

i Instructions

- 1 - We recommend that this questionnaire is completed with full input from the function in your organization responsible for Information / IT Security or IT (where a specific security function does not exist).
Note: **Un-answered questions** will be **treated as** being answered **No** when evaluating the response
- 2 - Return the questionnaire to DOMEL purchasing department.
- 3 - We will evaluate the response to the questionnaire and feed it into our supplier management processes
- 4 - Should you require further information, please do not hesitate to contact us.
Personal Data Privacy Policy ► <https://www.domel.com/privacy-policy>
- 5 - DOMEL reserves the right to perform information security audits for suppliers which poses Very High risk for DOMEL. A reasonable prior notice is sent, and audits are performed only during normal business hours.

🏢 Company Information

Company Name: _____

Registered Address: _____

CISO Contact Name: _____

CISO Contact Email: _____

🏷️ Information Security Certifications and Labels

1 - Does your company have been certified in Information Security Standards?

YES NO

*Please attach a pdf of the certificate.

2 - If yes, for which Standard?

ISO/IEC 27001 TISAX OTHER

Scope: _____

Details: _____

Certification Date: _____

If you have a Information Security certification or label, click on the End button,

End

otherwise complete the following Checklist:

Question	Answer	Comments
1.Information Security Policies		
Does your company have implemented cybersecurity policies, procedures, and standards based on industry standards (e.g., TISAX, ISO/IEC 27001 or similar)?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Are these policies reviewed in a regular intervals?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
2.Information Security Organization		
Does your company have a dedicated, full-time employee or subcontracted cybersecurity staff <u>thats is named, documented and known?</u>	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Are the roles and responsibilities clearly defined?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
3.Human Resources		
Do terms and conditions of employment clearly define information security requirements, including non-disclosure provisions for employees and contractors?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company conduct formal information security training for all users?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company conduct information security awareness activities for all users (e.g. awareness emails, newsletters, phishing simulations, questionnaires, others...)	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Are all users required to sign a confidentiality agreement?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
4.Asset Management		
Does your company maintain an inventory of all important information assets with asset owners clearly identified?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company have established a process for returning assets upon termination of employment or contract/agreement?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company have established a process to information classification and labelling practices?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company have procedures with regards to the handling, storage and disposal of information assets?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
5.Access Control		
Does your company have a access policy defined and implemented?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company conduct periodic checks on users' accesses to ensure their access matches their responsibilities?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company have established a process to remove the access upon employment or contract/agreement termination?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company have established a secure log-on procedure to control access to systems and applications?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company have established a procedures to control the access to network and network services?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company control web access based on the risk (e.g. reputation, content, and security) of the sites being visited (e.g. Web Proxy Controls)?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
6.Cryptography		
Does your company have a cryptography policy defined and implemented?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company protect sensitive information received from a third-party company during transmission, storage and sharing (i.e. Encryption, SSL/TLS connections)?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
7.Physical Security		
Does your company have a physical protection (including physical access) against external and environmental threats?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company have a visitor policy regarding registration, pickup and accompanying of visitors is implemented. There must be a visible distinction between a visitor and a regular employee while on secure areas (e.g. separately badge, name card)	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company have a clean desk policy implemented and it was shared with all users?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
8.Operations Security		
Are all devices that store or process sensitive information protected from the Internet by a firewall?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Do all devices that store or process sensitive information have commercially available antivirus with current signature files?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Do all devices that store or process sensitive information have a secure log on to access the system (unique user name and complex password)?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Do all devices that store or process sensitive information have vulnerability scanning performed regularly and are vulnerabilities being remediated?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Do all devices that store or process sensitive information have all unnecessary ports and services disabled?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Do all devices that store or process sensitive information have patches deployed for high risk operating system and third-party application vulnerabilities?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Are all laptop devices that store sensitive information encrypted?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Do all mobile devices (e.g. smartphones, tablets) that store sensitive information have configuration management by IT specialist?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Do all mobile devices (e.g. smartphones, tablets) that store sensitive information have the ability to remotely wipe the device?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company perform logging and monitoring on devices that store or process sensitive information?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company have established a policy for backup of information and information systems and it is tested regularly?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company have established rules for the software installation by users?	<input type="checkbox"/> YES <input type="checkbox"/> NO	

9. Communications Security

Does your company control and manage the network to protect information in systems and applications?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company have implemented network segregations?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company have implemented procedures and controls to protect the transfer of information by all types of communication facilities?	<input type="checkbox"/> YES <input type="checkbox"/> NO	

10. System acquisition, development and maintenance

Does your company includes Information security requirements when acquiring , develop or maintain an information system?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company have a system change control procedures in place?	<input type="checkbox"/> YES <input type="checkbox"/> NO	

11. Supplier Relationship

When your company share sensitive information with suppliers, does your company require those suppliers to follow policies, and procedures for cyber security?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company require a confidentiality or non-disclosure agreements before sharing sensitive information with suppliers?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company perform cybersecurity audits on 3rd parties IT systems/devices and IT services that store or process sensitive information ?	<input type="checkbox"/> YES <input type="checkbox"/> NO	

12. Incident Management

Does your company have capabilities of detecting and blocking malicious e-mail prior to delivery to the end user?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company have a Computer Incident Response Team (CIRT) with a formal process to respond to cyber attacks?	<input type="checkbox"/> YES <input type="checkbox"/> NO	

13. Business continuity

Does your company have a Business Continuity Policy with clear roles and responsibilities?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company have a contingency plans in place to address loss of key personnel, recovery from loss of manufacturing capacity or capability, disruption of delivery from a critical supplier, and loss of IT systems?	<input type="checkbox"/> YES <input type="checkbox"/> NO	

14. Compliance

Does your company have implemented procedures to ensure compliance with intellectual property rights and use of proprietary software?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company implement process and procedures to protect personal information according to relevant legislation and regulation (e.g. GDPR)?	<input type="checkbox"/> YES <input type="checkbox"/> NO	
Does your company perform a regular information security reviews/audits?	<input type="checkbox"/> YES <input type="checkbox"/> NO	

Cybersecurity Maturity Level	0%	
-------------------------------------	-----------	--

✓ Responder details

Responder Name: _____
Function: _____

Thank you for your collaboration, **please send your response** to DOMEI purchasing department.