung Microsoft 365 - Umsetzungsinstrument ICT-Coach, Volksschulamt Kanton Zürich.

Stand: 18.01.2023

Dienststelle Volksschulbildung | volksschulbildung.lu.ch

Inhaltsverzeichnis

1 Ausgangslage

Die Volksschulen und die kantonalen Schulen im Kanton Luzern nutzen die Microsoft 365 Plattform (nachfolgend M365).

Alle Schulen zeigen die Tendenz sich von der eigenen Serverinfrastruktur zu lösen und Clouddienste als Services zu nutzen. Aktuell werden drei Clouds eingesetzt. Die M365 Cloud, die LehrerOffice Cloud und die Cloud der Schulverwaltung. Ziel ist es, sämtliche Schuldaten in diesen drei Clouds zu speichern.

Um M365 in der Volksschule und den kantonalen Schulen datenschutzkonform einzusetzen, gilt es verschiedene Abklärungen und Massnahmen zu ergreifen. Dieses ISDS Nutzungskonzept konkretisiert den Einsatz der M365 Plattform an der Schule unter Berücksichtigung informations- und datenschutzrechtlicher Aspekte.

Für den konformen Einsatz ist der Mandant der Schule unter dem Rahmenvertrag von Educa lizenziert. Dieser legt den Gerichtsstandort Schweiz fest und beschränkt den Serverstandort für die Mehrheit der Dienste auf Europa [1] oder die Schweiz. Auf Dienste mit einem Serverstandort ausserhalb dieser Regionen wird im Nutzungskonzept (Kapitel 6.9) ein besonderer Fokus gelegt.

2 Nutzungskonzept

Die Schule setzt die unterschiedlichen Dienste der M365 Plattform für verschiedene Aufgaben ein. Erst die Kombination und das Zusammenspiel der einzelnen Dienste macht die Plattform zu einem vollwertigen digitalen Arbeitsraum.

Das Konzept nutzt zur Beschreibung dieser Aufgaben die folgenden drei Einsatzbereiche

- Persönliche Produktivität
- Gemeinsame Produktivität
  - Fokus Unterricht
  - Fokus Schulorganisation
- Kommunikation
  - Fokus Unterricht
  - Fokus Schulorganisation

Im Einsatzbereich der gemeinsamen Produktivität arbeiten unterschiedliche Benutzergruppen zusammen. Nachfolgend eine alphabetische Liste dieser Benutzergruppen.

- Bildungskommission
- Erziehungsberechtigte
- Gäste
- Hausdienst
- IT-Support (extern)
- IT-Support (intern)
- Lehrpersonen
- Lernende
- Praktikanten
- Rektor
- Schuldienste (SoZ, SPD, PSMo, Logo)
- Schulleitung
- Sekretariat
- Tagesstrukturen
- Zivildienstleistende

[1] Austria (Vienna), Finland (Helsinki), France (Paris, Marseille), Ireland (Dublin), Netherlands (Amsterdam)

Je nach Einsatzbereich und Benutzergruppe variiert der Einsatzzweck der Dienste. Die Aufstellung im nächsten Kapitel schafft diesbezüglich eine Übersicht.

3 Einsatzbereiche Produktivität und Kommunikation

Jeder M365 Benutzer der Schule hat je nach Einsatzbereich – persönliche Produktivität, gemeinsame Produktivität oder Kommunikation - Zugriff auf die aufgeführten Dienste. Wie die entsprechenden Dienste innerhalb dieses Einsatzbereichs genutzt werden, ist in der angefügten Tabelle beschrieben. Welche Art von Informationen mit einem Dienst verarbeitet werden dürfen, ist im Kapitel 4 beschrieben. Die Plattform bietet in jedem Bereich weitere Dienste an, die sind grundsätzlich global deaktiviert (Kapitel 6.9).

Der Einsatzbereich der ***persönlichen Produktivität*** geht davon aus, dass der Dienst für schulische Zwecke genutzt wird und die erzeugten Inhalte grundsätzlich nur dem Urheber zugänglich sind.

Der Bereich der ***gemeinsamen Produktivität*** geht davon aus, dass mehrere Benutzer über einen oder mehrere Dienste hinweg zusammenarbeiten. Die Benutzer sind in Gruppen (Teams) organisiert, die entsprechend der Vorgabe im Berechtigungskonzept (Kapitel 5) erstellt werden.

Der Bereich ***Kommunikation*** zeigt auf, wie die Benutzer die Kommunikationsmöglichkeiten Email und Chat intern und extern einsetzen.

3.1 Persönliche Produktivität

Die folgenden Dienste stehen allen Benutzern für die persönliche Produktivität zur Verfügung. Inhaltlich müssen die Benutzer darauf achten, dass sie nur zulässige Informationen mit dem Dienst verarbeiten (vgl. Kapitel 4).

