CYBERCAMPUS SVERIGE

Checklist - basic cybersecurity

Organizational security measures		Yes	No	Insufficient
	Permissions (read, write, none)			
	Storage (knowing where, how, who's responsible)			
	Safety copy (routines)			
	Shareing (sensitive, business-critical, public)			
	GDPR (knowledge of)			
	Education (SME security protection coordinator) and various staff training in cybersecurity			
	Policies (information management)			
	Data Protection Officer (DPO)			

Awareness

	Understanding the impacts of corporate cybersecurity (or lack thereof) e.g., costs, breaches, customer credibility, etc.			
	About the benefits of investing in cybersecurity as a competitive advantage.			
	About the most common risks and approaches, e.g. vulnerabilities in value chains.			
	About the most common and simplest measures that I as an individual or company can take to reduce the risks of being exposed to digital crime.			

Knowledge

	About digital threats and their consequences.			
	About the most common methods and approaches linked to digital crimes, such as phishing and ransomware attacks.			
	About the simplest and most effective measures to reduce the risk of being a victim of digital crime.			
	About relevant legislation and the requirements placed on operations when it comes to cybersecurity.			
	About continuity management to maintain operations regardless of events.			

Activities

	Gain practical skills in securing networks, managing endpoints, and incident management.			
	Implement the simplest and most effective measures to reduce the risks of digital crime, such as reviewing and administering permissions.			
	Act in such a way that the risk of being a victim of digital crime is greatly reduced and take simple measures to reduce the effect of having been a victim of a crime that has been committed.			
	Conduct basic information classifications and risk analyses.			
	Continuity management to maintain operations regardless of events.			
	Action plan if you are affected by cyber intrusions, digital crimes and fraud.			
	Actions in the event of a possible incident, which actions should be taken by users and service providers respectively.			

CYBERCAMPUS SVERIGE

Technical security measures		Yes	No	Insufficient
Hardware				
	Passwords (strong, unique, passphrase)			
	Encryption (Bitlocker), encryption service that has been activated on all computers			
	Updates (units, security updates)			
	Two-factor authentication (whenever possible)			
	Support (outsourcing, employed)			
	Training (for IT support)			
	Knowledge acquisition (self-learning)			
	Antivirus protection on employee mobile phones			
Software				
	Applications (from approved suppliers)			
	Antivirus programs (scheduling)			
	Updates (all programs, security updates)			
	Two-factor authentication (whenever possible)			
	Passwords (strong, unique, passphrase)			
	VPN (server, software) VPN- solution that secures data traffic for employees who work from locations outside company's premises			
	Support (outsourcing, employed)			
	Knowledge acquisition (self-learning)			
	Secure digital platforms, web pages and payment solutions.			
Network				
	Passwords (strong, unique, passphrase)			
	Router (complete control, at ISP)			
	Updates (units, security updates)			
	Firewall (activated, configured)			
	Public networks (policy)			
	Guest networks (WiFi)			
	Support (outsourcing, employed)			
	Knowledge acquisition (self-learning)			
Cloud services				
	E-services (established cloud services)			
	E-mail (established e-mail services)			
	Digital mailbox (Kivra, government mail)			
	Two- or multifactor authentication (whenever possible)			
	Agreements (incidents, responsibility for actions)			

CYBERCAMPUS SVERIGE

Education

	Yes	No	Insufficient
Do you currently have personal training in cybersecurity or information security?			
If yes: briefly describe their contents and formats			
	Introductory/ basic level	Continuation level	Advanced level
How many of your employees need the various levels of cybersecurity training? Please provide an approximate number.			
Do you need training aimed at a specific target group (e.g. procurement managers, managers)? Describe which ones.			

	A few hours	A day	Several days	Longer
What workload can training entail?				
	Physical	WEB-based with physical meetings	Online with real-time parts	Completely online, self study
What format would you like to receive training in? Multichoice is possible.				
	Swedish	English		
Which language do you prefer for teaching?				
	Swedish	English		
Which language do you prefer for course material?				
	Yes	No		
Is it important that your employees can work at their own pace and according to their own plan?				
	Yes	No		
Is it important that your employees get to test their knowledge in the courses?				
	Yes	No		
Is it important to use your own case studies in the courses?				
	Yes	No		
Is it desirable to organize study groups among your employees?				
	Yes	No		
Is it desirable for your own experts to participate in the training?				

	Yes	No
Is it important that you/your employees can influence the course content?		
	Yes	No
Is it important that your employees receive repetition and updating of course content after the course ends?		
	Yes	No
Would it add anything if the training ended with a test and a certificate?		
	Yes	No
Is it desirable to have formal credits such as HP/ECTS?		
	Yes	No
Is it important that your employees complete the training they have started?		