Intern · Vertraulich Dokument-Nr.: DS-IGP-PR-014 Version: 1.3 Gültig ab: 2025-04-01

Eigentümer: Fachbereich Digital Sales (FDS), FictaBank AG

Maßnahme: Regelmäßige Berechtigungsüberprüfung in FDS

Dieses Dokument beschreibt die abteilungsinterne Maßnahme zur risikobasierten Überprüfung von Zugriffsberechtigungen in den Kernanwendungen des Fachbereichs Digital Sales (FDS). Ziel ist die Reduktion des Risikos unberechtigter Datenzugriffe und fehlerhafter Transaktionen durch veraltete Rollen und Rechte.

1 Zweck und Geltungsbereich

Die Maßnahme regelt, wie FDS Zugriffsberechtigungen für in- und externe Mitarbeitende in den Anwendungen *CRM-SalesPro*, *DataLake-X*, *SFTP-Marketing* und *SAP BW* regelmäßig überprüft, freigibt oder entzieht. Sie gilt für alle FDS-Teams, inklusive befristet Beschäftigte, Werkstudierende und Lieferantenpersonal, soweit diese über FDS verantwortete Rollen verfügen.

Die Maßnahme nutzt die zentrale Identity-Governance-Plattform (IGP „Keystone“) für Review-Kampagnen und das Service-Management-System (SMS „ServiceDeskOne“) für Änderungsaufträge. Schnittstellen zu HR („PeopleCore“) und Vendor-Management („ThirdPartyHub“) liefern Stammdaten.

2 Risikobeschreibung & Ziel der Maßnahme

> **Risikothese:** Veraltete Berechtigungen (z. B. nach Rollenwechsel oder Vertragsende) können zum unautorisierten Zugriff auf Kundendaten und Finanzkennzahlen führen und regulatorische Meldepflichten auslösen.

Zielbild: FDS stellt sicher, dass Berechtigungen aktuell, zweckgebunden und minimal sind (*need-to-know*). Dies erfolgt durch halbjährliche Review-Kampagnen, anlassbezogene Prüfungen bei Personalveränderungen sowie dokumentierte Anpassungen im SMS.

3 Rollen & Verantwortlichkeiten

Die folgenden Rollen sind in IGP hinterlegt und im Delegationsregister (FDS-DELEG-List) mit Vertreterregelung dokumentiert.

Rollenbeschreibung (Auszug)

Rolle	Verantwortung
FDS-Anwendungs-verantwortliche (AV)	Starten und Freigeben der Review-Kampagnen pro Anwendung; finale Entscheidung über Entzug/Sperre; fachliche Eignungsprüfung anhand Aufgabenprofil.
Teamleads (TL)	Erstprüfung der Berechtigungen der Teammitglieder, Bestätigung der Arbeitsaufgaben und Projektzuordnungen; Meldung von Abwesenheiten & Rollenwechseln.

Delegationsprinzip: Nur von FDS-Leitung autorisierte AV/TL dürfen Reviews durchführen. Vertretungen sind namentlich benannt und zeitlich befristet (Urlaub, Krankheit). Schulung „IGP Reviewer Basics“ ist verpflichtend.

Rolle	Verantwortung
IGP-Kampagnen-koordinator:in (FDS-GRC)	Konfiguration der Kampagnen, Fristenmanagement, KPI-Reporting, Eskalation bei Fristüberschreitung.
ServiceDeskOne Change-Manager:in	Technische Umsetzung der genehmigten Änderungen, Vier-Augen-Freigabe, Ticket-Verknüpfung zur Kampagne.

4 Prozessbeschreibung der Berechtigungsüberprüfung

4.1 Ereignisgetriebene Prüfungen (Joiner/Mover/Leaver)

IGP erhält wöchentlich Stammdaten aus PeopleCore (Mitarbeiterstatus, Organisationseinheit, TL-Zuweisung). Bei *Leaver* wird automatisch eine Sofortsperre generiert; bei *Mover* wird eine anlassbezogene Einzelprüfung an den zuständigen TL ausgelöst. Lieferantenstatus wird monatlich aus ThirdPartyHub importiert.

4.2 Regelmäßige Review-Kampagnen

FDS führt halbjährlich (April & Oktober) kampagnenbasierte Reviews in IGP durch. AV und TL prüfen für jede betroffene Person die Zweckbindung, Rollen-Minimalität und Projektlaufzeiten. Entscheidungen (*Bestätigen*, *Entziehen*, *Ändern*) werden direkt in IGP erfasst; erforderliche Änderungen werden automatisiert als Tickets in ServiceDeskOne erstellt.

