

CYBERSECURITY CARD

Secure Data Communication

IT Services for Secure Communication and Collaboration
of external Business Partner with Siemens

Definition

Business Partner (BP): in this context it is every external party with a business relationship to Siemens, without authorized access to Siemens Intranet (e.g. via Business Partner Access) and therefore with no access to Siemens internal IT Services.

Situation

The exchange of information with Business Partners is our daily business. In some cases, data and documents (like costs, contracts or technical documents) are classified as “confidential” or even “strictly confidential”. To ensure secure communication and collaboration of such information, this use case based IT Service overview has been created. It helps Siemens end user as well as their Business Partners to identify the

respectively adequate Siemens IT Service, to know where to order it and how to use it. Please, be aware that IT Services for specific business processes (e.g. electronic data interchange via EDI) are still leading and the overview should only cover remaining use cases (e.g. for which so far unencrypted email process has been used).

Threat

Non Disclosure Agreements (NDAs) and the Siemens [“Rules for Business Partners”](#) define the right handling of confidential information, but do not contain concrete IT solutions for the implementation of the regulations.

That leads to the risk that, although the Information Security requirements are known, they might not be implemented correctly or completely.

This list highlights important topics.

Please note, however, that the list is not exhaustive and that all general cybersecurity regulations also apply.














Behavior

What to consider as a business partner when sending an email with SecuFEx:

The Business Partner needs a temporary account for SecuFEx to send data to a Siemens employee. This temporary account can be created and administrated by each Siemens employee. Users of the SecuFEx service shall comply with all applicable national and international (re-) export control regulations.

What to consider as a business partner when receiving a virtual conference or MS Teams invitation from a Siemens employee:

The Business Partner must ensure that there are no prying eyes and eavesdroppers in the virtual meeting. Furthermore, the Business Partner is not allowed to make hardcopies or screenshots from the screen, if confidential information is shown. During virtual meeting sessions open only those applications and documents that are relevant to your respective meeting and avoid sharing the complete desktop. Furthermore, no confidential documents shall be uploaded to the virtual meeting server.

Use Case	Recommended IT Service	Max. Protection Class	Technical Prerequisites	User instructions and technical contacts
Once secure document exchange  We want to exchange once a document securely	Secure File Exchange (SecuFEx)	C2 – Confidential 	A temporary user account for sending files must be created by the Siemens business partner contact	SecuFEx Website →
Continuous secure document exchange  We want to exchange continuously documents securely	MS OneDrive	C2 – Confidential ¹ 	None	MS OneDrive Web Site →
Continuous secure data and document exchange  We want to exchange continuously data and documents securely	E-Mail Encryption	C3 – Strictly Confidential 	<ul style="list-style-type: none"> • Prerequisites → • Implementation Guide of Email encryption → 	Siemens PKI Website →
Secure collaboration  We want to work jointly on the same documents	SharePoint Global Collaboration Service-Portal Workspace Strictly Confidential / High Secure file share	C2 – Confidential  C3 – Strictly Confidential 	<ul style="list-style-type: none"> • PC settings • Mobile phone or token for authentication Please get in touch with your Cybersecurity officer Siemens contact	SharePoint Website → —
Secure collaboration around PLM  We want to work on same docs / data in PLM area , incl. Integrated, complex scenarios (e.g. Digital Twin)	Siemens Teamcenter (TC)	C2 – Confidential ² 	TC Supplier Collaboration Foundation (SCF) →	SCF Website →
Real Time Collaboration  We want to make a secure virtual meeting	MS Teams	C2 – Confidential ³ 	Meeting shall be provided by Siemens contact	MS Teams →

¹ Protection Class "Confidential" will be possible when all participants have an account on the Siemens tenant or the documents are properly protected with MIP. In all other cases, only Protection Class "Restricted" is possible.

² Depends on local installation and configuration, maximum up to "Restricted". Exact Protection Class needs to be verified with your Siemens contact.

³ Protection Class "Confidential" will be possible when all participants have an account on the Siemens tenant. When there is a participant without an account in Siemens tenant or a participant uses dial-in via telephone, only Protection Class "Restricted" is possible.

Further information (links):

[Siemens Global Webpage →](#)

[Collaborating with Siemens →](#)