DSV*Gruppe*

Rollen- und Berechtigungskonzept
EMMA

S2 – für den internen Gebrauch

Version:	**1.0**
Autor:	Paul Pruß
Letzte Änderung:	30.11.2022
Gültig seit:	30.11.2022

Freigabe durch:	Paul Preuß	**Gültigkeit:**	Gültig bis auf Weiteres
Geprüft und abgestimmt mit:	ISDS		

Version	Datum	Autor	Art und Umfang der Bearbeitung	Bemerkungen
1.0	30.11.2022	Paul Preuß	Initiale Erstellung	Keine

Inhaltsverzeichnis

A. Allgemeines

A.1 Zweck und Grundsätze

Dieses Rollen- und Berechtigungskonzept wurde gemäß den Anforderungen der ISDS-Konzernregeln erstellt. Etwaige Abweichungen vom Regelwerk sind in diesem Dokument ebenfalls festgehalten.

Die unberechtigte Verarbeitung von Informationen wird durch die strukturierte Festlegung von Zugangs- und Zugriffsmöglichkeiten verhindert. Unter Berücksichtigung des Schutzbedarfs sowie dem Need-to-Know- und Least Privilege-Prinzip werden in diesem Dokument Rollen und Berechtigungen für die Verarbeitung von Informationen im betrachteten IT-Asset EMMA beschrieben werden.

Dieses Konzept wurde erstellt, weil in der Applikation produktive Informationen der Sensitivitätsstufe S2 und höher verarbeitet werden.

Diese Vorlage umfasst nicht alle Regeln der Konzernrichtlinie „Zugangs- und Zugriffskontrolle“. Sofern zweckmäßig, kann dieses Dokument zu einem vollständigen Konzept für die Zugangs- und Zugriffskontrolle erweitert werden.

A.2 Aktualisierungszyklus

Sofern keine anlassbezogenen Änderungen erfolgen, wird dieses Dokument jährlich auf Aktualisierungsbedarf geprüft.

A.3 Mitgeltende Dokumente

Keine

B. Allgemeines

B.1 Benutzerkreis und Mandanten

Die Applikation wird von Sparkasseninstituten genutzt. Für jedes Institut ist ein eigener Mandant eingerichtet. Die Administration erfolgt durch den Instituts-Admin der Sparkasse, das EMMA Produkt-Team und den beauftragten Dienstleister Mailingwork GmbH.

B.2 Benutzerverzeichnis

Zentraler Verzeichnisdienst: Zentrale Benutzerverwaltung (ZBV) der DSV-Gruppe.

B.3 Allgemeine Maßnahmen und Grundsatzentscheidungen

Zur Vereinfachung des Benutzererlebnisses wurde ein transparentes Single-Sign-On realisiert, sodass für Active Directory Benutzer, die sich aus dem Unternehmensnetzwerk anmelden möchten, kein erneuter Login angefordert wird.

B.4 Verfahren zur Zugangs- und Zugriffskontrolle

ZBV Antragswesen

- Die Genehmigung von Berechtigungen erfolgt nur durch den Dateneigentümer erfolgen. Es werden nur die Zugriffsrechte genehmigt werden, die für die Aufgabenwahrnehmung des Benutzers notwendig sind („Need-to-Know Prinzip“). Unvollständige oder unpräzise Berechtigungsanträge werden zurückgewiesen. Nach Abschluss der Bearbeitung werden Berechtigungsanträge als erledigt gekennzeichnet und zur Dokumentation ordnungsgemäß verwahrt.
- Die Vergabe, die Änderung und der Entzug von Zugangs- und Zugriffsberechtigungen wird durch eine unabhängige Instanz durchgeführt. Die Durchführung wird explizit und nachvollziehbar dokumentiert, sowohl organisatorisch als auch technisch in Protokollen auf den betroffenen IT-Assets. Die Möglichkeit zur zeitnahen Zusammenstellung aller an einen Benutzer vergebenen Berechtigungen ist sichergestellt.
- Die Einhaltung des Verfahrens wird in regelmäßigen Abständen kontrolliert.
- Benutzerkonten sind personalisiert und Personen eindeutig zuordenbar. Nach der Anlage werden Benutzerkennungen nur noch bei Namensänderungen von Personen geändert. Solche Änderungen werden nachvollziehbar dokumentiert. Verwendete Benutzerkonten werden nicht wiederverwendet (auch nicht bei Namensgleichheit).
- Vor dem Löschen von Benutzerkonten ist sichergestellt, dass noch benötigte Nutzdaten im IT-Asset verbleiben.
- Es ist festgehalten und zu dokumentiert, in welchen Zyklen aktive Benutzerkonten auf Notwendigkeit geprüft werden (gilt nicht für Kunden-Accounts).
- Die unbemerkte und unprotokollierte Übernahme von Benutzerkonten durch Administratoren ist ausgeschlossen.

