Incident Response: Checklist for SMEs

An incident response plan defines the procedure and responsibilities in the event of a (suspected) IT security breach.

Work through and define the following points and record the results in writing. The resulting incident response plan should always be available to everyone involved - even if secure access to your IT systems is not possible.

1.	**Preparation**	
	Define responsibilities for IT and IT security	
	Create a contact list with responsibilities, authorisations, and availability	
	Ensure external support for security incidents if required	
	Inventory of IT systems and resources	
	Identify business-critical assets and processes	
	Threat modelling: prioritising risks and vulnerabilities	
	Creating and publishing initial measures for IT security incidents	
	Define internal and external communication processes (e.g. media)	
	Prepare external reporting channels for security incidents	
	Establish an alternative communication channel	

2.	**Mastering**	
	Contact and inform all defined contact persons	
	Ask affected users (what, when, where, how?)	
	Document relevant facts	
	Collect and save system logs, log files	
	Inform affected persons (employees, customers/partners if applicable)	
	Comply with reporting requirements	

3.	**Follow-up**	
	Closing discovered security gaps or vulnerabilities	
	Close monitoring of network and IT systems	
	Review and optimisation of existing policies, procedures, and measures	
	Update emergency management documentations	
	Enhance the IT security architecture	

This checklist can serve as a starting point for smaller companies in creating an effective Incident Response Plan. The listed measures not only help strengthen defence and detect potential security incidents early but also enable an effective response in case of emergencies to minimize potential damages, quickly restore business operations, and strengthen cyber resilience in the long term.

Helpful links:

Threat Modelling: Guidelines for creating practical threat models

Incident Response: Guide to Managing IT Security Incidents

About IKARUS Security Software GmbH

Since 1986, the Austrian private company IKARUS Security Software has been developing and operating leading Cyber Security technologies. With efficient cloud solutions, Incident Response services, a modular Threat Intelligence platform, and services for securing critical infrastructures, IKARUS protects companies of all sizes.

IKARUS' proprietary Malware Scan Engine and Austrian data center ensure full transparency and security in data processing. Customers also appreciate the personalized technical support directly from the manufacturer.