Dienst	Zweck
Office Dokument Word, Excel, PowerPoint	Dienst zur Bearbeitung von Text-, Bild-, Ton- und Videomaterial.
OneDrive for Business	Dienst für das Speichern digitaler Inhalte die Benutzer nur in Ausnahmefällen anderen zugänglich machen.
OneNote	Dienst für die Sammlung von Informationen in Form von Notizen.
Forms	Dienst für die Erstellung von Umfragen und Quiz. Das Teilen einer Umfrage erfordert immer zusätzliche Massnahmen (Kapitel 6.9).
Sway	Dienst für das Erstellen von digitalen Präsentationen. Das Teilen einer Präsentation über einen öffentlichen Link erfordert zusätzliche Massnahmen (Kapitel 6.9).
Whiteboard	Digitale Pinnwand für die gemeinsame Arbeit.
Stream	Dienst für das Aufnehmen und Bearbeiten von Videos.
Plastischer Reader	Dienst der die Barrierefreiheit von Text verbessert.
To-Do	Dienst der bei der Aufgabenverwaltung hilft.
Power Automate	Dienst für die Automatisierung von Geschäftsprozessen in Form von Workflows.

3.2 Gemeinsame Produktivität

Der Einsatzbereich der gemeinsamen Produktivität unterscheidet den Fokus Unterricht und den Fokus Schulorganisation.

3.2.1 Fokus Unterricht

In diesem Fokusbereich steht die Zusammenarbeit zwischen Lehrpersonen und Lernenden im Zentrum. Inhaltlich müssen die Benutzer darauf achten, dass sie nur zulässige Informationen mit dem Dienst verarbeiten (vgl. Kapitel 4).

Dienst	Zweck
Office Dokument (geteilt)	Grundsätzlich findet die Zusammenarbeit an Dateien im Klassenteam statt. In Ausnahmefällen wird auf ein geteiltes Dokument ausgewichen.
Teams (SharePoint)	Die Zusammenarbeit und der Austausch von Dateien finden im dafür vorgesehen Teams (SharePoint) statt.
Klassennotizbuch (Class Notebook)	Klassennotizbücher unterstützen die Zusammenarbeit mit der Klasse. Entsprechend der im Notizbuch vorgegebenen Berechtigungsstruktur werden Inhalte zur Verfügung gestellt oder bearbeitet. Klassennotizbücher werden in einem Teams angelegt.
Sway (geteilt)	Lehrpersonen oder Lernende können Unterrichtsinhalte in einer Sway Präsentation aufbereiten und dann innerhalb der Institution teilen. Das Teilen einer Präsentation über einen öffentlichen Link erfordert zusätzliche Massnahmen (Kapitel 6.9).
Forms (geteilt)	Lehrpersonen oder Lernende können Unterrichtsinhalte in Forms aufbereiten und dann innerhalb der Institution teilen. Das Teilen einer Umfrage erfordert immer zusätzliche Massnahmen (Kapitel 6.9).
Whiteboard (geteilt)	Lehrpersonen oder Lernende können Unterrichtsinhalte im Whiteboard aufbereiten und dann innerhalb der Institution teilen.
Planner	Lehrpersonen oder Lernende können mit dem Werkzeug Pläne erstellen und Aufgaben innerhalb der Klasse organisieren.

3.2.2 Fokus Schulorganisation

Dieser Abschnitt fokussiert auf die Zusammenarbeit zwischen Mitarbeitern in der Institution. Inhaltlich müssen die Benutzer darauf achten, dass sie nur zulässige Informationen mit dem Dienst verarbeiten (vgl. Kapitel 4).

Dienst	Zweck
Office Dokument (geteilt)	Existiert für die Zusammenarbeit kein geeignetes Teams (SharePoint), kann zeitlich begrenzt auf ein geteiltes Dokument ausgewichen werden. Nach Abschluss der Zusammenarbeit wird die Funktion Teilen aufgehoben.
Teams (SharePoint)	Die Zusammenarbeit und der Austausch von Daten finden in den vorgesehenen Teams und ihren entsprechenden Strukturen (Kanalorganisation, Ordner) statt.
OneNote (geteilt)	Für die Zusammenarbeit im Schulteam werden Notizbücher in einem bestehenden Teams erstellt und genutzt. Nur in Einzelfällen wird auf ein geteiltes Notizbuch eines Benutzers ausgewichen.

