Algospark Information Risk Management Policy

Version: 0.02
Last updated: 15 November 2023
By Darren Wilkinson

Purpose
Information that is collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption. The implementation of controls to protect information must be based on an assessment of the risk posed to Algospark, and must balance the likelihood of negative business impact against the resources required to implement the controls, and any unintended negative implications of the controls. This policy sets out the principles that we use to identify, assess and manage information risk, in order to support the achievement of its planned objectives, and aligns with the overall Algospark risk management framework and approach.

Objectives
- Information risks are identified, managed and treated according to an agreed risk tolerance
- Physical, procedural and technical controls are agreed by the information asset owner, balance user experience and security and are cost-effective and proportionate.

Scope
This policy and its supporting controls, processes and procedures apply to all information used at Algospark, in all formats. This includes information processed by other organisations in their dealings with Algospark.

The Information Risk Management Policy and its supporting controls, processes and procedures apply to all individuals who have access to Algospark information and technologies, including external parties that provide information processing services to Algospark.

Compliance with the controls in this policy will be monitored by the Data Protection Officer and reported to Algospark management.

Review
A review of this policy will be undertaken by the Data Protection Officer annually or more frequently as required, and will be approved by Algospark management.

Policy Statement
Information Risk Assessment is a formal and repeatable method for identifying the risks facing an information asset. It is used to determine their impact, and identify and apply controls that are appropriate and justified by the risks. Algospark's policy to ensure that information is protected from a loss of:
- Confidentiality – information will be accessible only to authorised individuals
- Integrity – the accuracy and completeness of information will be maintained
- Availability – information will be accessible to authorised users and processes when required

Risk assessment
- Algospark business processes
- Risks to business assets
- The technical systems in place supporting the business
- Legislation
- Up-to-date threat and vulnerability assessments

A risk assessment exercise will be completed at least:
- For every new information-processing system
- Following modification to systems or processes which could change the threats or vulnerabilities
- Following the introduction of a new information asset
- When there has been no review in the previous three years

A risk score is calculated from Likelihood x Impact Level

Threats: Algospark will consider all potential threats applicable to a particular system, whether natural or human, accidental or malicious.

Vulnerabilities: Algospark will consider all potential vulnerabilities applicable to a particular system, whether intrinsic or extrinsic.

Risk Register: the calculations listed in the risk assessment process will form the basis of a risk register. All risks will be assigned an owner and a review date. The risk register is held by the Data Protection Officer.

Risk Treatment: the risk register will include a risk treatment decision. The action will fall into at least one of the following categories:

- Tolerate the risk – where the risk is already below risk appetite and further treatment is not proportionate
- Treat the risk – where the risk is above risk appetite but treatment is proportionate; or where the treatment is so simple and cost effective that it is proportionate to treat the risk even though it falls below Algospark risk appetite
- Transfer the risk – where the risk cannot be brought below Algospark's risk appetite with proportionate treatment but a cost-effective option is available to transfer the risk to a third party
- Terminate the risk – where the risk cannot be brought below Algospark's risk appetite with proportionate effort/resource and no cost-effective transfer is available

Roles and Responsibilities

The Data Protection Officer will review Medium and Low risks and recommend suitable action. Algospark management in collaboration with the Information Asset Owner will review High risks and recommend suitable action. In the event that the decision is to Treat, then additional activities or controls will be implemented via a Risk Treatment Plan.

Information Asset Owners and Information Asset Managers must be responsible for agreeing and implementing appropriate treatments to risks under their control. They must also take an active role in identifying and reporting new risks.