Mecklenburg-Vorpommern
Ministerium für Bildung,
Wissenschaft und Kultur

Betriebserlass eines zentralen Identitätsmanagementsystems für die öffentlichen allgemein bildenden und beruflichen Schulen des Landes Mecklenburg-Vorpommern

Inhaltsverzeichnis

I. Einleitung

1. Was ist das IDM?

Das vom Ministerium für Bildung, Wissenschaft und Kultur M-V betriebene zentrale Identitätsmanagementsystem (IDM) beinhaltet die sichere Verwaltung und Pflege digitaler Identitäten. Die Nutzung des zentralen IDM ist verpflichtend, wenn eine Schule eine neue Software einführt, die zur Erfüllung des Unterrichts- und Erziehungsauftrages, der Schulplanung, der Schulorganisation, sowie der Schulaufsicht erforderlich ist. Unter digitaler Identität ist die Sammlung von personenbezogenen Attributen, die eine Person im Umfeld der digitalen Schuldienste eindeutig kennzeichnet, zu verstehen. Das IDM stellt somit personenbezogene Daten konsistent, verlässlich, ständig verfügbar und aktuell für Schuldienste bereit und ermöglicht eine automatisierte Verwaltung der Kennungen und Berechtigungen für Nutzende im Sinne eines individualisierten und sicheren Betriebs von digitalen Schuldiensten. Grundsatz des Systems ist die Datensparsamkeit, es werden nur die Daten erhoben und verarbeitet, die für die Zweckerreichung wirklich erforderlich sind. Nutzerinnen und Nutzer besitzen für alle Dienste nur eine Identität und können sich mit den gleichen Zugangsdaten bei allen bereitgestellten Diensten (Single Sign-On) anmelden.

2. Begründung der Einführung und Gültigkeit dieses Erlasses

Der Betriebserlass ist erforderlich, da mit dem zentralen IDM ein neues Instrument der digitalen Verwaltung von schulischen Identitäten eingeführt wurde. Daher ist es wichtig, dass alle Nutzerinnen und Nutzer die Funktionen des IDM kennen und die zu beachtenden Nutzungsregeln zur Wahrung von Datenschutz und Datensicherheit sowie weiteren wichtigen Anwendungsvorgaben beachten.
Dieser Erlass gilt verbindlich für Beschäftigte und Bedienstete des Ressorts des Ministeriums für Bildung, Kultur und Wissenschaft des Landes Mecklenburg-Vorpommern, welche die personenbezogenen Daten des IDM verwalten, warten, verarbeiten oder weiterleiten. Des Weiteren gilt der Betriebserlass für alle landesseitigen und kommunalen Systeme, die das IDM als Datenquelle für das Schuldienstemanagement und die damit angebundenen Schuldienste zur Erfüllung des Unterrichts- und Erziehungsauftrages, der Schulplanung, der Schulorganisation, sowie der Schulaufsicht nutzen.
Grundlagen dieses Erlasses sind das Schulgesetz für das Land Mecklenburg-Vorpommern (SchulG M-V) sowie die Verordnung zum Umgang mit personenbezogenen Daten der Schülerinnen und Schüler, Erziehungsberechtigten, Lehrkräften und sonstigem Schulpersonal (Schuldatenschutzverordnung - SchulDSVO M-V) in der jeweils geltenden Fassung.

3. Aufbau des Erlasses

Der Erlass gliedert sich in eine Funktionsübersicht, grundlegende Regeln im Umgang mit dem IDM sowie einem dynamischen Teil mit Anlagen mit den auf das IDM bezogenen Konzepten. Bei diesem Erlass handelt es sich um ein der Revision unterstehendes „lebendiges“ Dokument. Dies bedeutet die Möglichkeit der bedarfsgerechten Anpassung bei signifikanten Änderungen im Kontext der Fachanwendung unter der Beteiligung der Mitbestimmungsgremien.

II. Wie funktioniert das IDM?

1. IDM-Funktionen

- Zentrale Bereitstellung einer digitalen Identität von Nutzenden
- Automatische regelbasierte Synchronisation bestimmter Daten von Nutzenden mit dem zentralen Verzeichnisdienst des Bildungsministeriums
- Anbindung des Schulinformations- und Planungssystems M-V (SIP) als zentrale Datenquelle an das IDM
- Kontenverwaltung für Nutzende
- User-Self-Service (Passwörter ändern)
- delegative Administrierung (siehe Rollen- und Rechtekonzept)
- Schnittstellenerweiterungen für die Anbindung weiterer Dienste
- revisionssichere Protokollierung
- Synchronisation digitaler Identitäten aus dem führenden IDM für ein Schuldienstemanagementsystem (SDM)
- Bereitstellung eines Anmeldedienstes und Realisierung einer SSO-Funktion (einmalige Authentifizierung gegenüber einem Server)

2. Zugang zum IDM über das Schulportal M-V

Der Zugang zum IDM erfolgt für die Anwenderinnen und Anwender über das Schulportal https://cloud.schule-mv.de. Mit der Zugangskennung und dem Passwort können alle angeschlossenen Schuldienste genutzt werden. Die aktuellen Kennwortrichtlinien sind der Anlage D zu entnehmen.

3. Authentifizierung über Single Sign-on (SSO)

SSO bedeutet, dass Nutzende nach einer einmaligen Authentifizierung am IDM auf alle Dienste, für die sie berechtigt (autorisiert) sind, vom selben Arbeitsplatz zugreifen können, ohne sich an den einzelnen Diensten jedes Mal zusätzlich anmelden zu müssen. Wechseln die Nutzenden den Arbeitsplatz, wird die Authentifizierung wie auch die lokale Autorisierung hinfällig. Durch diesen Dienst ist sowohl eine gesicherte Authentifizierung aus dem lokalen Schulnetz über Radius-Server als auch eine Authentifizierung aus dem Internet möglich.
Ziel des Single Sign-on ist es, dass sich die Nutzenden der Dienste des ISY M-V nur einmal unter Zuhilfenahme eines einzigen Authentifizierungsverfahrens (Name und Passwort der Nutzenden) identifizieren müssen. Danach übernimmt der SSO-Mechanismus die Aufgabe, die Nutzenden zu authentifizieren (die erkannte Identität zu bestätigen).

Das IDM wird zukünftig Grundlage für die Authentifizierung aller Schuldienste sein. Bei landesseitigen Diensten, die nach Einschätzung des behördlichen DSB oder behördlichen IT-SiBe einen kritischen Funktionsumfang aufweisen sowie den Zugriff auf besonders sensible Inhalte ermöglichen, wird zur Erhöhung des Sicherheitsniveaus für den Zugriff eine seitens des Systems bereitgestellte Zwei-Faktor-Authentifizierung notwendig. Die Authentifizierung über einen zweiten Faktor kann dabei direkt auf IDM-Ebene oder über den entsprechenden Dienst erfolgen.

4. Übersicht datenverarbeitende Stellen und verarbeitete personenbezogene Daten

Um die Aufgaben der Unterrichts- und Schulorganisation erfüllen zu können, ist es für angebundene digitale Systeme erforderlich, auf eine einheitliche, zentral verwaltete Identität zugreifen zu können und aufgabenspezifische Daten zu erhalten. Hierzu werden die entsprechenden Daten vom zentralen SIP M-V, welche im Active Directory gespeichert sind, regelmäßig mit dem IDM synchronisiert.

5. Übertragung von Daten der Nutzenden des Active Directory zum IDM

Die Aufgabe der Schnittstelle ist die Synchronisation der in der nachfolgenden Tabelle aufgezählten Daten zwischen dem Active Directory des BM und dem zentralen Identitätsprovider des BM (IDM-Master). Dabei werden die folgenden Datenkategorien von verschiedenen Nutzenden verarbeitet. Diese Gruppen der Nutzenden sind in § 5a der SchulDSVO M-V in ihrer jeweils aktuell gültigen Fassung festgelegt. Die Verarbeitung der einzelnen Datenkategorien erfolgt nur bei tatsächlicher Erforderlichkeit.

