Cyber security incident response plan

Follow the following steps in their order when a cyber security incident occurs:

1. Procedure

Step 1: Detection and Identification

- Document the incident
  A user or IT staff may detect and report a cyber security related incident (such as hacking or breach incident) to the helpdesk. ITServ staff responsible for the system security has to document the incident. The document should mention, among others, date and time of incident, location of the incident, description of the incident (such as what happened, what types of personal information involved), how was the incident detected, what systems (e.g. devices, email accounts, databases, worksites, etc.) have been affected by the
  Incident (if known), any evidence of the incident (e.g. computer logs, screenshots, relevant emails etc.)
- Report the incident to the IT services head of intERLab
- The security team analyses the report and determine the type of cyber security incident (such as data theft, a network attack, or a combination of threats) and its impact (application or services affected and its severity, data compromised or lost)

Step 2: Containment

- Prepare the right tools and staff to handle the containment.
- Take following actions to contain it:
  In the short term: shutting down programs or systems and disconnecting from networks
  In the long term: updating protections as needed, reviewing and strengthening access credentials as
- Identification and quarantine of any planted codes/malware discovered

Step 3: Remediation

- Eliminate whatever caused the incident and start working on repairing the damage.
- Ensure all artifacts of the incident have been fully removed from the system
- Repair or update systems as needed
- Check that all software patches are up-to-date, and protections strengthened
- Ensure backups are in place and functioning properly

Step 4: Recovery

Once the threat has been eliminated and the damage repaired, start to return to the normal operation:

- Monitor the affected system continuously to ensure that the incident has been fully resolved and that no further potential threats were detected.

- Test all systems for remaining or new vulnerabilities caused by the incidentb or the remediation process
- Restore the systems from backup and resume normal operations.

Step 5: Assessment

Compile a report of the incident using the documentation of each step that was taken in the incident response. The document shall have to include the following:

What happened?
How was the system hacked?
What preventive measures have been taken/are needed?
Are more changes needed to secure the systems?
Who needs to be included in changes or new prevention strategies?

This plan shall be reviewed at least once a year by responsible person(s) in ITServ and endorsed by the IT Committee.

2. Minimizing security related incidents

In order to minimize security related incidents, all computers, computer systems, computer networks and electronic communications devices must be updated with the latest but stable patches released by the respective vendors.

In relation to patches, the following procedure shall be followed:

- Those responsible for each system, device and application must monitor relevant sources of information which may alert them to a need to act in relation to new security vulnerabilities.
- Patches must be obtained from a known, trusted source.
- The integrity of patches must be verified through such means as comparisons of cryptographic hashes to ensure the patch obtained is the correct, unaltered patch.
- Patches must be tested and assessed before implementation in a production environment to ensure that there is no negative impact as a result.
- A backup of the production systems must be taken before applying any patch.
- An audit trail of all changes must be created and documented. Those responsible for each system must verify that the patches have been installed successfully after production deployment.
- Production patches must be deployed regularly