

SENSITIVITY LABELS

digital erfolgreich

redIT Services AG
Arbachstrasse 2d | CH-6340 Baar



Inhaltsverzeichnis

1	EINLEITUNG	3
2	PRODUKTSPEZIFIKATIONEN	3
3	MODULE.....	4
3.1	Envisioning & Zielbild.....	4
3.2	Readiness & Analyse	4
3.3	Label Governance & Konzept	4
3.4	Pilot, Testing & Validierung	4
3.5	Technische Konfiguration	4
3.6	Rollout & Enablement	5
3.7	Betrieb, Monitoring & Optimierung.....	5
3.8	Zusatzmodule	5
4	VORAUSSETZUNGEN	5
5	NICHT ENTHALTENE LEISTUNGEN	5
6	ALLGEMEINE BESTIMMUNGEN	6

1 EINLEITUNG

Das vorliegende Dokument beschreibt das Produkt «Sensitivity Labels» als modulare redIT Leistung zur strukturierten Einführung von Microsoft Purview Information Protection. Ziel ist es, Unternehmensdaten nachvollziehbar zu klassifizieren, zielgerichtet zu schützen und die Nutzung von Microsoft 365, Teams, SharePoint, Outlook, MS Office und KI-Lösungen wie Microsoft 365 Copilot und dahinterliegende agentische Lösungen sicherer zu gestalten.

Sensitivity Labels verbinden fachliche Datenklassifizierung mit technischen Schutzmassnahmen. Dadurch entsteht eine gemeinsame Sprache zwischen Business, IT, Security und Compliance. Gleichzeitig wird vermieden, dass Datenschutz und Informationssicherheit rein technisch betrachtet werden. Das Produkt richtet sich deshalb sowohl an IT Admins als auch an Geschäftsleitung, Datenschutz, Compliance und Fachbereiche.

redIT verfolgt einen pragmatischen Implementierungsansatz: Zuerst werden Verständnis, Zielbild und Readiness geschaffen. Danach werden Label Governance, Label Design und technische Konfiguration erarbeitet. Anschliessend folgen Pilotierung, Testing, Rollout, Schulung und Betrieb. Dieser rote Faden stellt sicher, dass Sensitivity Labels nicht nur konfiguriert, sondern in der Organisation verstanden, akzeptiert und nachhaltig genutzt werden.

Das Ziel: Kontrollierte Datensicherheit statt pauschaler Einschränkung. Sensitivity Labels sollen die Zusammenarbeit schützen, ohne den Arbeitsalltag unnötig zu blockieren.

2 PRODUKTSPEZIFIKATIONEN

Mit dem Produkt «Sensitivity Labels» bietet redIT eine ganzheitliche Einführungslösung für Datenklassifizierung und Informationsschutz in Microsoft 365. Sensitivity Labels sind Metadaten, die Dateien, E-Mails, Meetings, sowie Gruppenelemente wie Teams, SharePoint Sites, Microsoft 365 Gruppen und weitere Inhalte klassifizieren und je nach Konfiguration zusätzliche Schutzmassnahmen auslösen können.

Die Lösung basiert auf Microsoft Purview Information Protection und verbindet organisatorische Governance mit technischer Umsetzung. Labels werden in Microsoft Purview erstellt, mit Scopes und Schutzmassnahmen konfiguriert und über Publishing Policies an definierte Zielgruppen veröffentlicht. Erst durch diese Veröffentlichung werden Labels für Benutzer:innen in den unterstützten Anwendungen sichtbar und nutzbar.

Typische Schutzmassnahmen sind Verschlüsselung, Wasserzeichen, Kopf und Fusszeilen, Einschränkungen beim Weiterleiten, Standard Labels, Pflichtlabelung, Downgrade Begründungen sowie Governance Einstellungen für Teams, SharePoint Sites und Microsoft 365 Gruppen. Für erweiterte Szenarien können Sensitivity Labels als Signal für DLP, Endpoint DLP, Copilot und weitere Purview Funktionen genutzt werden.