C. Benutzerkonten, Rollen und Gruppen

C.1 Arten von Benutzerkonten

- **EMMA-Administratoren**
  EMMA-Team und ausgewählte Mitarbeiter des Dienstleisters Mailingwork GmbH.
- **Instituts-Administratoren**
  Relevant im Zuge der ZBV-Anbindung für die Benutzerverwaltung.
- **(Chef-)Redakteure**
  Klassische Rolle zur Nutzung des Tools für die Mitarbeitenden der Sparkasse zur Umsetzung der E-Mail Marketing Kampagnen.
- **Analysten**
  Analytische Rolle zur Auswertung der E-Mail Marketing Kampagnen. Stark eingegrenztes Rechteprofil.
- **Technische Benutzer**
  z. B. für die Bearbeitung täglicher Job-Routinen.

C.2 Rollen und Gruppen

In EMMA werden Benutzenden Rollen und Gruppen für festgelegte Verwendungszwecke zugewiesen.

In EMMA verläuft die Zuordnung zur jeweiligen „Gruppe“ in dem Sinne, dass Sie einem gewissen Mandanten zugeordnet werden. In diesem Mandanten haben die Benutzenden Zugriff auf die jeweiligen Institutsinhalte mit allen weiteren Mitarbeitenden des Instituts, die ebenfalls diesem Mandanten zugeordnet sind. Ein mögliches Szenario ist aber auch, dass es mehrere Mandanten pro Institut gibt.

Die Zuordnung von Rollen kann z. B. zur Strukturierung von Benutzern gemäß ihrer Organisationseinheit oder dem durchgeführten Projekt umgesetzt werden, um Berechtigungen an weniger Stellen in der Administration pflegen zu müssen. Benötigt ein Benutzer neue Berechtigungen, so kann dies über einen Rollenwechsel oder die zusätzliche Zugehörigkeit zu einer neuen Rolle schnell umgesetzt werden.

Für bestimmte fachliche oder administrative Aufgaben sind Rollen und deren Berechtigungen festgelegt. Diesen Rollen können Benutzern zugewiesen werden.

Im Folgenden wird auf die Rollenstruktur der Applikation EMMA eingegangen. Berücksichtigt sind dabei die unterschiedlichen Standard-Rollen für die Ausübung der etwaigen Aufgabenfelder in EMMA.

Rolle	Zwecke / Beschreibung
EMMA-Administratoren	*EMMA-Team und ausgewählte Mitarbeiter des Dienstleisters Mailingwork GmbH.*
Instituts-Administratoren	*Relevant im Zuge der ZBV-Anbindung für die Benutzerverwaltung.*
(Chef-) Redakteure	*Klassische Rolle zur Nutzung des Tools für die Mitarbeitenden der Sparkasse zur Umsetzung der E-Mail Marketing Kampagnen.*
Analysten	*Analytische Rolle zur Auswertung der E-Mail Marketing Kampagnen. Stark eingegrenztes Rechteprofil.*
Technische Benutzer	*z. B. für die Bearbeitung täglicher Job-Routinen.*