Sway (geteilt)	Für Aufgaben im Bereich der Schulorganisation können Sway Präsentation aufbereiten und innerhalb der Institution geteilt werden. Das Teilen einer Präsentation über einen öffentlichen Link ist nicht vorgesehen.
Forms (geteilt)	Für Aufgaben im Bereich der Schulorganisation können Umfragen in Forms aufbereiten und dann innerhalb der Institution geteilt werden. Das Teilen einer Umfrage erfordert zusätzliche Massnahmen.
Whiteboard (geteilt)	Für Aufgaben im Bereich der Schulorganisation können Whiteboards erstellt und innerhalb der Institution geteilt werden. Das Teilen von Whiteboards über einen öffentlichen Link wird nicht vorgesehen.
Planner	Für die Organisation und Planung von Aufgaben kann in einem Teams der Planner genutzt werden.

3.2.2.1 Handhabung von Daten mit erhöhtem Schutzbedarf für Lehrpersonen und Mitarbeiter

Lehrpersonen und Mitarbeiter nutzen grundsätzlich die Schulverwaltungslösung[2] als sichere Cloud für Daten mit einem erhöhten Schutzbedarf (vgl. Kapitel 4).

Da LehrerOffice auf der Volksschule aktuell keine Datenablage zur Verfügung stellt und keine Schulverwaltungslösung im Einsatz ist, können Lehrpersonen und Mitarbeiter übergangsweise bis zur Einführung der Schulverwaltungslösung Dokumente mit erhöhtem Schutzbedarf im M365 speichern (sofern keine andere sichere Alternative zur Verfügung steht). Alle Benutzer erfüllen die nachfolgenden drei Bedingungen.

- Haben eine A3 Lizenzierung mit A5 Compliance Suite.
- Die Funktion Customer Lockbox ist aktiviert (vgl. Anhang 1).
- Die Benutzer nutzen aktiv die 2FA (vgl. Anhang 1).

3.2.2.2 Handhabung von Daten mit erhöhtem Schutzbedarf für Rektorat, Schulleitung und Schulsekretariat

Rektorate und Schulleitungen nutzen grundsätzlich die Schulverwaltungslösung als sichere Cloud für Daten mit einem erhöhten Schutzbedarf (vgl. Kapitel 4).

Da LehrerOffice Zusatz auf der Volksschule aktuell keine Datenablage zur Verfügung stellt, keine Schulverwaltungslösung im Einsatz ist, speichert das Rektorat, die Schulleitung und das Schulsekretariat übergangsweise bis zur Einführung der Schulverwaltungslösung Dokumente mit erhöhtem Schutzbedarf im M365. Alle Benutzer erfüllen die nachfolgenden drei Bedingungen.

- Haben eine A3 Lizenzierung mit A5 Compliance Suite.
- Die Funktion Customer Lockbox ist aktiviert (vgl. Anhang 1).
- Die Benutzer nutzen aktiv die 2FA (vgl. Anhang 1).

3.2.2.3 Handhabung von Daten mit erhöhtem Schutzbedarf für die Schuldienste

Schuldienste (SoZ, SPD, PSMo, Logo) nutzen grundsätzlich die zur Verfügung stehende Schulverwaltungslösung als sichere Cloud für Daten mit einem erhöhten Schutzbedarf (vgl. Kapitel 4).

[2] Schulverwaltungslösungen bei den kantonalen Schulen sind: schulNetz, EcoOpen, Sephir und CMI-Axioma.

Da dem Schuldienst aktuell keine Schulverwaltungslösung zur Verfügung steht, und keine lokalen Speichermöglichkeiten existieren, speichert der Schuldienst übergangsweise bis zur Einführung der Schulverwaltungslösung Dokumente mit erhöhtem Schutzbedarf im M365. Alle Benutzer erfüllen die nachfolgenden drei Bedingungen.

- Haben eine A3 Lizenzierung mit A5 Compliance Suite.
- Die Funktion Customer Lockbox ist aktiviert (vgl. Anhang 1).
- Die Benutzer nutzen aktiv die 2FA (vgl. Anhang 1).

3.3 Kommunikation

Der Einsatzbereich Kommunikation unterscheidet wie der Bereich gemeinsame Produktivität den Fokus Unterricht und den Fokus Schulorganisation.

3.3.1 Fokus Unterricht

Dienst	Zweck
Teams Chat	Die Chatfunktion in Teams dient dem zielgerichteten, internen Austausch in der Klasse. Die Funktion wird nicht für das Teilen von Dateien eingesetzt, da geteilte Dateien sonst aus dem OneDrive des Senders geteilt werden. Besteht der Wunsch ein Dokument auf diesem Weg in eine Diskussion einzubetten, wird das Dokument aus der entsprechenden Ablage verlinkt. Lernende nutzen die Funktion nur intern.
Teams Kanäle	Die Beitragsfunktion in einem Kanal dient der Kommunikation innerhalb der Gruppe. Alle Mitglieder in der Gruppe können alle Beiträge lesen und kommentieren. Das Erstellen neuer Beiträge kann den Besitzern (Lehrpersonen) vorbehalten sein. Dateien werden ins Teams hochgeladen und nicht mittels Freigaben aus dem persönlichen Produktivitätsbereich geteilt.
Outlook	Lernende nutzen Emails für die unterrichtsbezogene Kommunikation mit internen und externen Personen. Eine automatische Weiterleitung von Nachrichten an eine Adresse ausserhalb der Plattform ist blockiert.

