# Algospark Logical Access Policy

**Version:** 0.02
**Last updated:** 6 June 2019
**By** Darren Wilkinson

**Purpose**
This guideline describes methodologies to use when implementing the logical access control requirements for Algospark resources. Effective implementation of this policy will minimise unauthorised access to these IT systems and services and provide more effective auditing of access controls by:

- Identifying policies and procedures used for logical access to system for granting user access, control, monitoring, and removal of access to Information Technology assets.
- The procedures for periodic review of Algospark users i.e. staff, suppliers, guests and their access rights.

**Roles and Responsibilities**

- IT Manager to monitor compliance with the logical access procedure and to inform the Data Protection Officer of suspected non-compliance and/or suspected breaches of the physical access procedure.
- IT Department: responsible for the safety and security of data on its network and the equipment used to run the network infrastructure.

**Definitions**

- User: an individual or group that require access to the Algospark IT network, systems and/or applications to allow them to fulfil their job functions.
- Access may be the means / method of access to IT either by using authorised access control channels.

**Scope**
Logical access controls are a technical means of implementing access policies i.e. interactions with computer systems & data through access control systems which usually feature identification, authentication and authorisation protocols. Development of the access policies should be directed by the IT Manager with the assistance of the system owners, and data owners.

**Logical Access Policy**
Development of such policies requires balancing the interests of security (sensitivity and risk) against what is needed to accomplish the day-to-day activities in respect of operational requirements, user-friendliness, and cost.

**Logical Access Procedure**
Physical access control protects IT systems through physical barriers. Logical access control protects IT systems and data by verifying and validating authorised users, authorising user access to IT systems and data, and restricting transactions (read, write, execute, delete) according to the user's authorisation level.

**Logical Access Authorisation**
Logical Access controls encompass the following disciplines

- Account Management: Effective account management is central to providing Logical Access control commensurate with sensitivity and risk. It consists of the processes of requesting, authorising, administering, and terminating accounts which access IT systems and data
- Password Management: passwords are required for accounts on all IT systems and are mandatory for accessing all IT systems. Algospark has documented its own password policy.
- Remote access to sensitive IT systems and data may present serious risks. All remote access to sensitive IT systems and data must be encrypted. The encryption must begin with the initiation of the session, include all user identification and authentication, and not end until the session is terminated. A Remote access policy document will be in place for each relevant project.

Logical access reviews which encompasses managing user authorisation access and remote access reviews) are scheduled by the Data Protection Officer.