Rolle	EMMA-Administratoren	Instituts-Administratoren	(Chef-) Redakteure	Analysten	Technische Benutzer
Abonnenten-Rechte					
Personalisierungen erstellen	X		X	X	
Personalisierungen löschen	X		X	X	
Abonnentenlisten erstellen	X		X		
Abonnentenlisten bearbeiten	X		X		
Abonnentenlisten löschen	X		X		
Abonnentenverwaltung erstellen	X		X		
Abonnentenverwaltung bearbeiten	X		X		
Abonnentenverwaltung löschen	X		X		
Ausschlusslisten verwalten	X		X		
Abonnentenfelder erstellen	X		X		
Abonnentenfelder bearbeiten	X		X		
Abonnentenfelder löschen	X				
Zielgruppe erstellen	X		X		
Zielgruppe bearbeiten	X		X		
Zielgruppe löschen	X		X		
Profilanreicherung verwenden	X		X		
Abonnenten importieren	X		X		
Abonnenten exportieren	X		X		
Abgleich logisch falscher E-Mails verwenden	X		X		

Blacklist-Abgleich verwenden	X		X		
Abmeldeabgleich verwenden	X		X		
Dublettenabgleich verwenden	X		X		
Dublettenabgleichssetup erstellen	X		X		
Dublettenabgleichssetup bearbeiten	X		X		
Dublettenabgleichssetup löschen	X				
Bounces exportieren	X		X	X	
Bounces zurücksetzen	X		X		
Bounces bereinigen	X		X		
Blacklist erstellen	X		X		
Blacklist bearbeiten	X		X		
Blacklist löschen	X		X		
Blacklist importieren	X		X		
Blacklist exportieren	X		X		
Anmeldungen verwenden	X		X		
Abmeldungen löschen	X		X		
Abmeldungen importieren	X		X		
Abmeldungen exportieren	X		X	X	
Abmeldungen wiederherstellen	X		X		
Beschwerden verwenden	X		X		
Beschwerden exportieren	X		X		
Mailing-Rechte					

Mailings allgemein Abonenntenzahl einblenden	X		X	X	
E-Mail erstellen	X		X		
E-Mail bearbeiten	X		X		
E-Mail löschen (Status: In Bearbeitung)	X		X		
E-Mail löschen (Status: aktiviert, pausiert, versendet)	X				
E-Mail kopieren	X		X		
E-Mail aktivieren	X		X		
E-Mail E-Mails ohne Template verwenden	X		X		
E-Mail Gesperrte Artikel bearbeiten	X				
E-Mail Gesperrte Link-Tracking Parameter bearbeiten	X		X		
E-Mail Anhänge anfügen	X		X		
E-Mail Testversand durchführen	X		X		
E-Mail-Archiv verwenden	X		X	X	
AB-Test erstellen	X		X		
AB-Test bearbeiten	X		X		
AB-Test löschen	X		X		
Conversion Tracker verwenden	X				
Statistik-Rechte					
Report per E-Mail versenden verwenden	X		X	X	
Report-Templates erstellen	X		X		
Report-Templates bearbeiten	X		X		

Report-Templates löschen	X				
E-Mail-Statistik verwenden	X		X	X	
Mailingvergleich verwenden	X		X	X	
E-Mail-Versand-Statistik verwenden	X		X	X	
Abonnentenstatistik verwenden	X		X	X	
Bildpersonalisierung-Statistik verwenden	X				
Module/Extras-Rechte					
Systembenachrichtigungen verwenden	X				
E-Mail-Templates erstellen	X				
E-Mail-Templates bearbeiten	X				
E-Mail-Templates löschen	X				
Personalisierungshelfer erstellen	X		X		
Personalisierungshelfer bearbeiten	X		X		
Personalisierungshelfer löschen	X				
Dynamische Inhalte erstellen	X				
Dynamische Inhalte bearbeiten	X		X		
Dynamische Inhalte löschen	X				
Bildpersonalisierung erstellen	X				
Bildpersonalisierung bearbeiten	X				
Bildpersonalisierung löschen	X				
Bildpersonalisierung Generierung erstellen	X				