3.3.2 Fokus Schulorganisation

Dienst	Zweck
Teams Chat	Die Chatfunktion in Teams dient dem internen Austausch zwischen Einzelpersonen oder Gruppen um unterrichtsbezogene oder organisatorischen Fragestellungen schnell zu klären.
Teams Kanäle	Die Beitragsfunktion in einem Kanal dient der Kommunikation innerhalb eines Teams. Alle Mitglieder in einem Teams können alle Beiträge lesen und kommentieren. Das Erstellen neuer Beiträge ist den Besitzern eines Teams vorbehalten.
Outlook	Outlook dient der dokumentierten internen und externen Kommunikation. Immer dann, wenn die Nachvollziehbarkeit einer Sache zu einem späteren Zeitpunkt wichtig ist, wird dieser Dienst Teams vorgezogen. Daten mit der Klassifizierung IV dürfen per Mail intern und extern nur mittels der Funktion Microsoft 365 Message Encryption (OME) ausgetauscht werden (vgl. Kapitel

	3.3.3). Eine automatische Weiterleitung von Nachrichten an eine Adresse ausserhalb der Plattform ist blockiert.

3.3.3 Emailversand von Daten mit erhöhtem Schutzbedarf

Für den Versand von Daten mit einem erhöhten Schutzbedarf per Email nutzen allen Benutzer die Microsoft 365 Message Encryption (OME-Legacy).

Option 1 – Nur verschlüsseln
Option 2 – Nicht weiterleiten.

Werden Nachricht mit der Option 1 – gekennzeichnet, können sie vom Empfänger nach einer Identitätsprüfung an einem beliebigen Ort gespeichert werden und sind anschliessend ohne Identitätsprüfung durch beliebige Benutzer bearbeitbar.

Wird die Option 2 gewählt – bleibt die Verschlüsselung auch nach dem Download bestehen und Anhänge (Einschränkung auf Office-Dokumente) können weiterhin nur nach einer Identitätsprüfung geöffnet werden.

Beim Austausch mit externen Personen müssen sich diese mit einer Einmalkennung über ihre Email-Adresse am Microsoft OME-Portal authentifizieren um die Nachricht und allfällige Anhänge abrufen.

Durch die Möglichkeit der erweiterten Nachrichtenverschlüsselung aus Microsoft Purview (A5 Compliance Suite) sind Richtlinien und Schlüsselwörter für die automatische Verschlüsselung konfigurierbar. Die native Inlineerfahrung im Outlook und die automatische Auszeichnung erhöhen die Nutzerfreundlichkeit deutlich.

Mit den individualisierten Brandingvorlagen können verschiedene Benutzergruppen (Schulverwaltung / Schuldienste) nach aussen unterscheidbar auftreten.

4 Datenklassifizierung

Die Daten an der Schule werden in vier Kategorien eingeteilt. Sind Schutzmassnahmen nötig, sind diese in der entsprechenden Zelle angegeben.

Klassifizierung	Beispiele	Speicherort **ohne** Schulverwaltungslösung (Volksschulen)
I Private Daten	• Jegliche privaten Dateien, Bilder und Medieninhalte	⊗ Ablage nicht erlaubt
II Unterrichtsmaterial ohne Personenbezug	• Unterrichtsvorbereitungen (bspw. Arbeitsblätter, Lernsoftware) • Prüfungsvorbereitungen	✓ Ablage erlaubt
III Unterrichtsmaterial mit Personenbezug	• Fotolisten • Korrigierte Prüfungen	✓ Ablage erlaubt
	• Gesammelte Daten über mehrere Lernende (bspw. Adresslisten, Klassenlisten, Notizen, Notenlisten, Prüfungsresultate)	✓ Wenn LehrerOffice die Funktionalität nicht bietet, befristet bis zur Einführung der neuen Schuladministrationssoftware.

IV – Daten mit erhöhtem Schutzbedarf	Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit mit anderen Informationen die Gefahr einer Persönlichkeits- oder Amtsverletzung besteht. • Zeugnisse, Verhaltensnotizen, Lernberichte • Schulärztliche oder Schulpsychologische Untersuchungsunterlagen • Informationen die dem Amts- oder Berufsgeheimnis unterstehen. • Religiöse oder politische Ansichten	✅ Wenn LehrerOffice die Funktionalität nicht bietet, befristet bis zur Einführung der neuen Schuladministrationssoftware. **Schutzmassnahmen:** 2FA und aktive «Customer Lockbox», alternativ 2FA und Verschlüsselung auf Datei oder Container Ebene. Interne und externe E-Mail Kommunikation via OME.

