Information Security Event / Incident Report Form

Version: 1.01 | 29th of January 2020

Purpose: This document serves as a template and is adjustable to your own needs. You can fill it out on paper or use it on your computer.

Audience: Digital first responders, IT-security and computer forensic experts. Everyone who needs to report an IT event / incident.

DigiTrace GmbH
Zollstockgürtel 59
50969 Köln
Tel.: +49 221 6778695-0
info@digitrace.de
www.DigiTrace.de

Information Security Event / Incident Report Form

No. 7. - 19. only applicable when Event is escalated to an Incident

1. Basic information on the security event / incident			
1.1 Date & time the event occurred		1.2 Date & time the event was discovered	
1.3 Date & time the event was reported		1.4 If the event is over, how long did it last?	

2. Event number / ID		3. Related events / incidents ID (if applicable)	

4. Details on reporting person			
4.1 Name		4.2 Address	
4.3 Organization & department		4.4 Phone number & e-mail-address	

5. Digital first responder			
5.1 Name		5.2 Address	
5.3 Organization & department		5.4 Phone Number & e-mail-address	

Information Security Event / Incident Report Form

No. 7. - 19. only applicable when Event is escalated to an Incident

6. Information security event / incident description	
• What? When? Where? How? (Why?) • Initial views on components / assets affected • Adverse business impacts • Identified vulnerabilities • Pictures & screenshots of the event and its impact (if taken)	

7. Information security incident details	
7.1 Date & time the event was classified as an incident	
7.2 Reason why the event was classified as an incident	

8. Category Examples: Theft, hacking, exfiltration, malware, ransomware, technical fault, human error, environmental damage classify, if actual or suspected incident	

Information Security Event / Incident Report Form

No. 7. - 19. only applicable when Event is escalated to an Incident

DigiTrace
Kompetenz in IT-Forensik

9. Components / assets affected Example categories: Information / date, hard- / software, communications, processes … (use serial and version numbers etc.)	

10. Adverse Business Impacts

(Confidentality, Integrity, Availability, non-repudiation)

Short description of effects:

- Financial loss / disruption of business process **(FD)**
- Loss of protection of commercial and economic interests **(CE)**
- Loss of personal data **(PA)**
- Violation of legal and official obligations **(LO)**
- impairment of management and business processes **(MB)**

	Scale 1 (min.) to 10 (max.)	Impact (short description)	Costs
Loss of confidentiality			
Loss of integrity			
Loss of availability			
Breach of obligations			

10.1 DSGVO / GDPR	
10.1.1 Is personal data affected?	☐ Yes ☐ No ☐ Unclear
10.1.2 GDPR expert consulted?	☐ Yes ☐ No, why:
10.1.3 Respected the notification obligation (72h)?	☐ Yes ☐ No, why:

11. Rough estimation of costs				
11.1 Rough estimation of financial damage (mark one per column)		Now / today	Soon	Future
	Low			
	Medium			
	High			
11.2 Rough estimation of recovery costs				
11.3 Rough estimation of budget				

12. Incident resolution			
12.1 Incident investigation commenced date		12.2 Investigator(s) / company name	
12.3 Incident end date		12.4 Incident impact date	
12.5 Investigation completion date		12.6 Reference and location of investigation report	

13. Insurance coverage in your company	
13.1 Does your organisation have insurance coverage?	☐ Yes ☐ No
13.2 Did you check for obligations against your insurance company?	☐ Yes ☐ No
13.3 Did you fulfill the obligations?	☐ Yes ☐ No, how + why:

14. Description of perpetrator (if applicable) e.g. person, institution, group, accident, human failure, natural elements, technical failure … Perceived / actual motivation, e.g. pastime, political, criminal, revenge …	

15. Actions PLANNED to resolve incident (outstanding)	

16. Conclusion Major / minor incident? Justify!	Major / minor incident, because ...

17. Internal entities notified e.g. CSIRT manager, CIO, CISO, report originator		18. external entities notified e.g. police, consultants, lawyer, PR, data protection officer	

19. Actions TAKEN to resolve incident					
No.	Date / time	Who?	Action / activity	State / next steps	Costs

Sign-Off Originator Name, role, date and signature:	**Sign-Off Reviewer I** Name, role, date and signature:	**Sign-Off Reviewer II** Name, role, date and signature: