Cybersecurity Card

SIEMENS

Sichere Datenübertragung

IT-Services für sichere Datenübertragung und Zusammenarbeit externer Geschäftspartner mit Siemens

Anwendungsfall	Einmaliger sicherer Austausch von Dokumenten „Wir wollen ein Dokument einmal sicher austauschen."	Kontinuierlicher sicherer Austausch von Dokumenten „Wir wollen kontinuierlich Dokumente sicher austauschen."	Kontinuierlicher sicherer Austausch von Daten und Dokumenten „Wir wollen kontinuierlich Daten und Dokumente sicher austauschen."	Sichere Zusammenarbeit „Wir wollen gemeinsam an denselben Dokumenten arbeiten."		Sichere Zusammenarbeit rund um PLM „Wir wollen an denselben Dokumenten/Daten im Bereich PLM arbeiten, auch bei integrierten, komplexen Szenarien (z. B. Digital Twin)."	Zusammenarbeit in Echtzeit „Wir wollen ein sicheres virtuelles Meeting abhalten."
Empfohlener IT-Service	Sicherer Dateiaustausch SecuFEx	MS OneDrive	E-Mail-Verschlüsselung	SharePoint Global Collaboration Service-Portal	Workspace Strictly Confidential / Secure Data Room (SDR)	Siemens Teamcenter (TC)	MS Teams
Max. Schutzklasse	„Vertraulich"	„Vertraulich"[1]	„Streng vertraulich"	„Vertraulich"	„Streng vertraulich"	„Vertraulich"[2]	„Vertraulich"[3]
Technische Voraussetzungen	▪ Der Siemens-Geschäftspartnerkontakt muss ein temporäres Benutzerkonto zum Senden von Dateien angelegen.	▪ keine	▪ Voraussetzungen ▪ Implementierungshandbuch E-Mail-Verschlüsselung	▪ Technische Voraussetzungen ▪ PC-Einstellungen ▪ Mobiltelefon oder Token für Authentifizierung	▪ Mobiltelefon für Authentifizierung	▪ TC Supplier Collaboration Foundation (SCF)	▪ Meeting muss durch Siemens-Kontakt bereitgestellt werden
Benutzerhandbücher und technische Ansprechpartner	▪ SecuFEx-Webseite	▪ MS OneDrive Webseite	▪ Siemens PKI Webseite	▪ Webseite SharePoint Global Collaboration Service Portal	▪ SDR-Webseite	▪ SCF-Webseite	▪ MS Teams

[1] Schutzklasse „Vertraulich" ist möglich, wenn alle Teilnehmenden ein Konto auf Siemens Tenant haben oder die Dokumente entsprechend mit MIP geschützt sind. In allen anderen Fällen ist nur Schutzklasse „Intern" möglich.
[2] Hängt von lokaler Installation und Konfiguration ab, maximal bis „Intern". Die genaue Schutzklasse muss mit Ihrem Siemens-Ansprechpartner geklärt werden.
[3] Schutzklasse „Vertraulich" ist möglich, wenn alle Teilnehmenden ein Konto auf Siemens Tenant haben. Wenn ein Teilnehmender kein Siemens-Tenant-Konto hat oder Teilnehmende sich per Telefon einwählen, ist nur Schutzklasse „Intern" möglich.

Cybersecurity Card

Sichere Datenübertragung

SIEMENS

Definition

Geschäftspartner (GP): In diesem Zusammenhang jede externe Partei mit einer Geschäftsbeziehung zu Siemens, ohne autorisierten Zugang zum Siemens-Intranet (z. B. über Business Partner Access) und damit ohne Zugang zu Siemens-internen IT-Services.

Situation

Der Austausch von Informationen mit Geschäftspartnern gehört zu unserem Tagesgeschäft. In manchen Fällen sind Daten und Dokumente (wie Kosten-, Vertrags- oder technische Dokumente) als „vertraulich" oder sogar „streng vertraulich" klassifiziert. Diese auf Anwendungsfällen basierende IT-Service-Übersicht wurde erstellt, um eine sichere Kommunikation und gemeinsame Nutzung solcher Daten zu gewährleisten. Sie hilft Endnutzern von Siemens und ihren Geschäftspartnern, den geeigneten Siemens IT-Service zu identifizieren, zu wissen, wo er bestellt werden kann und wie er zu nutzen ist. Bitte beachten Sie, dass IT-Services für bestimmte Geschäftsprozesse (z. B. elektronischer Datenaustausch über EDI) noch führend sind und die Übersicht nur die restlichen Anwendungsfälle abdecken sollte (z. B. für die bisher der Prozess für unverschlüsselte E-Mail genutzt wird).

Bedrohung

Non-Disclosure Agreements (NDAs) und Siemens' „Regelungen für Geschäftspartner" definieren den richtigen Umgang mit vertraulichen Informationen, nennen aber keine konkreten IT-Lösungen zur Umsetzung der Regelungen.

Das birgt das Risiko, dass, auch wenn die Anforderungen an die Informationssicherheit bekannt sind, diese nicht richtig oder nur unvollständig umgesetzt werden.

Ihr Verhalten

Was Geschäftspartner beachten müssen, wenn sie eine E-Mail mit SecuFEx versenden:

Um Daten an einen Siemens-Mitarbeitenden schicken zu können, benötigen Geschäftspartner ein temporäres Konto für SecuFEx . Dieses temporäre Konto kann von allen Siemens-Mitarbeitenden eingerichtet werden. Nutzer des SecuFEx-Services müssen alle anwendbaren nationalen und internationalen (re-)exportkontrollrechtlichen Bestimmungen einhalten.

Was Geschäftspartner beachten müssen, wenn sie eine Einladung zu einer virtuellen Konferenz oder MS Teams-Sitzung von einem Siemens-Mitarbeitenden erhalten:

Der Geschäftspartner muss gewährleisten, dass es während des virtuellen Meetings keine neugierigen Blicke und unerwünschte Zuhörer gibt. Zudem ist es dem Geschäftspartner nicht gestattet, Hardcopies oder Screenshots vom Bildschirm zu machen, wenn vertrauliche Informationen gezeigt werden. Öffnen Sie während virtuellen Meeting-Sessions nur die Anwendungen und Dokumente, die für das jeweilige Meeting relevant sind, und vermeiden Sie es, den gesamten Desktop zu teilen. Darüber hinaus dürfen keine vertraulichen Dokumente auf den virtuellen Meeting-Server hochgeladen werden.

Diese Liste enthält Informationen zu wichtigen Themen.

Bitte beachten Sie, dass diese Liste nicht vollständig ist und auch alle allgemeinen Sicherheitsvorschriften gelten.

Weitere Informationen

Siemens globale Webseite

Zusammenarbeit mit Siemens