5 Berechtigungskonzept

Die Schule legt mit diesem Berechtigungskonzept fest, welche Benutzergruppen in den zwei Einsatzbereichen – persönliche Produktivität und gemeinsame Produktivität - Zugriff auf die dort vorhandenen Informationen haben.

5.1 Berechtigungen im persönlichen Produktivitätsbereich

Standartmässig hat nur der Benutzer selbst Zugriff auf die mit einem Dienst erstellen Inhalte. Über die aktive Nutzung der Funktion Teilen kann der Benutzer einzelne Inhalte mit einem Lese- oder Schreibrecht an weitere Nutzer freigeben. Eine solche Freigabe soll in Ausnahmefällen erfolgen und immer zeitlich begrenzt werden. Im Fall einer öffentlichen Freigabe per OneDrive (Jeder mit dem Link) muss ein Passwort gesetzt werden.

5.2 Berechtigungen im gemeinsamen Produktivitätsbereich

Für die Erstellung und Löschung von Gruppen (Teams) ist der ICT-Verantwortliche in der Funktion technischer Betreuer im Aufgabenbereich M365 zuständig. Er hat eine Berechtigung für das Microsoft Teams Admin Center und kann dort Mutationen vornehmen ohne Einblick in die entsprechenden Teams zu nehmen. Im laufenden Betrieb haben Benutzer mit der Rolle Besitzer die Möglichkeit Mutationen innerhalb ihres Teams vorzunehmen. Besitzer einer Gruppe sind verantwortlich für die Nutzung der Teams entsprechend den definierten Angaben im Kapitel 3. Eine Liste aller Teamvarianten und SharePoint Ablagen der Schule inkl. Berechtigungsstruktur befinden sich im Anhang 2. Eine öffentliche Freigabe (Jeder mit dem Link) einzelner Inhalte ist nicht möglich.

6 Weitere Massnahmen zum Schutz der Daten

6.1 Protokollierung

Bei der Nutzung der M365 Dienste fallen Daten über die Benutzer und deren Aktivitäten automatisch an und werden erfasst und gespeichert. Die Funktionsdaten dürfen nur bearbeitet werden, wenn dies für das Funktionieren des Systems notwendig ist. Bei Verdacht auf einen Missbrauch der Dienste durch die Benutzer können Protokolldaten stichprobenweise und nach vorgängiger Information der Betroffenen ausgewertet werden.

Eine Auswertung erfordert die Zustimmung der Schulleitung und erfolgt nach dem 4-Augen Prinzip.

6.2 Passwort und Authentifizierung

Geht ein Passwort verloren, meldet sich der Benutzer beim ICT-Betreuenden der Gesamtschule, der ihm ein neues temporäres Passwort zustellt. Dieses ändert der Benutzer beim ersten erfolgreichen Login entsprechend der vorgegebenen Komplexität.

Sobald Personen auf Daten mit erhöhtem Schutzbedarf zugreifen, muss die 2 Faktoren Authentifizierung (2FA) für die jeweiligen Benutzer aktiviert sein. Diese kommt immer zur Anwendung, wenn Daten auf einem nicht schuleigenen Gerät oder ausserhalb des Schulnetzes abgerufen werden. Auf schuleigenen Geräten ist die Anmeldehäufigkeit reduziert und eine 2FA Prüfung findet entsprechend der konfigurierten Richtlinie statt. Wahlweise findet die zweite Authentifizierung über das Gerät statt, oder via «SMS Token» oder «Authenticator App».

Für Zugriffe mit einem geografischen Standort ausserhalb der Schweiz müssen sich Benutzer immer mittels 2FA authentifizieren.

6.3 Verschlüsselung der Daten und Customer Lockbox

Sämtliche Daten im M365 sind standartmässig verschlüsselt abgelegt. Der Schlüssel liegt aber im Besitz von Microsoft. Mit Hilfe der «Customer Lockbox» wird verhindert, dass Microsoft ohne Zustimmung der Schule auf die Daten zugreift. Die dem Freigabeprozess zugeordneten Personen ist im Anhang 1 aufgeführt.

6.4 Löschen

Mitarbeitende der Schule können gemäss ihren Berechtigungen Daten löschen bzw. an einen neuen Speicherort übertragen. Auch Lernende der Schule können entsprechend ihren Rechten Daten löschen bzw. an einen neuen Speicherort übertragen. Ein automatisches Löschen von Daten nach einer gewissen Zeit findet nicht statt.