Auflistung verarbeitbarer Daten (Nutzendendaten IDM):

Verarbeitetes Attribut:	**Erklärung**
Anrede	eventuell vorhandener Titel
Vorname	individueller Teil des Namens
Nachname	Familienname
N**ame der/des Nutzenden**	individuelle Anmeldekennung
Passworthash	Hashwert des Passworts
Primäre E-Mail-Adresse	individuelle dienstliche E-Mail-Adresse
Anzeigename	Wert aus Nach- und Vornamen: Mustermann, Max
Straße Stammdienststelle	Straße der Stammdienststelle der Lehrkraft bzw. der Stammschule der Schülerin bzw. des Schülers
PLZ Stammdienststelle	Postleitzahl der Stammdienststelle der Lehrkraft bzw. der Stammschule der Schülerin bzw. des Schülers
Stadt Stammdienststelle	Ort/Stadt der Stammdienststelle der Lehrkraft bzw. der Stammschule der Schülerin bzw. des Schülers
Typ der des Nutzenden	Zuordnung nach standardisierten IDM-Gruppen der Nutzenden (Lehrkräfte, Mitarbeitende, Schülerinnen und Schüler)
Schulzugehörigkeit (Schulkürzel)	Zuordnung zur jeweiligen Schule über spezifisches Kürzel
Klasse (nur Schülerinnen und Schüler)	Zuordnung der nutzenden Person zu einer übergeordneten Gruppe
mvSex	biologisches Geschlecht der nutzenden Person

mvRole[1]	weitere Untergliederung von Typen der Nutzenden zur erweiterten Rollen-Rechtesteuerung der internen Module und angeschlossenen Schuldienste (siehe Gruppen der Nutzenden in Anlage A)
mvStaffType	Zuordnung der Typen von Nutzenden (Lehrkräfte, Mitarbeitende, Schülerinnen und Schüler)
mvDst	schematische und zeitliche Zuordnungen der nutzenden Personen (Schulträger, Dienststelle/Schule, Stammdienststelle, Klasse (Schülerinnen und Schüler), Laufzeit-Beginn, Laufzeit-Ende)
UUID	interne Identifikationsnummer (darf ausschließlich für den technischen Zweck der Sicherstellung der Identifikation der nutzenden Person im Rahmen der Synchronisation verwendet werden)
Kontostatus	Status des Kontos der/des Nutzenden (aktiv oder deaktiviert)
Passwortänderung	Passwortänderung bei der nächsten Anmeldung notwendig

III. Grundlagen des IDM-Betriebs

1. Einführung

Die Zulässigkeitsvoraussetzungen für die Verarbeitung personenbezogener Daten sind in Art. 6 Abs. 1 littera. c) und e), Abs. 2 und 3 Datenschutz-Grundverordnung (DS-GVO) bzgl. der Daten von Schülerinnen und Schülern in Verbindung m. § 70 SchulG M-V sowie bzgl. der Daten von Lehrkräften in § 84 Landesbeamtengesetz M-V (LBG M-V) und § 10 Landesdatenschutzgesetz M-V (DSG M-V), jeweils in Verbindung mit der SchulDSVO M-V geregelt. Die administrative Verarbeitung personenbezogener Daten aus dem IDM hat ausschließlich mit vom Schulträger bzw. Auftragsverarbeiter zur Verfügung gestellten Datenverarbeitungsanlagen zu erfolgen.
Der Betrieb des IDM erfolgt entsprechend §5a SchulDSVO M-V in gemeinsamer Verantwortung gemäß Artikel 26 DS-GVO durch das Ministerium für Bildung, Wissenschaft und Kultur M-V mit den Schulen. Die darin enthaltenen Regelungen für die Umsetzung der Informationspflichten wie sie in den Vereinbarungen zwischen Schule und BM geschlossen sind, gelten als verbindlich. Weitere Informationen finden sich im Datenschutzkonzept (Siehe Anlage B).
Für die Beantwortung von technischen Fragestellungen und zur Lösung von Problemen im Zusammenhang mit der Nutzung des IDM finden sich Hinweise im Supportkonzept (Siehe Anlage C).

2. Nutzungsbedingungen für angeschlossene Schuldienste

Wenn öffentliche Schulen weitere Schuldienste nutzen wollen, so sind folgende Bedingungen für die Nutzung zu beachten und umzusetzen (siehe Checkliste Nutzungsbedingungen in Anlage E):

[1] Eine Erweiterung des Katalogwertes dieses Attributs in Zukunft sowie damit einhergehende Änderungen der Anlage A (Rollen- und Rechtekonzept) sind möglich und erfolgen unter Beteiligung der Mitbestimmungsgremien.

Die Schulleitung ist die Auftraggebende für den Anbietenden (Auftragnehmenden) eines Schuldienstes (Auftragsverarbeitung nach Art. 28 DS-GVO). Dieser Auftrag muss durch die Schule schriftlich erteilt und mit dem Auftragnehmenden in einem Auftragsverarbeitungsvertrag festgehalten werden. Im Vertrag müssen die eingesetzte Hardware, Software und Vernetzung konkret benannt sowie die bereits durch den Anbieter getroffenen technischen und organisatorischen Datenschutzmaßnahmen genau dargestellt werden. Ferner ist zu beachten, dass der Vertrag keine Formulierung enthalten darf, die es dem Auftragsverarbeiter ermöglicht, die Allgemeinen Geschäftsbedingungen bzw. andere Vertragsbestandteile einseitig zu ändern. Der Vertrag muss eine abschließende und vollständige Auflistung aller Stellen, Personen oder Firmen (Unterauftragsverarbeitende) enthalten, an die personenbezogenen Daten übermittelt werden. Bei späterer Unterauftragsverarbeitung muss eine Genehmigung des Auftraggebenden eingeholt werden. Die Schulleitung muss sich außerdem von den vom Auftragnehmenden getroffenen technischen und organisatorischen Maßnahmen überzeugen. Dabei hat sie sich durch ihre Datenschutzbeauftragten bei der Überprüfung der ordnungsgemäßen Verarbeitung der personenbezogenen Daten beraten zu lassen. Zudem müssen regelmäßig aktuelle und aussagekräftige Nachweise, beispielsweise Zertifikate von anerkannten und unabhängigen Prüfungsorganisationen, herangezogen werden. Im Vertrag muss der Auftragnehmende zudem zur Vertraulichkeit verpflichtet werden und seine Unterstützungspflicht bei der Umsetzung der Betroffenenrechte durch die Schulleitung vereinbart sein. Ferner muss die Lösch- oder Rückgabepflicht der Daten nach Abschluss der Verarbeitung vereinbart sein. Die Schulleitung muss sich auch Betretungs- und Kontrollrechte vertraglich zusichern lassen.

Erbringt ein Schulträger gegenüber einer Schule Leistungen im Rahmen der digitalen Schuldienste oder des Schuldienstemanagementsystems, so handelt der Schulträger im Auftrag der Schule (Auftragsverarbeitung nach Art. 28 DS-GVO). Die Schulträger dürfen die personenbezogenen Daten aus dem IDM nicht zu eigenen Zwecken verarbeiten.

3. Sicherheitsvorschriften für technisch Verantwortliche des IDM und daran angeschlossener Dienste

Hinweis: Die nachfolgenden Sicherheitsvorschriften richten sich an technisch verantwortliche IT-Fachkräfte des Landes, eines Schulträgers oder von diesem Beauftragte. Allgemeine Sicherheitshinweise zur Nutzung des IDM und das daran angeschlossene Schulportal M-V sind für Lehrkräfte und sonstiges Schulpersonal als Anlage F angefügt.

Betrieb des IDM-Kernsystems und daran angeschlossener Module

Das IDM sowie daran angeschlossene Module müssen konform zu den aktuellen operativen Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entsprechen. Der Betrieb hat konform zum BSI IT-Grundschutz und dem dazugehörigen BSI IT-Grundschutz Kompendium, insbesondere zu den Bausteinen CON.5 Entwicklung und Einsatz von Allgemeinen Anwendungen und CON.8 Software-Entwicklung zu erfolgen.
Sollte eine gültige Zertifizierung nach „ISO 27001 auf Basis IT-Grundschutz“ oder nach „ISO 27001“ für den Geltungsbereich der Anwendung vorliegen, sind die entsprechenden Nachweise dem Ministerium für Bildung, Wissenschaft und Kultur bereitzustellen.
Es müssen für das IDM sowie daran angeschlossene Module jeweils aktuelle Schutzbedarfsfeststellungen und daraus abgeleitete Sicherheitskonzepte für die personenbezogenen Daten, die verarbeitet werden sollen, vorhanden sein und auf Verlangen dem Ministerium für Bildung, Kultur und Wissenschaft zur Prüfung vorgelegt werden. Diese dienen als Grundlage für die umzusetzenden Sicherheitsanforderungen (vgl. BSI-Standard 200-2).
Sollte keine Zertifizierung vorliegen, sind folgende Anforderungen als Grundvorrausetzung für den Betrieb anzunehmen:

ISMS.1.A4: Eine Ansprechperson in Fragen der IT-Sicherheit ist zu benennen

Hinweis: Um auch in Bedrohungsfällen schnell und effektiv reagieren zu können, ist es zwingend notwendig, dass eine aktuelle Ansprechperson für den IT-Betrieb bzw. IT-Sicherheit benannt ist. Sollte sich diese ändern, ist dies umgehend dem Ministerium für Bildung, Wissenschaft und Kultur M-V mitzuteilen.

