SECURITY INCIDENT MANAGEMENT

1.1 Identify and respond to information security incidents

1.1.1 Establish incident response procedures and responsibilities

Policy
All staff will be trained to identify information security incidents and will be trained in the appropriate response.

Guidelines

- Security incidents may include, but are not limited to:
    - virus infections.
    - hacking attempts.
    - system failures and malfunctions or loss of services.
    - data corruption.
    - unauthorised disclosure of information.
    - loss or theft of data or information.
    - transfer of sensitive or confidential information to those who are not entitled to receive that information.
    - attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system.
    - unwanted disruption or denial of service to a system.
    - unauthorised use of a system.

1.1.2 Report information security events as quickly as possible

Policy
Events that result in the actual or potential loss of data, breaches of confidentiality, unauthorised access, changes to systems or unusual or suspicious behaviour will be reported immediately.

Guidelines

- All actual or suspected security incidents must be reported immediately to the Technical Manager or CEO, by email or telephone or in person.
- They will log the incident and notify relevant employees and the information owner and will initiate the escalation process, where necessary.
- All Security events must be recorded within Linear (project management software), under the Security Incidents project.

1.1.3 Identify and report all information security weaknesses

Policy
Any security weakness that is found within Xyris information systems, either applications or system, will be reported.

Guidelines

- The following information is to be supplied when reporting a security weakness:
    - Contact name and phone number of person reporting the incident.
    - The type of data or information involved.
    - Whether the loss of the data puts any persons or other data at risk.
    - Location of the incident.
    - Date and time the security incident occurred.
    - Location of data or equipment affected.
    - Type and circumstances of the incident.

    - The immediate manager should also be informed to enable them to investigate or assist in investigating the incident and apply the appropriate actions. The outcomes of these actions are to be included in the incident report.
- Security weaknesses must be notified via email to incident.reports@xyris.com.au.

1.1.4 Assess security events and decide if they are incidents

Policy

All security events reported will be assessed and determined if a classification of the security events should proceed as a security incident.

Guidelines

- All reported security issues should be identified as a security incident and thus classified. An identified security incident could be an incident of, and not limited to:-
    - suspicious system and network activities.
    - compromise of sensitive or classified data.
    - unauthorised access or attempts to access a system.
    - emails with suspicious attachments or links.
    - denial-of-service attacks.
    - ransomware attacks.
    - suspected tampering of electronic devices.
    - application version in use with a detected or known vulnerability.
    - operating system in use with a detected or known vulnerability.
- All identified incidents will be assessed to determine the classification of the incident. Incidents are to be classified as:-
    - Security incident:
        - Incident that has occurred.
        - Incident that is in progress.
    - Security Weakness:
        - Identified security concern that requires investigation.

- An incident, once the event has been identified and observed, can be allocated a priority that allows for the determination of the appropriate incident handling process.
    - System Impact.
    - Information Impact.
    - Time to Recovery.
- All results of categorisation, prioritisation and findings are to be updated in the Linear ticket created against the security incident and recorded in the post-mortem.

16.1.5 Follow procedures to respond to security incidents

Policy

A Xyris employee will be assigned as the owner of the categorised security incidents ticket in Linear and will be responsible for all responses regarding the incidents.

Guidelines

- With categories and priorities identified, incidents should be able to be analysed to determine a timeframe for resolution.
    - The resolution's timeframes should adhere to the standard Xyris Terms of Service.

- Security Incidents of a priority of high or above require escalation to CEO and Technical Manager.
- After the analysis of the incident has occurred then a notification of the incident at hand and the timeframes for resolution should be provided to internal staff.
- If the incident is of high or greater and the incident is affecting our clients, then notifications should be provided. The CEO or Technical Manager will provide external notifications.
- Once determined that the incident has been resolved, the vulnerability or weakness needs to be addressed to stop further or future infections.
- Update the Linear ticket with actions taken, and communications should also be added to this ticket, along with any supporting material.
- Update the post-mortem with an incident report including actions taken to resolve incident.
- Conduct a post-incident analysis on how this incident occurred and amend any processes to mitigate or eliminate future attacks.

1.1.6 Learn from security incidents and apply knowledge

Policy

Xyris management and staff will learn from security incidents and modify systems accordingly.

Guidelines

- The information collated and noted within the Incident Report and Post Incident Report must be analysed along with a review and measurement of the performance, response & resolution timings of the Xyris personnel together with their actions throughout the event.
- The types, volumes and costs of incidents will be analysed.
- Recurring and high impact security incidents will be identified and the resolutions used to update this Policy Manual and related procedures.
- Improvements must be made to information security, incident reporting and response processes, where any deficiency is found during this review.

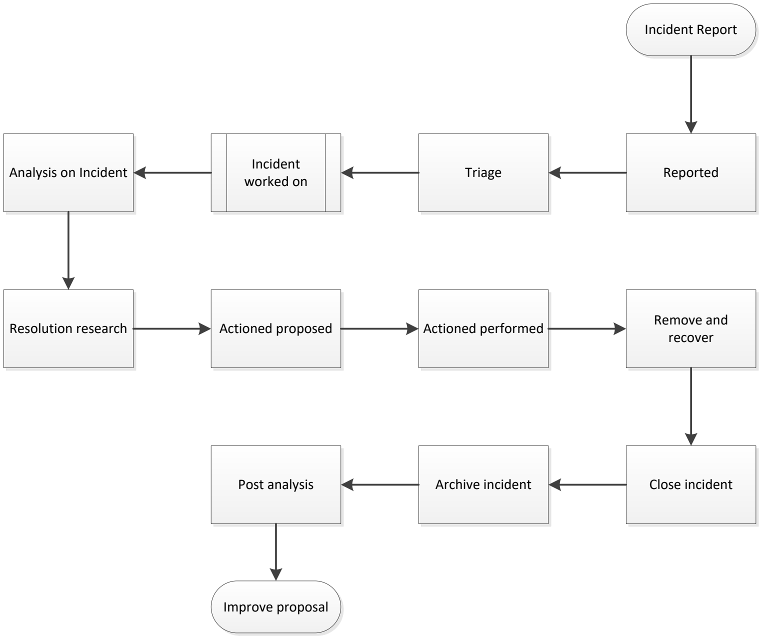
1.1.7 Collect evidence to document incidents and responses

Policy

Evidence relating to incidents will be identified, collected and preserved.

Guidelines

- Xyris' Incident Ticketing System and Incident Reports will be used to collect and preserve evidence of incidents.
- The process for collecting evidence and documentation regarding incidents and responses is as follows:


Incident Report
Reported
Triage
Incident worked on
Analysis on Incident
Resolution research
Actioned proposed
Actioned performed
Remove and recover
Close incident
Archive incident
Post analysis
Improve proposal