Bildpersonalisierung Generierung bearbeiten	X				
Bildpersonalisierung Generierung löschen	X				
Bildpersonalisierung Generierung generieren	X				
Kampagne erstellen	X		X		
Kampagne bearbeiten	X		X		
Kampagne löschen	X		X		
Kampagne aktivieren	X	X	X	X	
Content Management erstellen	X		X		
Content Management bearbeiten	X		X		
Content Management löschen	X		X		
Content Management freigeben	X				
Content Management downloaden	X		X		
Content Management Templates erstellen	X				
Content Management Templates bearbeiten	X				
Content Management Templates löschen	X				
Externes Archiv erstellen	X		X		
Externes Archiv bearbeiten	X		X		
Externes Archiv löschen	X				
Medien erstellen	X		X		
Medien bearbeiten	X		X		
Medien löschen	X		X		
Ordner erstellen	X		X		

Ordner bearbeiten	X		X		
Ordner löschen	X		X		
Landingpage erstellen	X		X		
Landingpage bearbeiten	X		X		
Landingpage löschen	X		X		
Landingpage-Templates erstellen	X				
Landingpage-Templates bearbeiten	X				
Landingpage-Templates löschen	X				
Profilmanager-Setup erstellen	X		X		
Profilmanager-Setup bearbeiten	X		X		
Profilmanager-Setup löschen	X				
Verteilen nach oben	X				
Verteilen nach unten	X				
Verteilen quer	X				
Verteilen Stellvertreter bearbeiten	X				
Umfrage erstellen	X		X		
Umfrage bearbeiten	X		X		
Umfrage löschen	X		X		
Umfrage Personalisierte Umfrage erstellen	X		X		
Umfrage-Templates erstellen	X				
Umfrage-Templates bearbeiten	X				
Umfrage-Templates löschen	X				

Umfragestatistik verwenden	X		X	X	
Weiterempfehlen-Setup erstellen	X				
Weiterempfehlen-Setup bearbeiten	X				
Weiterempfehlen-Setup löschen	X				
Webservice (API, Zapier) verwenden	X				X
Explorer verwenden	X				
Webspace verwenden	X		X		
Interessen erstellen	X		X		
Interessen bearbeiten	X		X		
Interessen löschen	X		X		
Accountkonstanten verwenden	X		X		
Admin/Setup-Rechte					
E-Mail Versandlog verwenden	X				
Benutzer erstellen	X	X			
Benutzer bearbeiten	X	X			
Benutzer löschen	X	X			
Benutzer Login per Hijack zulassen	X			X	
Benutzerrolle erstellen	X				
Benutzerrolle bearbeiten	X				
Benutzerrolle löschen	X				
Anmeldevorgang erstellen	X		X		
Anmeldevorgang bearbeiten	X		X		
Anmeldevorgang löschen	X				

Abmeldevorgang erstellen	X		X		
Abmeldevorgang bearbeiten	X		X		
Abmeldevorgang löschen	X				
Importsetup erstellen	X				
Importsetup bearbeiten	X				
Importsetup löschen	X				
E-Mail-Setup erstellen	X				
E-Mail-Setup bearbeiten	X				
E-Mail-Setup löschen	X				
Passwortregeln bearbeiten	X				
Eingabeprotokoll verwenden	X				
Redirect-Domain einstellen	X				

C.3 Rollenkonflikte

Folglich wurde bewertet und dokumentiert, welche Rollen nicht miteinander kombiniert werden dürfen. Die Ausübung mehrerer Rollen durch eine Person ist grundsätzlich möglich. Rollenkonflikte entstehen dann, wenn eigentlich unvereinbare Rollen in Personalunion wahrgenommen werden. Z. B. sollten Benutzer, die in Workflows eine Freigabefunktion haben, nicht gleichzeitig prüfende Rollen einnehmen.

nicht zu kombinierende Rollen	**EMMA-Administratoren**	**Instituts-Administratoren**	**(Chef-) Redakteure**	**Analysten**	**Technische Benutzer**
EMMA-Administratoren	-	X	X	X	X
Instituts-Administratoren	X	-	X	X	X
(Chef-) Redakteure	X	X	-		X
Analysten	X	X		-	X
Technische Benutzer	X	X	X	X	-

C.4 Kritische Vorgänge

Es sind keine kritischen Vorgänge dokumentiert.