ISMS.1.A10: Es ist ein Sicherheitskonzept für ein an das IDM angeschlossenes Modul durch den jeweiligen Auftragnehmenden bzw. dafür Verantwortlichen bereit zu stellen.

Hinweis: Das Sicherheitskonzept dient als Grundlage eines ganzheitlichen Risikomanagements und ist daher verpflichtend. Es beinhaltet auch die Schutzbedarfsfeststellung der jeweiligen Anwendung.

Die folgenden Anforderungen sind Teil des Sicherheitskonzeptes und sollen als Orientierungshilfe bei dessen Erstellung und Pflege, sowie als Maßgabe für den operativen Betrieb dienen.

APP.3.1 und APP.3.2: Webanwendungen und Webserver.

Hinweis: Das Hosting der Server und aller Daten, insbesondere personenbezogener Daten, ist im Geltungsbereich der DS-GVO (europäischer Wirtschaftsraum) vorzunehmen. Auch bei der Entwicklung von Client-Applikationen, die nicht Webanwendungen darstellen, ist die Kommunikation sicher zu verschlüsseln (CON.1.A3 und APP.1.2.A2). Wenn ein webbasiertes Modul an das IDM angebunden werden soll, ergeben sich die technischen Sicherheitsanforderungen insbesondere aus dem System-Baustein „APP.3.2 Webanwendungen“ des o.g. IT-Grundschutz Kompendiums. Dieser muss vom jeweiligen Auftragnehmenden bzw. dafür Verantwortlichen

bei der Entwicklung umgesetzt werden. Wird ein webbasiertes Modul an das IDM angebunden, so muss es den datenschutzrechtlichen Anforderungen der DS-GVO, des SchulG M-V, der SchulDSVO M-V, des DSG M-V sowie dem Telemediengesetz entsprechen. Ein entsprechendes Datenschutzkonzept ist dem Ressort des Ministeriums für Bildung, Kultur und Wissenschaft auf Verlangen vorzulegen. Beim IDM sowie daran angebundenen Modulen muss sichergestellt werden, dass die Sicherheit von Informationen nach dem Stand der Technik in und beim Austausch zwischen Webanwendungen/Webservices und der anwendenden Person gewährleistet ist. Die Systeme müssen als Mindeststandard eine Transportverschlüsselung zwischen Webserver und Webbrowser der nutzenden Person mittels eine vom BSI empfohlenen Version von TLS besitzen bzw. ist die Transportverschlüsselung so zu wählen, dass der Stand der Technik gewährleistet wird (siehe CON.1.A3). Nutzende müssen von dem Modul sicher authentifiziert werden. Das System muss fehlerhafte Authentisierungsversuche protokollieren. Wiederholte fehlerhafte Authentifizierungsversuche müssen zu einer Sperrung führen. Dies betrifft sowohl Zugriffe von Nutzenden als auch von administrierenden Personen. Jeweils Verantwortliche oder Auftragnehmende haben ein Konzept zur abgestuften revisionssicheren Protokollierung von Eingaben nutzender Personen im Rahmen des Datenschutzkonzepts vorzulegen. Wird zu anderen Modulen oder Webseiten per Webservice kommuniziert, muss als Mindeststandard ebenso eine aktuelle Transportverschlüsselung realisiert sein, die dem Stand der Technik entspricht.

OPS.1.1.4 Schutz vor Schadprogrammen

Hinweis: Ein Virenschutz ist für alle in das angebundene System geladenen Inhalte sicherzustellen. Die Virensignaturen müssen so aktualisiert werden, dass ein aktueller Virenschutz jederzeit gegeben ist.

OPS.2.2 Cloud-Nutzung

Hinweis: Wird ein an das IDM angeschlossenes System in einer Cloud-Plattform betrieben, muss eine Trennung der darin betriebenen Systeme und gespeicherten Daten gemäß deren Schutzbedürfnissen erfolgen. Der Cloudanbieter muss nach ISO 27001 oder nach BSI ISO 27001 auf Basis IT-Grundschutz zertifiziert sein und sich im europäischen Wirtschaftsraum befinden. Des Weiteren sollten die ISO/IEC 27017 (Code of practice for information security controls for cloud computing services) und ISO/IEC 27018 (Code of practice for controls to protect personally identifiable information processed in public cloud computing services) als Grundlage des Betriebes dienen.

Sollten Eigenentwicklungen zum Einsatz kommen, dann sind folgende Anforderungen zwingend zu berücksichtigen:

CON.5 – Entwicklung und Einsatz von Individualsoftware

Hinweis: Individualsoftware, die nicht über Standardsoftware abgedeckt werden kann, sind dedizierte Anforderungen vorgegeben.

CON.8 – Software-Entwicklung

Hinweis: Zur sicheren Umsetzung von Applikationen ist die IT-Sicherheit frühzeitig mit zu planen. Dies wird auch als „Security by Design“ bezeichnet. Eine geeignete und sichere Entwicklungsumgebung, Bibliotheken aus vertrauenswürdigen Quellen sowie ein sicheres Systemdesign sind anzuwenden.

OPS.1.1.6 – Software-Tests und –Freigaben

Hinweis: Vor dem Produktivbetrieb und der Anbindung sind die Anwendungen zu testen. Eine strikte Trennung von Testsystemen mit realistischen Testdaten und dem Produktivsystem sind umzusetzen. Testdaten haben mit anonymisierten und fiktiven personenbezogenen Datensätzen zu erfolgen. Sind reale personenbezogene Daten für Tests notwendig, ist dies mit dem verantwortlichen Datenschutzbeauftragten abzustimmen.

Darüber hinaus sind je nach Anwendungsszenario eigenständig weitere Anforderungen aus dem BSI IT-Grundschutz Kompendium zu bestimmen.

4. Nutzende Personen und deren Berechtigungen

Anhand von Rollen definiert das Ministerium für Bildung, Wissenschaft und Kultur M-V bestimmte Rechte für landeseigene Schuldienste vor. Durch das Schuldienstemanagementsystem auf kommunaler Ebene werden die Konten von Nutzenden darüber hinaus mit Rechten für weitere Schuldienste der Schulträger bzw. Schulen angereichert. Rechte werden automatisiert anhand der jeweils zugeordneten Rolle übertragen. Nutzende im Sinne dieses Erlasses sind im IDM-Rollen- und Rechtekonzept (siehe Anlage A) beschrieben.
Nutzende eines SDM und daran angeschlossener Schuldienste müssen in einem eigenen Rollen- und Rechtekonzept beschrieben werden.

Schwerin, 18.05.2021

Im Auftrag

Thomas Jackl

IV. Anlagen

Anlage A IDM-Rollen- und Rechtekonzept

Der Datenzugriff der jeweiligen Rolle erfolgt auf Grundlage der DS-GVO, des, des DSG M-V, des §70 SchulG M-V sowie §5 SchulDSVO M-V in der jeweils gültigen Fassung.

Rollen Univention

Administrationsrollen

Rollen/Rechte	Globale administrierende Personen systemadministrierende Person (BM)	administrierende Personen Schulträger /IT-Dienstleister SDM	IDM-Verantwortliche der Schule[2]
Zugriff auf Nutzendenkreis der administrierende Personen des Schulträger	X		
Zugriff auf Nutzendenkreis der IDM-Verantwortlichen der Schule	X	X	
Zugriff auf Nutzendenkreis der Lehrkräfte	X	X	
Zugriff auf Nutzendenkreis der Schülerinnen und Schüler	X	X	X
Zugriff auf Nutzendenkreis der BM-Mitarbeitenden	X		
Zugriff auf Nutzendenkreis der kommunalen Mitarbeitenden	X	X	X
Rechte	Administration der Nutzenden, zentrale Konfiguration und Verwaltung IDM, Administration Schnittstellen der führenden Quellsysteme, Administration Landesdienste, Administration Schulportal	Administration der Nutzenden, zentrale Konfiguration und Verwaltung SDM des Schulträgers, Administration Schuldienste, Administration Schulportal kommunaler Part	Optionales Zurücksetzen der Passwörter von Schülerinnen und Schüler der eigenen Schule

[2] Die Schulleitung hat optional die Möglichkeit, Lehrkräfte als IDM-Verantwortliche an der Schule zu benennen. Diese verfügen über die Berechtigung nach Bedarf für Schülerinnen und Schüler die Passwortrücksetzung und Neuvergabe vorzunehmen. Näheres dazu regelt eine entsprechende Verpflichtungserklärung.

