Cybersecurity Card

Secure Data Communication

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

SIEMENS
Ingenuity for life

Use Case	Once Secure document exchange "We want to exchange once a document securely."	Continuous secure document exchange "We want to exchange continuously documents securely."	Continuous secure data and document exchange "We want to exchange continuously data and documents securely."	Secure collaboration "We want to work jointly on the same documents."		Secure collaboration around PLM "We want to work on same docs / data in PLM area, incl. Integrated, complex scenarios (e.g. Digital Twin)."	Real Time Collaboration "We want to make a secure virtual meeting."
Recommended IT Service	Secure File Exchange (SecuFEx)	MS OneDrive	E-Mail Encryption	SharePoint Global Collaboration Service-Portal	Workspace Strictly Confidential / Secure Data Room (SDR)	Siemens Teamcenter (TC)	MS Teams
Max. Protection Class	"Confidential"	"Confidential"[1]	"Strictly Confidential"	"Confidential"	"Strictly Confidential"	"Confidential"[2]	"Confidential"[3]
Technical Prerequisites	▪ A temporary user account for sending files must be created by the Siemens business partner contact.	▪ none	▪ Prerequisites ▪ Implementation Guide of Email encryption	▪ Technical prerequisites ▪ PC settings ▪ Mobile phone or token for authentication	▪ Mobile phone for authentication	▪ TC Supplier Collaboration Foundation (SCF)	▪ Meeting shall be provided by Siemens contact
User instructions and technical contacts	▪ SecuFEx Website	▪ MS OneDrive Web Site	▪ Siemens PKI Website	▪ SharePoint Global Collaboration Service Portal Website	▪ SDR Website	▪ SCF Website	▪ 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.

Cybersecurity Card

Secure Data Communication

SIEMENS
Ingenuity for life

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.

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.

This list highlights important topics.

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

Further Information

Siemens Global Webpage

https://www.siemens.com

Collaborating with Siemens

https://www.siemens.com/scm/collaboration