Check List – IT Incident Immediate Measures

Immediate measures are needed to limit damage and are the first incident management measures to be taken.

Which immediate measures should be taken depends on which infrastructure components, systems, applications and services are affected.

Legend

 Task, Check

 Activity

General Measures

Checking the impact

 Which IT resources (systems, applications, services) are affected?

 Which users are affected?

 Are business critical systems, applications or services affected?

 Is an outsourcing partner involved?

 Is it cyber attack?

 Is it a fraud or an illegal act?

 Update damage (impact) in the Incident Management Tool.

 If business critical systems, applications or services are affected or an outsourcing partner is involved, the IT incident manager should be informed immediately.

 If it is a cyber attack, the IT Security Officer and the Computer Security Incident Response Team (CSIRT) should be informed immediately.

 If there is a suspicion of fraud or unlawful acts, the Legal & Compliance department and the Computer Security Incident Response Team (CSIRT) should be informed immediately.

Sensitive Data

- The IT incident manager assesses what kind of information is affected.
  - Are confidential or secret data affected?
  - Are personal data or special personal data affected?
- In the case of confidential information, the Legal & Compliance department, the data protection and the owner of the data should be informed immediately. The Legal & Compliance department and the data protection will decide on the next steps.
- In the case of personal data, the data protection officer should be informed immediately. The data protection officer will decide on the next steps.
- Updating the information classification in the Incident Management Tool.

Communication

- The affected users should be informed promptly and continuously updated the incident is closed and normal operation restored.
- If sensitive information is affected or there are special circumstances, such as a cyber attack, communication requires great care.
- The IT incident manager Information is responsible for the internal communication. Media Relations is responsible for external information.
- The external and internal communication should be coordinated and information should be provided at the same time.
- Information of the affected users by the IT Service Desk according to instruction by the IT incident manager.
- Internal communication by the IT incident manager.
- External communication (public and media) by Media Relations.

Incident Coordination

- The IT incident manager informs senior management if necessary.
- The IT incident manager engages external specialists if required.

- The IT incident manager contacts all permanent members of the incident management team or their deputy and the ad hoc members as required and informs them about the IT incident.
- The IT incident manager organizes incident team conference calls to check the status and progress and to keep all members of the incident management team informed.
- The IT incident manager informs the IT Service Desk to keep users informed.

Specific Measures

Suspicion of fraud or unlawful acts

- Legal & Compliance authorizes the Computer Security Incident Response Team CSIRT to perform investigations.
- The Computer Security Incident Response Team (CSIRT) conducts the investigations in accordance with the mandate of the IT incident manager and within the scope authorized by the Legal & Compliance department.
- The IT incident manager informs the incident management team that the Computer Security Incident Response Team (CSIRT) has been tasked with investigating.
- The Computer Security Incident Response Team (CSIRT) documents the results of the investigation in detail. Chain of custody should be maintained and documented in the CSIRT logbook to enable the traceability and verification of authenticity and integrity.

Cyber Attack

- If a cyber attack is suspected, the IT incident manager informs the Computer Security Incident Response Team (CSIRT).
- In the event of a cyber attack, the Computer Security Incident Response Team (CSIRT) takes over the management and responsibility for IT incident management.
- If there is a suspicion that the cyber attack was carried out by FTS employee(s), the investigations by the Computer Security Incident Response Team (CSIRT) should be approved by the Legal department. The necessary immediate measures to limit damage are explicitly excluded.

- The Computer Security Incident Response Team (CSIRT) takes the necessary steps to mitigate damage.
- The Computer Security Incident Response Team (CSIRT) informs the IT incident manager on an ongoing basis (at least twice a day) about the status and progress of the measures initiated.
- For detailed instructions, please see the CSIRT Manual.

Network Outage

- The IT incident manager contacts the network team to determine which areas of the FTS network are affected.
- The IT incident manager instructs the IT Service Desk inform the affected users about the network outage. If electronic communication is not possible other information way phone calls, SMS, etc. should be considered.
- The network team investigates the cause of the network failure and initiates recovery measures.
- The network team checks to see if all systems affected by the network outage have been restarted and that any damage such as data loss has been repaired.

Power Outage

- The IT incident manager contacts the infrastructure manager to determine which IT systems are affected by the power outage.
- The IT incident management team instructs the IT Service Desk to inform users of an IT systems affected by the power outage.
- The infrastructure manager informs the IT incident manager as soon as the power outage is resolved.
- The IT incident management team verifies that the systems affected by the power outage have been restarted and any damage such as data loss has been repaired.