Rollen nutzender Personen

Rollen/Rechte	Lehrkraft	Schülerinnen und Schüler	Mitarbeitende des Ressorts des Bildungsministeriums	kommunale Mitarbeitende
Gruppen nutzender Personen	**Schulleitung stellv. Schulleitung, Koordinatorinnen und Koordinatoren, IT-Beauftragte/schulische Medienbildungsbeauftragte, Lehrkräfte/Referendarinnen und Referendare, unterstützende pädagogische Fachkräfte (upF)**	**Schülerinnen und Schüler**	**Mitarbeitende des Bildungsministeriums und nachgelagerter Behörden**	**Integrationshelferinnen und Integrationshelfer, verwaltendes Personal, haustechnisches Personal**
Dienst SSO	X	X	X	X
Dienst Self Service - Password Reset	X	X	X	X
Landeseigene Schuldienste	X	X	X	X
Kommunale Schuldienste	X	X		X
Zugriff Schulportal https://cloud.schule-mv.de	X	X	X	X

Datenbereiche

Die mit den Rollen verbundenen Rechte gelten immer für die zugehörige Schule bzw. Dienststelle. Eine Ausnahme bilden dabei die globalen Administratoren, deren Rechte datenbereichübergreifend bzw. schulübergreifend gelten. Für nicht landeseigene digitale Schuldienste muss der Anbieter bzw. der verantwortliche Träger oder die Schule ein eigenes Rollen- und Rechtekonzept erstellen und vorhalten.

Anlage B Datenschutzkonzept für das IDM

Präambel	Das IDM ermöglicht es Lehrkräften, Schülerinnen und Schüler und sonstigen schulischen Mitarbeitenden sich bei bereitgestellten Schuldiensten zum Zweck der Erfüllung des Bildungs- und Erziehungsauftrages, der Schulplanung, der Schulorganisation, sowie der Schulaufsicht mit einheitlichen Daten von Nutzenden anzumelden. Diese zentrale Datenbereitstellung stellt hohe Anforderungen an die Datensicherheit sowie den Schutz der personenbezogenen Daten. Daher zielt dieses Konzept darauf ab, die wichtigsten Ziele, Informationen und ergriffenen Maßnahmen zur Gewährleistung des Schutzes der personenbezogenen Daten von Lehrkräften, Schülerinnen und Schüler und sonstigen schulischen Mitarbeitenden übersichtlich und transparent darzustellen. Es kann auch als Grundlage für datenschutzrechtliche Prüfungen genutzt werden. Dadurch soll die Einhaltung der europäischen Datenschutz-Grundverordnung (DS-GVO) nicht nur gewährleistet, sondern auch der Nachweis der Einhaltung geschaffen werden. Das Datenschutzkonzept ist kein statisches Dokument, sondern kann an sich verändernde Bedingungen angepasst werden.
Rechtliche Rahmenbedingungen des Datenschutzes beim IDM	§ 70 SchulG M-V – Umgang mit personenbezogenen Daten: Verarbeitung personenbezogener Daten zur Erfüllung des Unterrichts- und Erziehungsauftrages, der Schulplanung, der Schulorganisation, sowie der Schulaufsicht § 5a SchulDSVO M-V: Verarbeitung von personenbezogenen Daten für die Bereitstellung von digitalen Schuldiensten und Lern- und Lehrinhalten DS-GVO: • Allgemeine Rechenschaftspflichten nach Art. 5 (2) • Weisungsbindung des Auftragsverarbeiters nach Art. 28 • Dokumentation der technischen und organisatorischen Maßnahmen (TOM) nach Art. 24 bei der jeweiligen nutzenden Person des IDM • Erstellung und Führen eines Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 jeweils vom Verantwortlichen und dem Auftragnehmenden • Rechte der Betroffenen nach Art 12 ff. • gemeinsame Verarbeitung der Daten durch Schulen oder Schulträger und BM nach Art. 26

Datenschutzziele	Das Ministerium für Bildung, Kultur und Wissenschaft hat für seine Mitarbeitenden sowie Schülerinnen und Schüler aber auch für Auftragsverarbeitende sowie weitere Empfängerinnen und Empfänger personenbezogener Daten klare Datenschutzziele festgelegt, die sich an den Datenschutzgrundsätzen nach Art.5 DS-GVO orientieren. Wichtig ist es dabei, die Verarbeitung dieser Daten transparent zu gestalten. Dazu gehört die genaue Auflistung der Betroffenen, des Umfangs und der Art der gespeicherten und verarbeiteten Daten, deren Herkunft sowie die Art der Verarbeitung und die mögliche Weiterleitung an Dritte. Aus personenbezogenen Logdaten werden keine Nutzerprofile angelegt. Anfallende Protokolldaten werden anonymisiert für den statistischen Zweck abgeleitet. Das Ministerium für Bildung, Kultur und Wissenschaft stellt den Betroffenen deren Daten es verarbeitet, Möglichkeiten zur Verfügung diese Daten vollständig einzusehen, sie ggf. zu korrigieren sowie Auskunft über die Verarbeitung zu verlangen und zu erhalten. Die obersten Ziele dieses Datenschutzkonzeptes sind: - die Beschränkung der verarbeiteten personenbezogenen oder personenbeziehbaren Daten auf das benötigte Minimum orientiert an den oben genannten Rechtsgrundlagen. Dies erfolgt durch die Beschreibung der personenbezogenen Daten und Angabe der jeweiligen Zweckbindung (Nutzungszweck) - die klare Festlegung der Rollen und damit verbundenen Zugriffsrechte sowie Verantwortlichkeiten - die Sicherstellung eines hohen Datenschutzniveaus bei allen an der Verarbeitung der Daten beteiligten Parteien - die Wahrung der Rechte der Betroffenen - der Aufbau und die kontinuierliche Verbesserung eines Datenschutzmanagements - die nachweisbare Schulung, Sensibilisierung und Verpflichtung der Mitarbeitenden

Verantwortliche	Verantwortlichkeit für Datenschutz: Ministerin Frau Bettina Martin Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern 19048 Schwerin Datenschutzbeauftragter Herr Michael Tiedke E-Mail: M.Tiedke@bm.mv-regierung.de Telefon: 0385 588-7676 IT-Sicherheitsbeauftragter: Herr Dr. Jan Skodzik E-Mail: J.Skodzik@bm.mv-regierung.de Telefon: 0385 588-7012 Technische Zuständigkeit für den Datenschutz des IDM: Integriertes Schulmanagementsystem M-V Herr Sven Korff E-Mail: S.Korff@bm.mv-regierung.de Telefon: 0385 588-7260
Einbindung der Angestellten und Bediensteten	Die Einbindung erfolgt über: 1. Unterrichtung und Beratung der Verantwortlichen oder der Auftragsverarbeitenden sowie der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten, die sich aus dem Datenschutzrecht (DS-GVO sowie allgemeine und bereichsspezifische nationale Datenschutzregelungen) ergeben durch die jeweils zuständigen Datenschutzbeauftragten. 2. Überwachung und Überprüfung der Einhaltung der DS-GVO und nationaler Datenschutzvorschriften im Zusammenhang von Auftragsdatenverarbeitungen sowie der Strategien der Verantwortlichen oder der Auftragsverarbeitenden für den Schutz personenbezogener Daten. Hierzu gehört auch die Zuweisung von Zuständigkeiten, die Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiterinnen und Mitarbeiter und diesbezügliche Überprüfungen durch die jeweils zuständigen Dienstvorgesetzten in Zusammenarbeit mit den Datenschutzbeauftragten. 3. Die mit der Verarbeitung personenbezogenen Daten beauftragten Mitarbeiterinnen und Mitarbeiter und Bediensteten sind zur Einhaltung der datenschutzrechtlichen Anforderungen nach der DS-GVO zu verpflichten. 4. Die Lehrkräfte sowie die unterstützenden pädagogischen Fachkräfte (upF) erhalten durch die Schulleitung einmal jährlich eine Datenschutzunterweisung. Sie werden außerdem bei der Umsetzung des Datenschutzes in den Schulen durch die zuständigen Datenschutzbeauftragten beraten.

