Algospark Incident Response Policy

Version: 0.02
Last updated: 7 June 2019
By Darren Wilkinson

The Information Security Incident Response Policy specifies a repeatable methodology which defines the roles and responsibilities staff/student(s) have when dealing with a security incident. Algospark has adopted the following principles, which underpin this policy:

- All information assets must be appropriately handled and managed in accordance with their classification.
- Information assets should be made available to all who have a legitimate need for them.
- The integrity of information must be maintained; information must also be accurate, complete, timely and consistent with other related information and events.
- All staff who have access to information assets, have a responsibility to handle them appropriately and in accordance with their classification.
- Information Asset owners are responsible for ensuring that the data classification scheme, which is described in the Information Security Policy, is used appropriately.

Objectives

- To define appropriate mechanisms for responding to different security incidents
- To ensure that asset owners are appropriately identified and have been informed of security incidents
- To assign responsibilities for the security incident response management process
- To ascertain the seriousness and the extent of damage of an incident
- To identify any vulnerabilities created
- To estimate what resources are required to mitigate the incident
- To ensure that proper follow-up reporting occurs and that procedures are reviewed and adjusted in order to mitigate risks and to establish appropriate actions to prevent future incidents.

Action Implementation

Procedures will be put in place in order to ensure effective security incident management; the objectives of those procedures will be:

- To ensure that security incidents are reported to the relevant sources.
- To define the roles and responsibilities of staff
- To minimise the potential negative impact to Algospark, clients and third parties as a result of such incidents.
- To inform, where appropriate, the affected customer and/or third party of action that is recommended or required on their behalf.
- To restore services to a normal and secure state of operation in a timely manner.
- To provide clear and timely communication to all relevant parties.

Security Incident Management

All Security incidents must be reported to the Data Protection Officer immediately.

Detecting Information Security Incidents

Staff must ensure that Algospark assets are appropriately protected. The steps needed to accomplish this include:

- Compliance and Monitoring (Manual or Systematic reporting)
- Proactive threat discovery e.g. system and network monitoring of current and new threats
- Intrusion Detection and Prevention
- Vulnerability Prevention and Scanning
- Root Cause Analysis

Information security incidents can be accidental or malicious actions or events that have the potential to have unwanted effects on the confidentiality, integrity and availability of Algospark information and IT assets. Examples of information security events and incidents that may pose a threat to information assets include:

- Presence of unauthorised personnel in sensitive areas/buildings
- Theft or physical loss of Algospark information assets (electronic/non-electronic information assets) known to have sensitive information associated (e.g. laptops/mobile phones)
- Loss of storage media (removable drive, CD, DVD, flash drive,)
- A server known to hold sensitive data which has been accessed or otherwise compromised by an unauthorised entity
- An outside entity which is subjected to attacks originating from within the University's data network
- An unauthorised or unwarranted entity causing a network outage
- System slowdown or failure
- Changes in default or user-defined settings
- Unexplained or unexpected use of system resources
- Unusual activities appearing in system or audit logs
- Changes to or appearance of new system files
- Users unexpectedly locked out
- Appliance or equipment failure
- Unexpected enabling or activation of services or ports

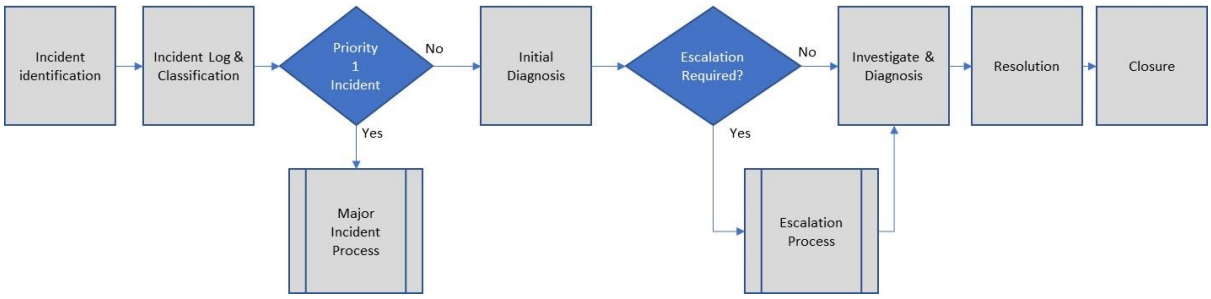
Reporting Information Security Incidents

- Must be reported to the Data Protection Officer as soon as possible.
- It is important that anyone who reports a security incident provides as much relevant information as possible.
- Contact: Data Protection Officer, info@algospark.com, +44 207 558 8728
- Data Protection Officer will co-ordinate with IT team and disseminate communication.

Table 1: Risk, Definition & Response Time

Risk	Priority Level	Response Time	Communication
High: security incident affecting critical systems or sensitive / secret information assets.	1	<12 hours	Updates sent every 2 hours from IT team.
Medium: security incident affecting general systems / confidential information assets	2	<24 hours	Case update on a daily basis.
Low: possible security incident, low potential damage to Algospark and clients.	3	<48 hours	Case update on a weekly basis.

Incident Management Process



Compliance and Monitoring
All staff are directly responsible and liable for the information they handle and are bound to abide by the terms of their employment. Authorised staff members may monitor the use and management of information assets to ensure effective use and to detect unauthorised use of information assets.