Beim Austritt einer Person aus der Schule wird der Account und alle damit zusammenhängenden Daten aus dem **persönlichen Produktivitätsbereich** gelöscht. Der Löschvorgang sieht eine Aufbewahrungsfrist von 30 Tagen vor, nach Ablauf dieser Frist ist eine Wiederherstellung nicht mehr möglich. Im Fall einer Zugriffsdelegierung wird der Benutzer vor der Delegierung darüber informiert.

Alle im **gemeinsamen Produktivitätsbereich** (Teams/SharePoint) entstanden Daten bleiben bis zur Löschung des jeweiligen Teams (SharePoint) erhalten.

Nicht mehr benötigte Teams werden jeweils am Ende eines Kalenderjahrs gelöscht, falls die Löschung nicht vom Teambesitzer selbst initialisiert wird.

Nicht mehr benötigte Teams können anhand der Namensgebung und der Anzahl Mitglieder identifiziert werden. Wird der Löschvorgang durch einen Administrator initialisiert, erhält der Teambesitzer eine Ankündigung. Der Löschvorgang sieht eine Aufbewahrungsfrist von 30 Tagen vor, nach Ablauf dieser Frist ist eine Wiederherstellung nicht mehr möglich.

6.5 Meldung von Sicherheitsvorfällen

Alle Meldungen zu Sicherheitsvorfällen sind an die Schulleitung zu richten und müssen mindestens folgende Informationen enthalten:

(1) Beschreibung zum Vorfall, (2) Erkennungsdatum, (3) Dauert der Vorfall noch an oder ist er schon behoben (4) Befund, wie es zum Vorfall gekommen ist (5) Massnahmen

Die Schulleitung entscheidet, ob die Massnahmen ausreichend sind und ob für weitere Schritte der Einbezug der Bildungskommission notwendig ist. In jedem Fall muss die Bildungskommission umgehend informiert werden, wenn weitere Stellen (bspw. Datenschutzbeauftragter, Kantonspolizei) in den Vorfall involviert sind, ansonsten reicht eine Information im Rahmen der bestehenden Austauschgefässe aus.

6.6 Externer Support

Die Unternehmung X hat ein globales Administratoren Konto und nutzt dieses Konto zur Leistungserbringung im Rahmen des vereinbarten Vertrags.

6.7 Backup und Notfallplanung

Dieser Bereich unterscheidet die Datenablage (SharePoint und OneDrive) und die E-Mail-Postfächer (Exchange-Online). Hier werden die seitens der Plattform erbrachten Schutzmassnahmen aufgeführt.

6.7.1 Schutzmassnahmen SharePoint und OneDrive

Seitens der M365-Plattform

Aspekt	Schutzmassnahme	Beschreibung
Datenverlust im Fall von	Hardwarefehlern, Netzwerk- oder Stromausfällen und Naturkatastrophen	Echtzeit Duplizierung der Daten und Metadaten in ein primäres und sekundäres Rechenzentrum (Georedundante Speicherung). Duale Netzwerkschnittstelle und Stromversorgung im Rechenzentrum.
Verfügbarkeit	Automatisches Failover	Bei einem sandortspezifischen Ereignis werden Benutzeraktivitäten automatisch in die sekundäre Umgebung weitergeleitet.
Speichermedium	Azure Storage (Blob-Container)	Cloud-Speicherlösung von Microsoft für das Speichern grosser, unstrukturierter Datenmengen.
Sicherungsart und BackUp-History	**Versionsverwaltung**	Standartmässig werden 500 Versionen einer Datei beibehalten
	Datenwiederherstellung (Point-in-Time) - Schützt vor Ransomware, Massenlöschung)	Daten können innerhalb der letzten 30 Tage an einen beliebigen Zeitpunkt zurückgesetzt werden.
	Papierkorb	Gelöschte SharePoint Dateien werden 93 Tage in der Wiederverwendungspipline aufbewahrt. Anschliessend erfolgt die endgültige Löschung nach einer Frist von 14 Tagen.

Quelle: https://docs.microsoft.com/de-de/compliance/assurance/assurance-sharepoint-onedrive-data-resiliency