<table>
<tr><td>Gestaltung kontinuierlicher Verbesserungsprozesse</td><td>Folgende Bereiche werden regelmäßig durch die Verantwortlichen gemäß Art. 24 sowie Art. 25 und 32 DS-GVO überprüft:
- Feststellung der aktuellen Anforderungen betreffend die personenbezogenen Daten und Abgleich mit den festgelegten Verfahren und Prozessen
- Feststellung, ob festgelegte Maßnahmen und Verfahren ausreichend definiert, dokumentiert bzw. auch eingehalten werden
- Gewährleistung der Einhaltung von folgenden Kriterien:
o Verfügbarkeit der personenbezogenen Daten
o Vertraulichkeit der personenbezogenen Daten
o (Daten)-Integrität der personenbezogenen Daten
o Fristgemäßes Löschen der personenbezogenen Daten
- Berücksichtigung und Anpassung der Verarbeitung an aktualisierte Rechtsprechung und technische Entwicklung
Darüberhinausgehend sind weitere Maßnahmen im vertraulichen IT-Sicherheitskonzept aufgeführt, welches basierend auf dem Schutzbedarf der Informationen Anforderungen nach BSI IT-Grundschutz definiert.</td></tr>
<tr><td>Bestehende technische und organisatorische Maßnahmen</td><td>Die Listung der TOMs ist in der nichtöffentlichen Anlage „Technische und organisatorische Maßnahmen (TOM) bei der Verarbeitung personenbezogener Daten des Ministeriums für Bildung, Wissenschaft und Kultur M-V“ zu finden. Die Einsichtnahme kann beim zuständigen IT-Sicherheitsbeauftragten beantragt werden.</td></tr>
<tr><td>Beschreibung der personenbezogenen Daten mit Verwendungszweck und Löschfristen</td><td>Die personenbezogenen Daten und Gruppen von Nutzenden, die durch das IDM verarbeitet werden, sind in §5a (5) SchulDSVO M-V (in der jeweils gültigen Fassung) konkretisiert.

Speicherort für alle Daten ist das LDAP-Verzeichnis des USC@School als Teil des IDM.

Die Aktualisierung und somit auch die Löschung von Daten, die der Verarbeiter nicht mehr für den angegebenen Verwendungszweck benötigt, erfolgt über die tägliche Synchronisation zwischen dem IDM und SIP. Die Daten der Nutzenden haben einen Gültigkeitszeitraum. Dieser beschreibt, in welchem Zeitraum sie einer bestimmten Schule zugeordnet sind. Die Daten des IDM werden täglich mit der Datenquelle (SIP) synchronisiert.

Der Verwendungszweck der Daten im IDM erlischt, wenn eines der folgenden, oder damit vergleichbaren, Szenarien eintreten:

<table>
<tr><th></th><th>Lehrkraft/ mitarbeitende Person des BM/kommunale Mitarbeitende</th><th>Schülerin bzw. Schüler</th><th>Sonstige</th></tr>
</table>
</td></tr>
</table>

Beispiel1	Der Zuweisung einer Lehrkraft für eine Schule, die Daten aus dem IDM bezieht, endet.	Schülerin bzw. Schüler wechselt in eine Schule, die nicht die Dienste des IDM nutzt.	Das (kommunale) Personal verlässt die Schule und/oder bekommt ein nichtschulisches Aufgabenfeld zugewiesen.
Beispiel 2	Das Beschäftigungsverhältnis endet	Schülerin bzw. Schüler beendet Schullaufbahn	Das Beschäftigungsverhältnis endet

Name	**Verwendungszweck**	**Löschfrist**
Anrede	Erfüllung des Unterrichtsauftrages	24h nach Beendigung des Verwendungszweckes
Vorname	Erfüllung des Unterrichtsauftrages	24h nach Beendigung des Verwendungszweckes
Nachname	Erfüllung des Unterrichtsauftrages	24h nach Beendigung des Verwendungszweckes
Name des Nutzenden	Erfüllung des Unterrichtsauftrages	24h nach Beendigung des Verwendungszweckes
Passworthash	Erfüllung des Unterrichtsauftrages	24h nach Beendigung des Verwendungszweckes
Primäre E-Mail-Adresse	Erfüllung des Unterrichtsauftrages	24h nach Beendigung des Verwendungszweckes
Anzeigename	Erfüllung des Unterrichtsauftrages	24h nach Beendigung des Verwendungszweckes
Straße Stammdienststelle	Erfüllung des Unterrichtsauftrages	24h nach Beendigung des Verwendungszweckes
PLZ Stammdienststelle	Erfüllung des Unterrichtsauftrages	24h nach Beendigung des Verwendungszweckes
Stadt Stammdienststelle	Erfüllung des Unterrichtsauftrages	24h nach Beendigung des Verwendungszweckes
Typ des Nutzenden	Erfüllung des Unterrichtsauftrages	24h nach Beendigung des Verwendungszweckes
Schulzugehörigkeit (Schulkürzel)	Schulorganisation	24h nach Beendigung des Verwendungszweckes

	Klasse (nur Schülerinnen und Schüler)	Schulorganisation	24h nach Beendigung des Verwendungszweckes
	mvSex	Erfüllung des Unterrichtsauftrages	24h nach Beendigung des Verwendungszweckes
	mvRole	Schulorganisation	24h nach Beendigung des Verwendungszweckes
	mvStaffType	Schulorganisation	24h nach Beendigung des Verwendungszweckes
	mvDst	Schulorganisation	24h nach Beendigung des Verwendungszweckes
	UUID	Schulorganisation	24h nach Beendigung des Verwendungszweckes
	Personenbezogene Protokolldaten	Systemüberwachung	24h nach Erfassung
Dokumentation	Die weiterführende Dokumentation getroffener Maßnahmen für den Schutz und die Sicherheit der personenbezogenen Daten findet sich im Betriebserlass sowie den dort beigefügten sonstigen Anlagen.		

Anlage C Supportkonzept

Aufbau	Servicezeiten	Tickettracking/Weiterleitung	Kontaktdetails
1st Level Support			
Service-Desk M-V	Mo-Fr: 7-16 Uhr	Top-Desk	Telefon: Schulen, die durch die IKT-Ost betreut werden: +49 395 3517 30 30 Schulen, die durch den KSM betreut werden: +49 385 633 3030 Schulen, die durch die HRO betreut werden: +49 381 381 3030 Schulen, die durch sonstige Dienstleister betreut werden: +49 395 3517 30 30 E-Mail-Adresse: support@servicedesk-mv.de
2nd Level Support			
UHD	Mo-Do: 7-17 Uhr Fr: 7-15 Uhr	Weiterleitung an das Ticketsystem Helpline des User-Help-Desk (UHD) des Bildungsministeriums	E-Mail: servicedesk@kultus-mv.de Portal: https://servicedesk.kultus-mv.de
ISY M-V	Mo-Do: 7-17 Uhr Fr: 7-15 Uhr	Weiterleitung der Tickets innerhalb des Ticketsystem Helpline bei fachlichen Themen durch den UHD an das Projektteam ISY M-V	E-Mail-Adresse: isy@schule-mv.de
3rd Level Support			
Univention GmbH	Mo-Fr: 9-17 Uhr	Bearbeitung der Anfragen des 2nd Level Support und Rückmeldung bei Problemlösung oder Abstimmungsbedarf an den 2nd Level Support	Supportformular: https://www.univention.de/produkte/support/support-kontaktieren/supportformular/ Telefon: +49 421 222 32 40 E-Mail: support@univention.de
DVZ GmbH	Mo-Do: 7-17 Uhr Fr: 7-15 Uhr	Bearbeitung der Anfragen des 2nd Level Support und Rückmeldung bei Problemlösung oder Abstimmungsbedarf an den 2nd Level Support	Ticketsystem des Bildungsministeriums M-V

IT-Bereich des Bildungsministeriums	Mo-Do: 7-17 Uhr Fr: 7-15 Uhr	Bearbeitung der Anfragen des 2nd Level Support und Rückmeldung bei Problemlösung oder Abstimmungsbedarf an den 2nd Level Support	E-Mail: it-service@bm.mv-regierung.de Telefon: +49 385 588-7555

