Check List – IT Incident Recovery Measures

The recovery measures serve to return from emergency operation to normal operation.

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

Legend

 Task, Check

 Action

General Recover Measures

 Information on the immediate measures already taken and the current status of emergency operations

 Create a list of recovery measures to be taken, including the schedule, which is used for the status messages to the IT incident manager

 Replacement of defective hardware

 Restoring network connections

 Installing the system software (operating system, middleware, etc.)

 Installing the application software

 Restore data from backup

 Functional test of the application

 Checking the data for correctness, completeness, and up-to-dateness

 Notification of successful recovery to the IT incident manager

 Checking network connections and communication with other systems and applications

 Ask users if the problem has been resolved

- Notification of successful recover of normal operation to the IT incident manager

Specific Recovery Measures

Sensitive Data

- If sensitive data is affected, the instructions of the IT incident manager, Legal & Compliance department, and the data protection officer should be followed.

Cyber-Attack

- If, in the course of the recovery measures, it turns out that a cyber attack was carried out by FTS employee(s), investigations by the Computer Security Incident Response Team (CSIRT) should be approved by the Legal & Compliance department.
- 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 recovery measures until normal operation is restored.
- For detailed instructions, please see the CSIRT Manual.

Communication

- Communication always should be approved by the IT incident manager. The IT incident manager decides what is communicated internally and coordinates external communication with media relations.

Suspicion of fraud or unlawful acts

- In the event of suspicious activities, a fraud, or unlawful acts, the instructions of the IT incident manager and the Legal & Compliance department should must be followed.
- In such a case, the lead is with the Computer Security Incident Response Team (CSIRT).