4.3 Fristen, Eskalation, Qualitätssicherung

- Frist: 15 Arbeitstage je Kampagne; automatische Erinnerungen nach 5/10 Tagen; Eskalation an FDS-Leitung ab Tag 12.
- Stichprobe (GRC): 5 % der „Bestätigt"-Entscheidungen werden gegen Aufgabenprofile und Projektverträge quergeprüft.
- Abwesenheiten: TL-Vertretungen sind verpflichtet, offene Positionen im Review zu übernehmen.

5 Nachweise, Protokollierung & Aufbewahrung

Alle Review-Entscheidungen werden in IGP mit Zeitstempel, Entscheider:in, Begründung und betroffenen Rollen protokolliert. IGP übergibt eine unveränderbare Kampagnen-Zusammenfassung (*Campaign Evidence PDF*) an das DMS. Jede Änderung (Entzug/Änderung) erzeugt ein verknüpftes SMS-Ticket mit Umsetzung, Vier-Augen-Freigabe und Abschlussprotokoll.

Aufbewahrungs- & Nachweisregeln

Nachweis	System	Inhalt	Aufbewahrung
IGP Kampagnen-Log	IGP „Keystone"	Reviewer, Entscheidungen, Zeitstempel, Änderungsbegründungen	3 Jahre (unveränderbar, revisionssicher exportiert ins DMS)
Änderungstickets	ServiceDeskOne	Request, Genehmigungen, Umsetzung, Vier-Augen-Freigabe, Abschluss	3 Jahre (Verknüpfung zur Kampagne)
Stichprobenberichte	Confluence	5 %-Sample, Prüfnotizen, Abweichungen & Korrekturmaßnahmen	3 Jahre

6 Abgrenzung: Administrative Berechtigungen

Diese Maßnahme umfasst ausschließlich fachliche Rollen (z. B. *CRM_READ*, *DLX_MARKETING_ANALYST*). Administrative Berechtigungen (*CRM-SP-ADMIN*, *DLX-ADMIN*, *SAP_BASIS_ADMIN*) werden derzeit **nicht** im Rahmen der FDS-Kampagnen geprüft. Für diese Gruppen ist die zentrale IT (CIO-Bereich) verantwortlich; ein abgestimmtes, mindestens jährliches Review über Systemowner und IT-Security ist in Arbeit (CIO-Projekt „ADMIN-GOV-2025“, geplante Inbetriebnahme Q4/2025).

> **Bekannte Lücke:** FDS erhält bisher keine Bestätigung über die erfolgten Admin-Reviews der zentralen IT; es existiert auch kein Abgleich zwischen FDS-Personalliste und Admin-Gruppen.

7 Metriken & Steuerung

KPIs letzte Kampagne (Oktober 2024)

KPI	Wert	Ziel	Anmerkung
Fristgerecht abgeschlossen	97 %	≥ 95 %	3 verspätete Teams, Eskalation an FDS-Leitung
Anteil Entzüge/Änderungen	11 %	—	Hinweis auf Bereinigungsbedarf, kein Alarmwert
Stichproben-Beanstandungen	2 Fälle	0	Beide Fälle externes Personal mit abgelaufenem SOW

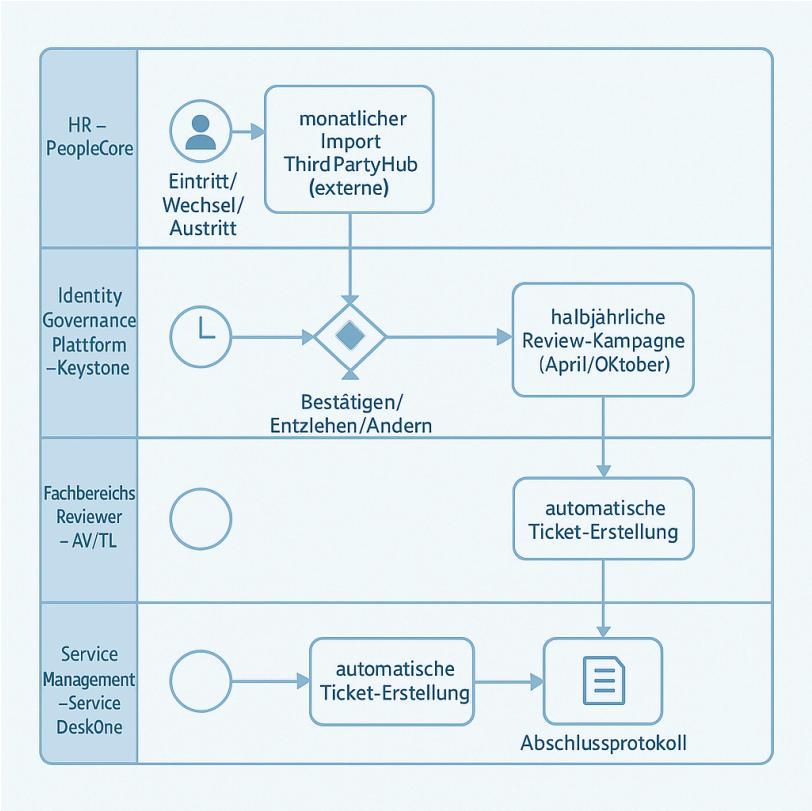
8 Review-Zusammenfassung (Datenauszug)

