

Incident Response

The institution shall have an operational incident-handling capability for institutional systems, including preparation, detection, analysis, containment, recovery, and user response activities.

The institution shall notify the public authority in charge of cybersecurity about every incident. This also pertains to the incidents that can be handled by the institution itself. If the institution cannot handle the incident and/or the incident concerns critical public safety, the institution shall request support from the appropriate public authority.

The institution shall have documented and implemented procedures for responding to cybersecurity incidents.

The procedures shall include at least:

- Reporting information security incidents,
- Planning and preparing to respond to incidents,
- Monitoring, detecting, analyzing and reporting events and incidents related to information security,
- Response, including escalation, supervised post-incident recovery and internal and external communications.
- The public institution shall ensure that incident-handling capability is supported at the appropriate level by human, technical, information and financial resources.

Revision #2

Created 11 July 2025 15:20:39 by RISA

Updated 11 July 2025 18:49:45 by RISA