Das redIT Angebot ist modular aufgebaut und folgt einem klaren Implementierungsverlauf:

- Envisioning & Zielbild: Gemeinsames Verständnis, Business Nutzen und Entscheidungsgrundlage.
- Readiness & Analyse: Prüfung von Ausgangslage, Lizenzierung, Tenant Einstellungen und Risiken.
- Label Governance & Konzept: Erarbeitung von Label Struktur, Scopes, Schutzmassnahmen und Verantwortlichkeiten.
- Pilot, Testing & Validierung: Prüfung der Wirkung mit realen Use Cases und definierter Testgruppe.
- Technische Konfiguration: Umsetzung in Microsoft Purview, Entra ID, SharePoint, Teams und Office.
- Rollout & Enablement: Kommunikation, Schulung und Befähigung von IT Support, Key Usern und Mitarbeitenden.
- Betrieb & Monitoring: Etablierung von Kontrollen und Supportprozessen.

Der Mehrwert liegt in einer belastbaren Balance zwischen Datensicherheit und Benutzerfreundlichkeit. Unternehmen erhalten klare Leitplanken für den Umgang mit sensiblen Informationen, reduzieren Risiken bei interner und externer Zusammenarbeit und schaffen eine wichtige Grundlage für moderne KI und Copilot Szenarien.

3 MODULE

3.1 ENVISIONING & ZIELBILD

- Absprache mit Kunde
- Inhaltliche Vorbereitung gemäss Ausgangslage
- Impuls Session zu Sensitivity Labels
- Einordnung in Microsoft Purview, M365 und Copilot
- Roadmap und Handlungsempfehlungen

3.2 READINESS & ANALYSE

- Analyse bestehender Klassifizierungen und Prozesse
- Stakeholder und Risikobereiche erfassen
- Lizenz und Tenant Readiness prüfen
- Abgleich von Datenschutz, Compliance und Business Anforderungen
- Readiness Report mit Massnahmenplan

3.3 LABEL GOVERNANCE & KONZEPT

- Vorbereitung Konzept Workshop
- Durchführung Workshop
- Definition Label Taxonomie
- Definition Scopes und Schutzmassnahmen
- Definition Publishing Policies
- Namenskonzept und Tooltip Logik
- Dokumentation und Abnahme

3.4 PILOT, TESTING & VALIDIERUNG

- Erstellung Testkonzept
- Pilotkonfiguration in Microsoft Purview
- Begleitete Tests mit Business Vertretern
- Validierung von Sharing, Verschlüsselung und Label Priorität
- Feedbackschlaufen und Nacharbeiten
- Abnahme der Pilotkonfiguration

3.5 TECHNISCHE KONFIGURATION

- Konfiguration Sensitivity Labels
- Konfiguration Group Labels und Item Labels
- Konfiguration Label Publishing Policies
- Aktivierung relevanter Tenant Einstellungen
- Konfiguration von Verschlüsselung und Inhaltskennzeichnung
- Konfigurationskatalog und technische Dokumentation

3.6 ROLLOUT & ENABLEMENT

- Rollout- und Schulungskonzept
- Schulung IT Support, Key User und Business Vertreter
- Anwenderdokumentation und FAQ
- Begleitung Rollout

3.7 BETRIEB, MONITORING & OPTIMIERUNG

- Definition Betriebsmodell
- Einführung Activity Explorer
- Einführung Content Explorer
- Troubleshooting Leitfaden
- Regelmässige Governance Reviews
- Optimierungsbacklog

3.8 ZUSATZMODULE

- Advanced Labeling & Auto Labeling
- Hybride Daten & AIP Client
- Double Key Encryption Assessment

4 VORAUSSETZUNGEN

Damit das Produkt «Sensitivity Labels» erfolgreich umgesetzt und betrieben werden kann, müssen folgende Voraussetzungen erfüllt sein:

