

# First Response Checklist

## First Response by Non-forensics Staff

1. Whether the non-forensics staff is responsible for protecting the crime scene	<input type="checkbox"/>
2. Whether the forensic team keeps the crime scene remain in a secure state	<input type="checkbox"/>
3. Whether there are notes and photographs of the crime scene and those present	<input type="checkbox"/>
4. Whether the crime scene evidence is handed over to the attending forensics team	<input type="checkbox"/>
5. Whether the surrounding areas linked to the incident are secured	<input type="checkbox"/>
6. Whether there is enough security for computing systems or other electronic devices	<input type="checkbox"/>

## First Response by System/Network Administrators

1. Whether the administrator has reported the incident according to the current organizational incident reporting procedures	<input type="checkbox"/>
2. Whether the administrator performed any action unless directed to do so by the incident manager assigned to the case	<input type="checkbox"/>
3. Whether the admin is responsible for the monitoring and maintenance of the system as well as the network	<input type="checkbox"/>
4. Whether the admin is recording what is on-screen if the computer is switched on during the incident investigation	<input type="checkbox"/>
5. Whether the administrator has transferred the copies of system logs onto a clean media	<input type="checkbox"/>
6. Whether there is any approval from the top management before powering down any computing systems, if an ongoing attack is detected	<input type="checkbox"/>
7. Whether the computing systems or other digital devices are isolated from further use or tampering	<input type="checkbox"/>
8. Whether the administrator has documented every detail relevant to the incident	<input type="checkbox"/>
9. Whether the administrator has explained the security protocols and procedures followed for using the systems and storage media to the incident responder	<input type="checkbox"/>

10. Whether the administrators are present during the legal proceedings to explain the measures taken during the first response phase	<input type="checkbox"/>
---	--------------------------

### First Response by Laboratory Forensics Staff

1. Whether the laboratory forensics staff has documented the electronic crime scene	<input type="checkbox"/>
2. Whether the laboratory forensics staff has collected incident information at the crime scene to provide the basis for the forensic investigation	<input type="checkbox"/>
3. Whether there are any individual interviews conducted to verify if a crime has occurred and the nature of the incident	<input type="checkbox"/>
4. Whether there is a proper plan for the search and seizure activity to ensure that the investigating team has proper authorization and guidelines	<input type="checkbox"/>
5. Whether the investigating team has obtained consent to begin the investigation process	<input type="checkbox"/>
6. Whether the investigating team has taken witness signatures to begin the investigation process	<input type="checkbox"/>
7. Whether the investigating team has obtained a search warrant for search and seizure activity	<input type="checkbox"/>
8. Whether the laboratory forensics staff has identified and collected electronic evidence	<input type="checkbox"/>
9. Whether the forensics staff has conducted an initial search of the crime scene	<input type="checkbox"/>
10. Whether the forensics staff has secured and evaluated the crime scene	<input type="checkbox"/>
11. Whether the forensics staff has seized the	<input type="checkbox"/>
12. Whether the forensics staff is documenting and enlisting the evidence at the time of packaging all collected electronic evidence	<input type="checkbox"/>
13. Whether the staff has labelled all the containers appropriately and following the exhibit numbering during packaging	<input type="checkbox"/>
14. Whether the staff has filled the panel on the front of evidence bags with proper details	<input type="checkbox"/>
15. Whether the staff has avoided folding and scratching of storage devices during packaging	<input type="checkbox"/>
16. Whether the staff has labelled the containers that hold the evidence in an appropriate way	<input type="checkbox"/>

17. Whether the incident responders has taken special precautions for transporting electronic evidence	<input type="checkbox"/>
18. Whether there is a policy to ensure proper handling and transportation of evidence to the forensics laboratory	<input type="checkbox"/>
19. Whether there is a strict chain of custody to keep track of all the forensics processes applied	<input type="checkbox"/>

### First Responder Common Mistakes

1. Whether the administrator have properly handled computer crime security incidents as they do not have complete knowledge of the forensic investigation process	<input type="checkbox"/>
2. Whether the forensic team has shut down or rebooted the victim's computer	<input type="checkbox"/>
3. Whether the forensic team have assumed that some components of the victim's computer are reliable and usable	<input type="checkbox"/>
4. Whether the forensic team is not having access to baseline documentation about the victim's computer	<input type="checkbox"/>
5. Whether the forensic team has failed to document the data collection process	<input type="checkbox"/>