6.7.2 Schutzmassnahmen Exchange-Online

Seitens der M365-Plattform

	Schutzmassnahme	Beschreibung
Datenverlust	Schutz vor Hardwarefehlern, Netzwerk- oder Stromausfällen und Naturkatastrophen	Echtzeit Duplizierung der Daten und Metadaten in ein primäres und sekundäres Rechenzentrum (Georedundante Speicherung). Duale Netzwerkschnittstelle und Stromversorgung im Rechenzentrum
Verfügbarkeit	Automatisches Failover	Bei einem sandortspezifischen Ereignis werden Benutzeraktivitäten automatisch in die sekundäre Umgebung weitergeleitet.
Sicherungsart und BackUp-History	**Papierkorb** (Gelöschte Elemente)	Gelöschte Elemente bleiben bis zur Leerung im Papierkorb. Beim Löschen aus dem Papierkorb, werden sie in den Bereich Wiederherstellbare Elemente verschoben.
	Wiederherstellbare Elemente	Abhängig von den Einstellungen werden gelöschte Elemente nach Ablauf der hinterlegten Frist (standardmässig 14 Tage) endgültig gelöscht. Die Funktionen Archiv, In-Place Hold oder Litigation Hold können den Aufbewahrungszeitraum verlängern.
	Datenwiederherstellung (Point-in-Time)	nicht möglich

Quelle: https://docs.microsoft.com/de-de/exchange/back-up-email

6.8 Information an die Eltern

Die Eltern werden in einem Schreiben über die Nutzung der M365 Plattform informiert. Lernende ab der 3. PS verfügt über ein M365 Login. Durch eine Einführung der Lehrperson ist sichergestellt, dass die Lernenden die wichtigsten Punkte im Unterricht kennenlernen. Ergänzend haben alle Lernenden und Eltern das Nutzungsreglement (X) unterschrieben.

6.9 Dienste mit besonderen Massnahmen

Dienst		Schutzmassnahmen
Sway (geteilt)	Werden Sway Präsentationen öffentlich geteilt, müssen Persönlichkeitsrechte und Urheberrechte berücksichtigt werden. Im Zweifelsfall soll der Zugang mit einem Passwort abgesichert werden. Es dürfen nur Daten mit der Klassifizierung II verarbeitet werden.	Nur Daten mit der Klassifizierung II Öffentliches Teilen einschränken oder beim öffentlichen Teilen ein Passwort für die Anzeige setzen.
Forms (geteilt)	Werden Umfragen geteilt, müssen die Teilnehmer der Umfrage in der Beschreibung über die folgenden Punkte informiert werden:	

	Wer sammelt die Daten (Ansprechperson) Wozu werden die Daten gesammelt (Zweck) Werden die Daten mit oder ohne Personenbezug ausgewertet.	

6.10 Archivierung

Nicht mehr benötigte Dokumente sind nach Ablauf der Aufbewahrungsdauer dem Gemeindearchiv anzubieten (gesetzliche Anbietepflicht gemäss § 33 Gemeindegesetz vom 4. Mai 2004 i.V.m § 6 des Gesetzes über das Archivwesen vom 16. Juni 2003). Die Auswahl der archivwürdigen Akten wird durch das Gemeindearchiv getroffen. Für weitere Informationen hierzu vgl. Merkblatt Amtsgeheimnis und Datenschutz, Aufbewahrung von Daten der Dienststelle Volksschulbildung.

Anhang 1 – Benutzerrollen, 2FA und Customer Lockbox (immer zum Schuljahresstart aktualisieren).

Benutzer mit speziellen Berechtigungen in administrativen Rollen

Rolle	Beschreibung	Aufgaben	Vorname	Nachname
Globaler Administrator	Kann alle Aspekte von Azure AD und Microsoft Diensten verwalten.	Tenant Grundkonfiguration		
Benutzeradministrator	Kann alle Aspekte von Benutzer und Gruppen verwalten.	Benutzer erstellen und löschen Zuordnung in Sicherheitsgruppen		
Teams Administrator	Kann den Microsoft Teams-Dienst verwalten	Erstellung und Löschung von Gruppen (Teams). Zuweisung der Besitzer.		
Intune Administrator	Kann alle Aspekte des Intune-Produkts verwalten	Zuständig für die Verwaltung und Einrichtung der schuleigenen Geräte.		
Genehmiger für Kunden-LockboxZugriff	Kann Microsoft Supportanfragen zum Zugriff auf Benutzerdaten genehmigen	Kann Microsoft eine Freigabe auf die vorhandenen Daten gewähren.		

Benutzergruppe(n) mit aktiver 2FA

AzureAD Gruppen	Beschreibung	Anstellungsfunktionen	
ADM-Lehrer	Benutzergruppe(n) die alle Personen in den aufgeführten Anstellungsfunktionen umfasst.		

Benutzergruppe(n) mit OME oder zugewiesener A5 Compliance Suite

AzureAD Gruppen	Beschreibung	Hinweis	
	Benutzergruppe(n) die für den Customer-Lockbox Prozess lizenziert sind.	Müssen eine Lizenz für die A5 Compliance Suite haben.	
	Benutzergruppe(n) welche die Möglichkeiten von OME oder Microsoft Purview Nachrichtenverschlüsselung nutzen.		