1. Meldung an den 1st Level Support:

- Schülerinnen und Schüler bzw. Sorgeberechtigte wenden sich an ihre Lehrkräfte
- Lehrkräfte und an Schule tätiges Personal wenden sich an die IDM-Verantwortlichen an Schule
- IDM-Verantwortliche streben eigenständige Lösung bei einfachen Problemen an
- falls keine Lösung durch die IDM-Verantwortlichen möglich ist, wenden sie sich an den 1st Level Support
- dadurch wird eine Bündelung der Anfragen sowie eine qualifizierte Meldung beim 1st Level Support sichergestellt
- das Ticket wird beim 1st Level Support aufgenommen

2. Aufgaben des 1st Level Support:

- erste Anlaufstelle für alle eingehenden Unterstützungsanfragen zum Schulportal
- Irrtümlich eingegangene Anfragen zur Schul-IT werden an die Aufgabenträger Schul-IT weitergeleitet. Bei Schulen, die von keinem kommunalen Dienstleister betreut werden, wird auf die Zuständigkeit des Schulträgers verwiesen.
- vollständige Erfassung (Registrierung und Einordnung) der Anfragen, inklusive aller erforderlichen Zusatzinformationen
- Bearbeitung der Anfragen und unmittelbarer Lösungsversuch unter Zuhilfenahme der Wissensdatenbank
- falls keine schnelle Sofortlösung möglich ist, erfolgt umgehend eine strukturierte Weitergabe der Anfrage inklusive Vorklärung/Fehlerbild an den 2nd Level-Support

3. Vorqualifizierung Tickets im 1st Level

Zur Annahme und Weiterleitung von Anfragen werden folgenden Angaben abgefragt:

- Name der meldenden Person
- Vorname meldende Person
- Name der Schule
- Schulart
- Emailadresse
- Rückrufnummer der meldenden Person, bei der Problem auftrat bzw. die es gemeldet hat
- Problemschilderung

4. Weitergabe an 2nd Level Support

- Weitergabe an den 2nd Level Support des Bildungsministeriums sowie die Fertigmeldung an den 1st-Level Support erfolgt via E-Mail aus den einzelnen Helpdesk-Tools
- Die Weitergabe an das ISY M-V-Team erfolgt via E-Mail, die Rückmeldung über Lösung erfolgt per E-Mail

5. Aufgaben des 2nd Level Support:

- Bearbeitung der der Anfragen vom 1st Level Support
- Bearbeitung globaler Fehlermeldungen im Portal (Anmeldung, Anzeige)
- Bearbeitung der Anfragen zum Datenbestand
- Zuordnung von Rechten
- Bearbeitung der Anfragen zum Anmeldeprozess
- Rückmeldung an den 1st Level Support
- Bei Bedarf Weiterleitung an den 3rd Level Support

6. Aufgaben des 3rd Level Support:

- Administration und Weiterentwicklung der Dienste, sowie Betreuung der IT-Systeme und IT-Infrastruktur
- Rückmeldung an den 2nd Level Support bei Problemlösung

7. Test-User für den 1st und 2nd Level Support

Das Bildungsministerium stellt dem 1st Level Support Testnutzende zur Verfügung, um in Supportfällen den Nutzenden Schritt für Schritt begleiten zu können. Die Testnutzenden erhalten Zugriff im produktiven System auf eine Testdienststelle.

Um den Anforderungen der IT-Sicherheit und des Datenschutzes zu genügen, wird protokolliert, wann welche testnutzenden Personen durch welche Mitarbeitende eingesetzt wurden. Sollten Schadensfälle auftreten (Missbrauch, Manipulation etc.) werden die Protokolle zur Analyse genutzt.

a. Zuordnung der Rollen zu Nutzenden:

Supportlevel	Erforderliche Rollen	Mitarbeitende
1st Level	Lehrkraft	Team
1st Level	IDM-Verantwortliche Person (Lehrkraft mit erweiterten Rechten)	Team
1st Level	Schülerin bzw. Schüler	Team

b. Übermittlung Kennwörter

Die Übermittlung der Kennwörter erfolgt verschlüsselt.

Anlage D Kennwortrichtlinien

Richtlinie	**Einstellung**
Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert
Kennwortchronik erzwingen\gespeicherte Kennwörter	1 gespeichertes Kennwort
Minimale Kennwortlänge	10 Zeichen
Maximales Kennwortalter	365 Tage

Die Komplexitätsvoraussetzungen beinhalten folgendes:

Das Kennwort enthält Zeichen aus drei der folgenden Kategorien:

- Großbuchstaben europäischer Sprachen (A bis Z, mit diakritischen Zeichen, griechischen und kyrillischen Zeichen)
- Kleinbuchstaben europäischer Sprachen (a bis z, Sharp-s, mit diakritischen Zeichen, griechischen und kyrillischen Zeichen)
- Basis 10 Ziffern (0 bis 9)
- Nicht alphanumerische Zeichen (Sonderzeichen): (~! @ # $% ^& : -+ = ' | \ \ *(){}\ []:; "' <>,.? /) Währungssymbole wie Euro oder britisches Pfund werden nicht als Sonderzeichen für diese Richtlinieneinstellung gezählt.*
- Ein beliebiges Unicode-Zeichen, das als alphabetisches Zeichen kategorisiert ist, aber kein Groß- oder Kleinbuchstabe ist. Dazu gehören Unicode-Zeichen aus asiatischen Sprachen.

Anlage E Checkliste Nutzungsbedingungen für Schulleitungen (datenschutzrechtliche Verantwortliche)

1. Wurde ein gemeinsamer schriftlicher Auftragsverarbeitungsvertrag (Auftragsverarbeitung nach Art. 28 DS-GVO) zwischen Auftraggebenden (Schulleitung) und Auftragnehmenden (Dienstanbietenden) vereinbart und unterschrieben? ☐
2. Wurde in diesem Vertrag die eingesetzte Hardware, Software und Vernetzung konkret benannt? ☐
3. Wurden in diesem Vertrag die durch den Auftragnehmenden getroffenen technischen und organisatorischen Datenschutzmaßnahmen genau dargestellt? ☐
4. Enthält der Vertrag keine Formulierung, die es dem Auftragnehmenden ermöglicht, die AGB bzw. andere Vertragsbestandteile einseitig zu ändern? ☐
5. Wurde der Auftragnehmende im Vertrag zudem zur Vertraulichkeit verpflichtet? ☐
6. Ist die Unterstützungspflicht des Auftragnehmenden bei der Umsetzung der Betroffenenrechte durch die Schulleitung vereinbart worden? ☐
7. Ist Lösch- oder Rückgabepflicht des Auftragnehmenden für die personenbezogenen Daten nach Anschluss der Verarbeitung vereinbart worden? ☐
8. Hat sich der Auftraggebende Betretungs- und Kontrollrechte vertraglich versichert? ☐
9. Enthält der Vertrag eine abschließende und vollständige Auflistung aller Stellen, Personen oder Firmen (Unterauftragsverarbeitende),
   an die personenbezogenen Daten übermittelt werden? ☐
10. Nur bei späterer Unterauftragsverarbeitung: Hat der Auftragnehmende dafür eine Genehmigung des Auftraggebenden eingeholt? ☐
11. Hat sich der Auftraggebende von der Umsetzung der vom Auftragnehmende getroffenen technischen und organisatorischen Maßnahmen überzeugt? ☐
12. Wurde dabei und insbesondere auch bei der Überprüfung der ordnungsgemäßen Verarbeitung der personenbezogenen Daten die Unterstützung der für die jeweilige Schule zuständigen Datenschutzbeauftragten in Anspruch genommen? ☐
13. Wurden bei der regelmäßig durchzuführenden Prüfung des Auftragnehmenden durch den Auftraggebenden aktuelle und aussagekräftige Nachweise, beispielsweise Zertifikate von anerkannten und unabhängigen Prüfungsorganisationen, herangezogen? ☐
14. Ist die administrative Verarbeitung personenbezogener Daten auf Datenverarbeitungsanlagen des Schulträgers bzw. Auftragnehmenden beschränkt? ☐
15. Hat der Auftragnehmende ein entsprechendes Datenschutz- und Datensicherheitskonzept erstellt und vorgelegt? ☐
16. Hat der Auftragnehmende für den Schuldienst ein eigenes Sicherheitskonzept vorgelegt bzw. ist dieses entsprechend den Vorgaben erstellt? ☐
17. Liegt für den Schuldienst ein eigenes Rollen- und Rechtekonzept vor? ☐

Anlage F Sicherheitshinweise für die Gruppe nutzender Lehrkräfte und unterstützende pädagogische Fachkräfte beim Umgang mit an das IDM angeschlossenen Schuldiensten

Die nachfolgenden Sicherheitshinweise basieren auf Umsetzungsempfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der Allianz für Cyber-Sicherheit.

