ISO/IEC 27001:2013 Information security management systems
-Management of information security incidents (1)-

Security category – 16.1. Management of information security incidents and improvements

Control – 16.1.1. Responsibilities and procedures
There should be responsibilities and procedures in place to respond effectively and in time to information security incidents.

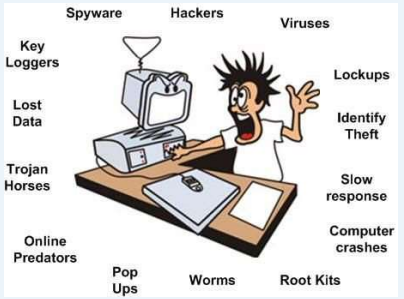
Consider the idea of creating a list of potential security incidents.

There should be procedures in place to ensure that security incidents are reviewed and investigated:
- planning and preparation of incident response
- monitoring, detecting, analyzing and reporting security events and incidents;
- logging incident management;
- handling of forensic evidence collected;
- escalation of incidents and recovery from an incident.

ISO/IEC 27035 - incident management.

ISO/IEC 27001:2013 Information security management systems
-Management of information security incidents (1)-

Control – 16.1.2. Reporting information security events
The organization is required to establish communication channels for reporting security events as quickly as possible.



What can be considered a security event that needs to be reported:

- a security control that is not effective;
- human errors;
- a virus detected on a system;
- breaches of physical security leading to theft;
- passwords being exposed;
- hardware or software that is not functioning correctly;
- uncontrolled system changes;
- unauthorized access to systems;
- non-compliance with legal requirements or procedures …

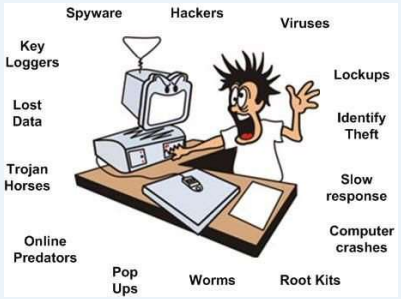
A security event can be considered anything that can result in loss or damage to assets or an action that is against the security policies of the organization

ISO/IEC 27001:2013 Information security management systems
-Management of information security incidents (1)-

Point of contact – a person or department where events are being reported and that is the first line of response to the incident.

All personnel should be aware of the contact point identity.

The reporting of events should be standardized and all staff should be advised to report events as soon as possible



ISO/IEC 27001:2013 Information security management systems
-Management of information security incidents (1)-

Control – 16.1.3. Reporting information security weaknesses
All employees and contractors need to be trained to report any security weakness – be it observed or suspected.

Weaknesses need to be reported to the point of contact to prevent information security incidents.

The reporting mechanism has to be easy, accessible and efficient.

All users should understand that they are required to report any weaknesses and not try to test the weaknesses to be sure or exploit them.