Incident Response Plan

# Annotation

All educational facilities can use this strategic document, they can also extend and modify the strategic document according to the current situation in the area of setting up security policies within school ICT infrastructures.

## Importancy of the Risk management plan

It is very important that educational institutions are prepared for attempts to steal data or attempt to penetrate internal networks. School staff, work partners, school leaders, as well as teachers, should have at least general knowledge and minimization of cyber risks. Understanding these incidents is particularly valuable in defining strategic preventive measures, but also in mitigating the effects of cyber attacks. For example, to recognize the difference between network attacks and data theft is also very valuable in providing accurate communication during a crisis situation. Similar skills should not only be available to school staff, but also to pupils and students of educational establishments.

 In relation to the steady increase in cyber attacks, it will be necessary for educational establishments to have clearly defined steps to act legally and effectively in case of cyber threats. No crisis plan can be successful without clearly defined roles and responsibilities. To prepare the plan must be invited by all the partners who cooperate with that educational establishments in the field of ICT. In case the training facility uses the services of an external entity / outsourcing, etc., it is appropriate to invite these partners to participate in the risk management plan. Other recommended subjects are:

1. Internet provider
2. Cloud service provider
3. Network administrators and providers
4. External hardware and software vendors
5. External security technicians
6. Educational staff

All these entities then work together to identify risks, prepare safety procedures and continually assesses the quality of the crisis plans and take measures to minimize risks.

### The risk management plan should include the next segments:

* Identify potential risks and implement appropriate risk mitigation strategies.
* Preparing for new, not yet described, cyber attacks, and continually updating the risk management plan.
* Procedures to verify that incidents have actually occurred.
* Clear communication rules and procedures that determine what is to be communicated to and in what timeframe. It must be clear from the communication what incident has occurred and what steps are being taken to mitigate the incident.
* Possible use of communication templates that can be used in case of threat. Communication templates can be created for the most risky incidents to save time.
* Active safety audit that can determine how the incident occurred, can identify vulnerabilities and potential ongoing risk.
* Clearly defined strategies to ensure that risk does not continue.
* An evaluation system set up to improve security measures.
* Continuous Education Plan for Employees / Educators etc. in the field of cyber security.
* Compliance with the Cyber Security Law

The next step is to describe the incidents that may occur. And developing detailed action plans for every risk situation.

### The most common incidents include:

* Denial of service (DoS), Distributed Denial of Service (DDoS)
* Disruption of standard computer system activity by malware or other hostile software.
* An unauthorized access attempt.
* Data theft or damage.
* Abuse of services and information.

## Scheme for promoting ICT security in schools

**RULES ENFORCEMENT**

**Modern digital technology, internal network tools.**

Directives Technical

Orders means

Policies

**EDUCATION CONTROL**

Training Sanction

Awareness Audit