Wir wollen Sie bei der Erfüllung der Anforderungen an die Informationssicherheit und Vorgaben des Datenschutzes bei der Nutzung des IDM und den daran angeschlossenen Schuldiensten unterstützen. Die wesentliche Strategie, die dabei genutzt wird, ist das so genannte Erforderlichkeitsprinzip. Im Wesentlichen haben Sie restriktiv zu bewerten, ob Sie eine Information wirklich wissen bzw. weitergeben müssen. Nachfolgend finden Sie auf Basis dieser Strategie organisatorische und technische Maßnahmen, die in Ihrem Alltag zu berücksichtigen sind. Weiterführende Umsetzungshinweise des BSI finden Sie in den angefügten Fußnoten.

a. Organisatorische Maßnahmen

- **Gehen Sie sorgsam mit sensiblen oder personenbezogenen Daten um**
  Eines der wichtigsten Güter, die wir derzeit haben, sind Informationen. Diese können einen beachtlichen Wert besitzen und sind daher oftmals Ziel von so genannten Hackerangriffen. Insbesondere bei personenbezogenen Daten kann dies neben einem materiellen Schaden auch einen immensen immateriellen Schaden zu Folge haben, wenn diese publik werden. Daher ist es umso wichtiger, dass Unbefugte keinen Zugriff/Einblick auf die Informationen erhalten, wenn sie erstellt, transportiert oder entsorgt werden. Es gilt dabei den ganzen Lebenszyklus einer Information zu schützen.
  Vermeiden Sie daher öffentliche WLAN-Zugänge und nutzen Sie Ihr gesichertes Heimnetzwerk. Eventuell steht Ihnen ein VPN-Netzwerk zur Verfügung, dass Sie nutzen können. Sollten Unterlagen nicht mehr benötigt werden, entsorgen Sie diese bitte fachgerecht (z. B. in Ihrer Dienststelle)

- **Schaffen Sie sich nach Möglichkeit einen Arbeitsraum**
  Es ist empfehlenswert einen adäquaten Raum für Ihre Arbeit zu nutzen, der über einen entsprechenden Zutrittsschutz und Sichtschutz verfügt.
  Auch bei kurzer Abwesenheit sind die technischen Geräte zu sperren (z. B. Bildschirmsperre bei Windowsgeräten über Windowstaste + kleines „L“ oder Strg+Alt+Entf/Ende).
  Bei längerer Abwesenheit und Dienstschluss: Melden Sie sich von Fachanwendungen ab und fahren Sie Ihre Endgeräte herunter. Außerdem sind ebenso die Arbeitsmittel, Unterlagen, Akten usw. zugangsgesichert und verschlossen zu verwahren (z. B. Schrank, Raum). Sollten entsprechende Verschlussmöglichkeiten nicht vorhanden sein, sind die Geräte anderweitig vor dem Zugriff durch Dritte (insbesondere Familienmitglieder) geschützt zu lagern.

- **Vorsicht bei E-Mails mit potentiell gefährlichen Anhängen und Links**
  Die meisten erfolgreichen Angriffe durch Hacker basieren auf sogenannten Fake- oder Phishing-E-Mails. Zum Teil werden bekannte alte Konversationen aufgegriffen, um Ihnen ein Gefühl der Vertrautheit zu vermitteln, um Sie dazu zu verleiten, schadhafte Anhänge oder Links zu öffnen. Fragen Sie sich immer: „Ist der Absender bekannt?“, „Ist der Betreff sinnvoll?“ und „Erwarte ich einen Anhang von diesem Absender?“ Hierdurch sind Sie in der

Lage, einzuschätzen, ob die E-Mail vertrauenswürdig ist. 3 Haben Sie Zweifel an der Authentizität der E-Mail kontaktieren Sie den vermeintlichen Absender direkt z. B. durch einen Anruf.

- **Nutzen Sie vertrauenswürdige Quellen für jegliche Downloads (Software, Medien und Updates)**
  Sollten Sie Daten aus dem Internet benötigen, laden Sie diese bitte direkt vom Hersteller herunter. Laden Sie die Daten von anderen Quellen, könnte so genannte Ad-Malware in den Daten versteckt sein. Es empfiehlt sich immer, die heruntergeladenen Daten mittels einer aktuellen Anti-Viren-Software zu prüfen.

- **Vergessen Sie das Backup nicht**
  Erstellen Sie regelmäßig Backups von Ihren wichtigen Daten. Sollte ein Angriff auf Ihr Endgerät erfolgreich sein, so haben Sie die Möglichkeit Ihre Daten wiederherzustellen. In der Regel werden durch Angriffe Ihre Daten auf Ihrem Gerät verschlüsselt. Gehen Sie nicht auf etwaige Erpressungsversuche ein, es gibt keine Garantien, dass die Angreifer Ihre Daten wieder entschlüsseln werden. Informieren Sie umgehend Ihre Vorgesetzten und IT Verantwortlichen.

- **Meldepflicht für Diebstahl oder Verlust von Endgeräten oder Datenträgern**
  Jede Sekunde zählt, wenn sensible oder personenbezogene Daten betroffen sind. Melden Sie daher umgehend den Verlust oder Diebstahl eines Endgerätes oder Datenträgers bei Ihrem Vorgesetzten und Ihrem bestellten Datenschutzbeauftragten.

b. Technische Maßnahmen

- **Führen Sie regelmäßig Aktualisierungen durch**
  Veraltete Software weist oft kritische Sicherheitslücken auf. Viele dieser Lücken werden öffentlich kommuniziert, um mögliche Softwareupdates bereitzustellen. Daher ist es wichtig, das Betriebssystem sowie jegliche andere Software auf einem möglichst aktuellen Stand zu halten. Dies kann heutzutage über die Nutzung der Funktion zur automatischen Aktualisierung komfortabel umgesetzt werden. Nach dem eingangs erwähnten Erforderlichkeitsprinzip empfiehlt es sich, Programme die längere Zeit nicht in Anspruch genommen wurden, zu deinstallieren. Denn die Angriffsfläche wird kleiner, desto weniger Programme auf Ihrem System installiert sind.

- **Verwenden Sie einen aktuellen Virenschutz und Firewall**
  Zum Schutz vor Angriffen von außen ist eine Firewall essenziell. Sie schützt Sie vor dem Ausspähen sowie Ausführen von unerwünschten Programmen durch nichtautorisierte Dritte. Sollte doch einmal eine Schadsoftware auf Ihren Rechner platziert worden sein, greift im besten Fall der Virenschutz. Beide Komponenten (Virenschutz und Firewall) sind in den gängigen Betriebssystemen integriert. Prüfen Sie, ob diese beiden Komponenten aktiviert sind. Alternativ können Sie auch den Virenschutz und Firewall eines anderen vertrauenswürdigen Anbieters einsetzen. Aber denken Sie daran, die erste und wichtigste Maßnahme ist Ihre eigene Aufmerksamkeit.

[3] https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Menschenverstand/E-Mail/E-Mail_node

- **Verwenden Sie in Ihrem Betriebssystem verschiedene Konten/Passwörter für verschiedene Einsatzzwecke**
  Schadprogramme erhalten die gleichen Rechte wie die angemeldete nutzende Person, die sie unabsichtlich installiert bzw. ausgeführt hat. Daher ist es wichtig, dass im täglichen Betrieb ein Benutzungskonto verwendet wird, was keinem Administrator entspricht. Werden Rechte einer administrierenden Person benötigt, wird explizit nach dem Passwort gefragt, so dass Sie mitbekommen, ob ein Programm unerlaubte Funktionen aufruft.
  Dieser Rat gilt auch für Passwörter. Verwenden Sie bitte unterschiedliche Passwörter für unterschiedliche Dienste (Online-Banking, Online-Shopping, E-Mail-Konten usw.). Hierfür eignen sich auch Passwortprogramme.

- **Achten Sie darauf, dass Sie einen aktuellen Webbrowser verwenden**
  Bei der Verwendung von Webbrowsern ist darauf zu achten, dass diese noch vom Hersteller unterstützt werden. Somit ist garantiert, dass wesentliche Sicherheitsupdates noch bereitgestellt werden können. Da auch Werbung auf schadhafte bzw. unerwünschte Internetseiten/Inhalte führen kann, sollten Sie nach Möglichkeit einen sogenannten Werbeblocker (engl. ad blocker) verwenden. Des Weiteren überprüfen Sie die Einstellungsmöglichkeiten Ihres Browsers, um unerwünschte Datenabflüsse zu vermeiden (z. B. "privater Modus", "Verlauf löschen", "Cookies nicht für Drittanbieter zulassen"). Sind Sie sich bei einem Link zu einer bekannten Seite nicht sicher, dann geben Sie die Adresse per Hand in die Adressleiste Ihres Browsers ein und verzichten auf die Nutzung des Links.