Anhang 2 – Berechtigungen für Teams und SharePoint Ablagen

Berechtigungsfokus Unterricht

Klassen- und Fachgruppenteams (Teams)	Lernende	Lehrpersonen	Gäste	Keinen Zugriff
Beispiele: PS-3/4-a Sek-19-22-AB	Lernende der entsprechenden Klasse partizipieren in der Rolle Mitglied im entsprechenden Klassenteam.	nur Lehrpersonen mit einem Bezug zur Klasse werden in der Rolle (Besitzer) ergänzt. Mutationen werden durch die Klassenlehrperson vorgenommen.	Studierende der PHLU werden für den Zeitraum ihres Praktikums mit dem Account der PHLU in die Klasse als Gast aufgenommen.	Schulleitung SSA Hausdienst BIKO und die restlichen Benutzergruppen aus Kapitel 2

Berechtigungsfokus Schulorganisation

Gesamtschule

Schulteams Teams	Lehrpersonen	Lehrpersonen mit Leitungsfunktion im Zyklus	Gäste	Keinen Zugriff
Beispiele: BS-ALLE PS-ALLE SEK-ALLE	Lehrpersonen haben Zugriff auf die zu ihrem Vertrag passenden Zyklen. Sie werden in der Rolle Mitglied erfasst.	Lehrpersonen die eine Leitungsfunktion im Zyklus innehalten werden in der Rolle Besitzer ergänzt. Sie können für die ihnen zugeordnete Teammitglieder Mutationen vornehmen.	Studierende der PHLU werden für den Zeitraum ihres Praktikums mit dem Account der PHLU in das Schulteam aufgenommen	Lernende Hausdienst BIKO und die restlichen Benutzergruppen aus Kapitel 2

Aufgabenspezifische Teams

Teams	Lehrpersonen	SL	BIKO	Keinen Zugriff
Krisenmanagement	Lehrpersonen in der Funktion SIBE haben die Rolle Mitglied	Die Schulleitung ist Mitglied in der Rolle Besitzer und nimmt Mutationen vor.	In der Rolle Mitglied	die restlichen Benutzergruppen aus dem Kapitel 2

Teams	BIKO			Keinen Zugriff
BIKO	Das Mitglied in der Funktion als Präsident nimmt Mutationen vor und hat die Rolle Besitzer.			die restlichen Benutzergruppen aus dem Kapitel 2

Weitere Möglichkeiten

- IF Fachgruppe
- Fachspezifische Teams
- Schulhaus Teams

Anhang 3 - Checkliste technische und organisatorische Massnahmen

	Technische Massnahmen	Details	Link	Datum
1	Benutzerrollen, Customer-Lockbox	✎ Anhang 1 Export aus AAD	 AAD-AC Link	
2	Benutzergruppen mit aktiver MFA Erfassung für 2FA	✎ Anhang 1	AAD-AC Link	
3	Bedingter Zugriff - Signale (Standort, Gerät) für MFA Anforderung konfiguriert	Vgl. Kapitel 6.2	AAD-AC Link	
4	Datenspeicherort Schweiz für Dienste prüfen.	Vgl. Kapitel 1	AdminPortal	
5	Nicht erforderliche Dienste / Apps deaktivieren.	Vgl. Kapitel 3	AAD-AC Link	
6	Benutzerfreigabe für Zustimmung von Benutzern zu Apps auf Administratoren einschränken.	Vgl. Kaptiel 3	AdminPortal	
7	Diagnosedaten, Telemetrie und externe Speicheranbieter innerhalb der Microsoft Cloud deaktivieren Client: Microsoft 365 Apps for Enterprise Cloud: Office-Cloudrichtliniendienst Viva Learning – Diagnosedaten deaktivieren Viva Insights – Teams App blockieren Cortana – Zugriff auf CloudDaten deaktivieren	Vgl. Kapitel 6.1	 AdminPortal Teams Admin Portal AdminPortal	
8	SharePoint: Richtlinien für das Teilen Einrichten. Standardberechtigung für Datei- und Ordnerlinks festlegen auf Option: Nur Personen in Ihrer Organisation. Teilen ohne Anmeldung für SharePoint einschränken.	Vgl. Kapitel 5.2	SP AC SharePoint Admin Center	
9	Sway: Teilen mit Personen ausserhalb der Organisation einschränken, oder organisatorische Massnahme umsetzen.	Vgl. Kapitel 6.9	AdminPortal	
10	Email-Forwarding Policy und OME	Vgl. Kapitel 3.3	Exchange Admin Center	

	Organisatorische Massnahmen	Details	Link	Datum
	Alle Mitarbeiter kennen die Datenklassifizierung und können entsprechend den aufgeführten Teams (SharePoint-Ablagen) Daten an ihren vorgesehenen Bestimmungsort speichern.	Kaptiel 4 Vgl. Anhang 2		