Auszug Kampagne „FDS-Q4-2024“

Benutzer	Typ	Team	System/Rolle	Entscheidung	Begründung (Kurz)	IGP-Zeitstempel	Ticket-ID
Anna Schmidt	Intern	Performance Marketing	DataLake-X / DLX_MARKETING_ANALYST	Bestätigt	Aktives Projekt „Attribution 2.0“	2024-10-07 10:14	SDO-124558
Ben Müller	Extern (Lieferant)	CRM Ops	CRM-SalesPro / CRM_EDIT	Entzogen	SOW abgelaufen 2024-09-15	2024-10-08 15:22	SDO-124733
Ch. Nguyen	Intern	Data Science	SFTP-Marketing / SFTP_WRITE	Ändern	Reduzierung auf READ (Rollentausch)	2024-10-09 09:03	SDO-124840
D. Keller	Intern (Elternzeit)	CRM Ops	CRM-SalesPro / CRM_READ	Bestätigt	Ersatz übernimmt keine Rolle	2024-10-10 13:47	—
E. Rossi	Extern (Lieferant)	Data Science	DataLake-X / DLX_CONTRACTOR	Bestätigt	SOW Verlängerung in Prüfung	2024-10-11 08:26	—

Hinweis: Zeile „D. Keller“ illustriert die Lücke bei Langzeitabwesenheit – keine automatisierte temporäre Entziehung möglich, nur TL-Entscheid (siehe Abschnitt 4). Zeile „E. Rossi“ zeigt Abhängigkeit von ThirdPartyHub-Rhythmus.

9 Visualisierung



10 Maßnahmenplan & Verbesserungen

- **TPH-Frequenz erhöhen:** Abstimmung mit Vendor-Management zur wöchentlichen Aktualisierung von ThirdPartyHub (Ziel: < 7 Tage Latenz).
- **PeopleCore-Attribut „Langzeitabwesenheit“ integrieren:** Erweiterung der IGP-Schnittstelle, automatische temporäre Entziehung oder Suspension.
- **Admin-Reviews:** Verbindliche Schnittstelle zur CIO-Review-Bestätigung (API/Report), Synchronisierung mit FDS-Personalliste.
- **Policy-Update:** Ergänzung der TL-Meldepflicht um tägliche Reminder bis Umsetzung im System erfolgt.

11 Anhang

11.1 RACI-Matrix (Auszug)

Aktivität	R	A	C	I
Kampagnen konfigurieren	FDS-GRC	AV	IT-IGP	FDS-Leitung
Review durchführen	TL	AV	GRC	HR
Änderungen umsetzen	ServiceDesk	AV	TL	Betroffene/r

11.2 Prüfpfad-Checkliste (für interne Nutzung)

1. IGP-Kampagnen-Export vorhanden und vollständig?
2. Stichproben-Abgleich: Aufgabenprofil ↔ bestätigte Rollen
3. Ticket-Verknüpfungen vorhanden & abgeschlossen (Vier-Augen-Prinzip)?
4. Externe: SOW-Gültigkeit ↔ Berechtigungsstatus
5. Langzeitabwesenheiten: manuelle Suspendierung erfolgt?

Erstellt von: FDS-GRC · Genehmigt durch: FDS-Leitung · Nächste Überprüfung des Dokuments: 2026-04-01

Änderungshistorie: v1.3 – Klarstellung Geltungsbereich, KPI-Update, Ergänzung Lückenanalyse Admin-Rollen.