- Eine aktive Microsoft 365 Umgebung mit Entra ID, Exchange Online, SharePoint Online, OneDrive und Teams.
- Administrative Berechtigungen für Microsoft Purview, Microsoft 365 Admin Center, Teams, SharePoint und bei Bedarf Entra ID oder PowerShell.
- Geeignete Microsoft Lizenzen gemäss gewünschtem Funktionsumfang, insbesondere für Purview Information Protection, Auto Labeling, Teams Meeting Labels oder Zusatzmodulen.
- Benennung von technischen Ansprechpersonen sowie fachlichen Vertretungen aus Datenschutz, Compliance, Security und relevanten Business Bereichen.
- Bereitstellung realer Testszenarien, Pilotbenutzer und Beispieldaten, sofern dies für Testing und Validierung erforderlich ist.
- Bereitschaft, organisatorische Entscheidungen zu Klassifizierung, Schutzbedarf, Sharing und Verantwortlichkeiten verbindlich zu treffen.

5 NICHT ENTHALTENE LEISTUNGEN

Die in diesem Dokument beschriebenen Leistungen umfassen explizit nicht die folgenden Punkte, sofern sie nicht separat offeriert werden:

- Umfassende rechtliche Bewertung von Datenschutz, Branchenregulatorik oder vertraglichen Geheimhaltungspflichten.
- Aufarbeitung oder Bereinigung bestehender Berechtigungsstrukturen ausserhalb definierter Module.
- Datenmigrationen, File Share Bereinigungen oder umfassende SharePoint Restrukturierungen.
- Individualentwicklungen, komplexe Automatisierungen oder Integrationen mit Drittsystemen.
- Betrieb und Support nach Projektabschluss ausserhalb einer separat vereinbarten Betriebsleistung.
- Flächendeckende Klassifizierung historischer Daten ohne separates Advanced Labeling oder Migrationsmodul.

6 ALLGEMEINE BESTIMMUNGEN

redIT kann nicht für Konfigurations- oder Manipulationsfehler des Kunden oder Dritten haftbar gemacht werden. Für Services, bei welchen Systemressourcen geteilt verwendet werden (Shared Services), nimmt der Kunde Rücksicht und schränkt die übermässige Nutzung dieser Ressourcen ein, um eine Beeinträchtigung der Leistung anderer Kunden auf demselben System zu verhindern («Fair use»). Beansprucht der Kunde die Systemressourcen über Gebühr (Vergleich mit dem Durchschnitt der Systemnutzer plus Toleranz), unterbreitet redIT dem Kunden ein Angebot für eine höhere Leistungsklasse. Nimmt der Kunde dieses Angebot nicht an, behält sich redIT vor, fristlos vom Vertrag zurückzutreten.

Die Services werden «Best effort» gewährleistet. Es gibt, wo nicht anders vermerkt, keine Garantie für bestimmte zugewiesene Systemressourcen oder Leistungsmerkmale. Bestehen Anzeichen eines rechts- oder vertragswidrigen Verhaltens, insbesondere einer missbräuchlichen Nutzung eines Service, kann redIT den Zugriff auf den Service ohne Vorankündigung umgehend entschädigungslos sperren oder einschränken, den Kunden zur rechts- und vertragskonformen Benutzung anhalten, den Vertrag frist- und entschädigungslos auflösen und gegebenenfalls Schadenersatz sowie die Freistellung von Ansprüchen Dritter verlangen.

Sollten einzelne Bestimmungen dieser Leistungsbeschreibung/Nutzungsbedingung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der übrigen Bestimmungen des jeweiligen Vertrags nicht tangiert.

digital erfolgreich

redIT Services AG

Arbachstrasse 2d | CH-6340 Baar

+41 41 747 50 50

info@redit.ch

www.redit.ch

Weitere Standorte:

Delfterstrasse 10 | CH-5000 Aarau

Bahnhofstrasse 25 | CH-5647 Oberrüti