- **Setzen Sie auf eine starke Verschlüsselung Ihrer sensiblen und personenbezogenen Daten**
  Mittels einer Verschlüsselung können Daten bei der Übertragung und/oder Speicherung vor dem Zugriff durch unberechtigte Dritte geschützt werden. Für das Surfen mit einem Browser nutzen Sie bitte nur verschlüsselte Verbindungen wie das https-Protokoll. Sie erkennen in Ihrem Webbrowser, dass eine gültige Verschlüsselung vorliegt, an einem geschlossenem Schloss-Symbol neben der eigentlichen Internetadresse.
  Bei der Übertragung von sensiblen bzw. kritischen Daten nutzen Sie bitte die Möglichkeit der Verschlüsselung von E-Mails und deren Anhängen (z. B. mit den Programmen Winzip oder Winrar mit zusätzlichem Passwort). Die Übertragung beginnt aber bereits beim Medium wie dem WLAN. Daher ist darauf zu achten, dass dieses nach dem Stand der Technik verschlüsselt und mit einem ausreichend sicheren Passwort (mind. 20 Zeichen) geschützt ist.
  Auch die Daten auf dem eigentlichen Endgerät sollten durch eine dem Schutzbedarf der Daten entsprechende Verschlüsselung geschützt sein Hierfür bieten die gängigen Betriebssystemhersteller bereits integrierte Lösungen an (MacOS: FileVault, Windows: EFS) die auch für mobile Endgeräte (IOS: standardmäßig aktiv, Android: meist über Einstellungen aktivierbar) möglich sind.

- **Nutzen Sie nur vertrauenswürdige Cloud-Speicher-Dienste**
  Nutzen Sie keine privaten Cloudspeicher von Dritten (z. B. Dropbox) für die Speicherung von dienstlichen personenbezogenen Daten.

Weitergehende Informationen zur Umsetzung der Organisatorischen und Technischen Maßnahmen nach BSI finden Sie unter: www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/empfehlungen_node.html .

V. Glossar

AD	Active Directory: Speicherpunkt der Daten des schulischen Informations- und Planungssystems (SIP)
Ad-Blocker	Werbeblocker: Ein Programm, welches dafür sorgt, dass auf Webseiten enthaltene Werbung dem Betrachter nicht dargestellt wird.
Ad-Malware	Software, die eine Internet-Verbindung ohne explizite Zustimmung des Anwenders nutzt.
Backups	Eine Kopie, die man als Sicherung von einer Datei herstellt.
Konto des Nutzenden	Zugangsberechtigung zu einem zugangsbeschränkten IT -System durch welche das System die nutzende Person identifiziert.
BM	Ministerium für Bildung, Kultur und Wissenschaft des Landes Mecklenburg-Vorpommern
Browser	Software zur grafischen Darstellung des Internets.
BSI	Bundesamt für Sicherheit in der Informationstechnik (BSI): Verfolgt die Aufgabe der Untersuchung von Sicherheitsrisiken bei der Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen.
Cloudspeicher	Ein Dienst, mit dem Daten gespeichert werden können, indem sie über das Internet oder ein anderes Netzwerk an ein standortexternes System übertragen werden, das von einem Dritten verwaltet wird.
DSB	Datenschutzbeauftragte(r) des Ministeriums für Bildung, Kultur und Wissenschaft des Landes Mecklenburg-Vorpommern
DS-GVO	Datenschutz-Grundverordnung: Verordnung der Europäischen Union, mit der seit 2018 EU-weite vereinheitlichte Regelungen zur Verarbeitung personenbezogener Daten durch die meisten privaten und öffentlichen Datenverarbeiter festgelegt worden sind
EFS	Encrypting File System (EFS): Kennzeichnet ein System der Dateiverschlüsselung auf NTFS-Datenträgern unter Windows-NT-basierten Betriebssystemen wie Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8 und Windows 10.
eGo M-V	Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern
FileVault	Eine Funktion von Mac OS X/OS X/macOS zum Verschlüsseln von persönlichen Daten.
Firewall	Ein Sicherungssystem, welches ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt.
Https-Protokoll	Hypertext Transfer Protocol Secure Protokoll: Zustandsloses Protokoll zur Übertragung von Daten auf der Anwendungsschicht über ein Rechnernetz.
IDM	Zentrales Identitätsmanagementsystem: Instrument der digitalen Verwaltung von schulischen Identitäten
IT	Informationstechnik: Ein Oberbegriff für die elektronische Datenverarbeitung und die dabei verwendete Hard- und Software-Infrastruktur

IT-SiBe	IT-Sicherheitsbeauftragte(r): Übernimmt alle anstehenden Aufgaben hinsichtlich der IT-Sicherheit
Link	Eine Abkürzung für Hyperlink: Das ist ein Querverweis der einen Sprung zu einem anderen elektronischen Dokument oder an eine andere Stelle innerhalb eines Dokuments ermöglicht
lit.	Eine in der Rechtswissenschaft verwendete Abkürzung für lat. Littera, um einen bestimmten Punkt von nach Buchstaben gegliederten Aufzählungen in Rechtsnormen zu zitieren
Passwort Manager	Ein Computerprogramm, welches einer den Computernutzenden Person hilft, ihre Kennwörter und Geheimzahlen verschlüsselt zu speichern, zu verwalten und sichere Kennwörter zu erzeugen.
Phishing-E-Mails	Versuche, sich über gefälschte E-Mails als vertrauenswürdiger Kommunikationspartner in einer elektronischen Kommunikation auszugeben.
Podcast	Eine Serie von Mediendateien, also Audio- oder auch Video-Dateien.
SchulDSVO-MV	Verordnung zum Umgang mit personenbezogenen Daten der Schülerinnen und Schüler, Erziehungsberechtigten, Lehrkräften und sonstigem Schulpersonal
SchulG M-V	Schulgesetz für das Land Mecklenburg-Vorpommern
SDM	Schuldienstemanagementsystem: Instrument der digitalen Verwaltung von schulischen Identitäten zur Verwendung in angeschlossenen Schuldiensten
Signatur	Textabschnitt mit Angaben zum Absender.
SIP	Schulinformations- und Planungssystems M-V: Modul zur Datenerhebung der benötigten Daten von Schülerinnen und Schüler und Lehrkräften an den allgemein bildenden und beruflichen Schulen in Mecklenburg Vorpommern
SSO	Single Sign-on: Er erlaubt über einen einzigen Authentifizierungsprozess Zugriff auf Services, Applikationen oder Ressourcen. Dabei ersetzt der SSO einzelne Anmeldeverfahren mit unterschiedlichen Daten von Nutzenden und nutzt eine einzelne übergreifende Identität dafür.
TOM	Technische und Organisatorische Maßnahmen: Beschreibt alle Maßnahmen, die vom Verantwortlichen für den Schutz der personenbezogenen Daten ergriffen werden
UHD	User-Help-Desk: Technische Ansprechperson des Ministeriums für Bildung, Kultur und Wissenschaft M-V bei der Nutzung des IDM
Updates	Aktualisierung: Eine neue und verbesserte Version eines Programms.
Verschlüsselung von Daten	Umwandlung von Daten in eine Form, die von nicht autorisierten Personen nicht zu verstehen ist.
Verschlüsselung von E-Mails	Wird verwendet, um vertrauliche Informationen per E-Mail von Absendenden zu Empfangenden zu schicken.
VPN	Virtuelles privates Netzwerk: Darunter ist ein in sich geschlossenes Kommunikationsnetz zu verstehen. Es ist virtuell in dem Sinn, dass es keine eigene physische Verbindung aufweist, sondern ein bestehendes Kommunikationsnetz als Transportmedium verwendet. Es verbindet Teilnehmer des bestehenden Kommunikationsnetzes mit einem anderen Netz
WinZIP/WinRAR	Packprogramm zur Datenkompression.

WLAN	Wireless Local Area Network: Ein lokales Funknetz zur Datenübertragung.
WPA2	Wi-Fi Protected Access 2: Implementierung eines Sicherheitsstandards für Funknetzwerke nach WLAN-Standards.

VI. Änderungshistorie

Datum	Version	Vorgenommene Änderungen
12. Mai 2021	1.0	-