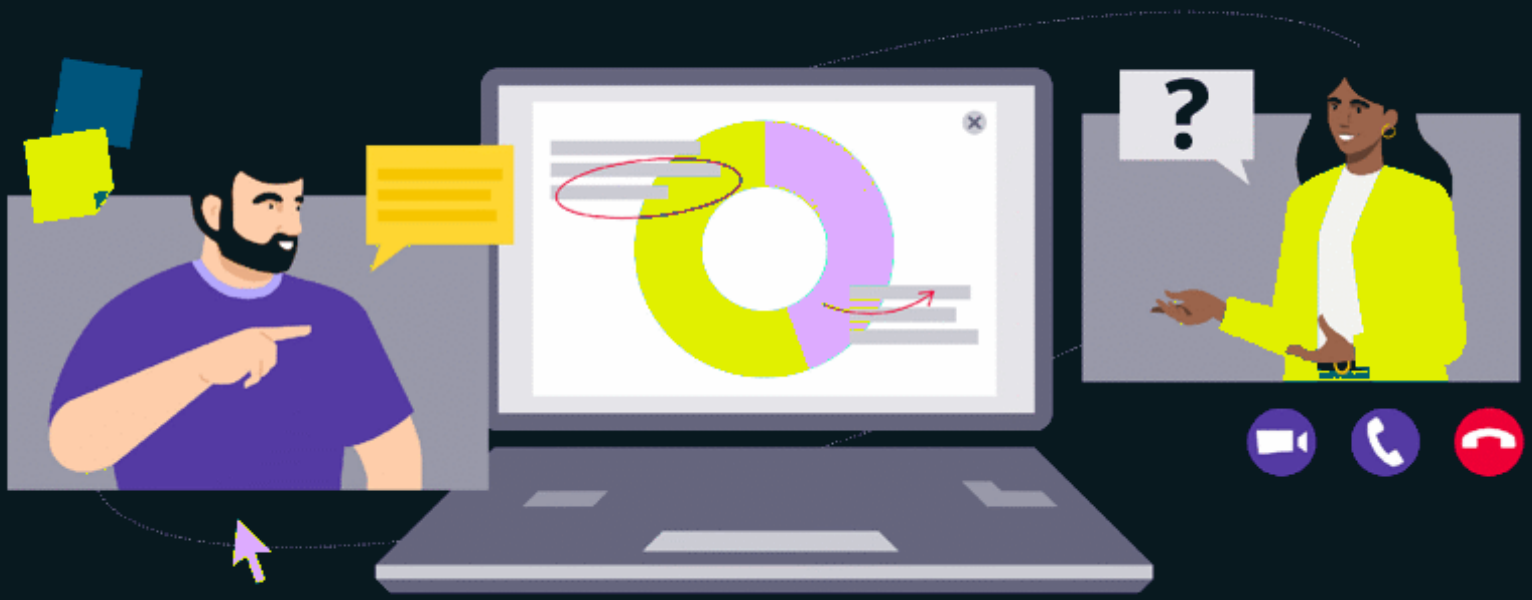

CYBERSECURITY CARD

Secure Data Communication:

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

Definition

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

C1 – RESTRICTED Data includes company information like circulars, instructions, policies, and directories, shareable with Innomotics employees and partners; operational data is assumed restricted unless differently labeled.

C2 – CONFIDENTIAL Data includes sensitive information like controlling data, contracts, source code, and design docs that could harm Innomotics if disclosed. Share only with those having a legitimate need.

C3 – STRICTLY CONFIDENTIAL Data (e.g., key tech records, financial results pre-release) could harm Innomotics; special protection is necessary as most employees do not handle 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 Innomotics' "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.

INNOMOTICS

Behavior

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

The Business Partner needs a temporary account for GlobalX to send data to an Innomotics employee. This temporary account can be created and administrated by each Innomotics employee. Users of the GlobalX service shall comply with all applicable national and international (re-) export control regulations. Read further here: Secure Data Exchange with GlobalX.

What to consider as a business partner when receiving a virtual conference or MS Teams invitation from an Innomotics 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.

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”. The table below contains case overview of processes for classifying IT assets. Thorough compliance of the case will ensure secure communication and collaboration of information. The table serves both Innomotics’ end users and Business Partners to identify the adequate IT Services, to know where to order it and how to implement them.

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 (GlobalX)	C2 – Confidential	A temporary user account for sending files must be created by the Innomotics business partner contact	GlobalX Website
Continuous secure document exchange				
 “We want to exchange **continuously documents *securely***	MS OneDrive	C2 – Confidential[1]	None	MS OneDrive Website
Continuous secure data and document exchange				
 “We want to exchange **continuously data and documents *securely***	E-Mail Encryption	C3 – Strictly Confidential	Please get in touch with your Cybersecurity Officer Innomotics contact	Digital ID | Innomotics
Secure collaboration				
 “We want to **work jointly** on the same documents	SharePoint Global Collaboration Service-Portal	C2 – Confidential	PC settings Mobile phone or token for authentication	SharePoint Website
	Workspace Strictly Confidential / High Secure file share	C3 – Strictly Confidential	Please get in touch with your Cybersecurity Officer Innomotics contact	
Real Time Collaboration				
 “We want to make a ***secure*** **virtual meeting**	MS Teams	C2 – Confidential[3]	Meeting shall be provided by Innomotics contact	MS Teams

[1] Protection Class ”Confidential” will be possible when all participants have an account on the Innomotics 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 Innomotics contact.

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

Further information:

Innomotics Global Website

Collaborating with Innomotics