Algospark Change Control Policy

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

Overview
Change Control is a formal process for making changes to IT systems, services or IT service providers. This policy stabilizes Algospark's production environment by controlling changes made to it. Formal change control policy and procedures will help to ensure that only authorized changes are made, that they are made at the approved time, that they are made in the approved manner, and they are properly documented for auditing purposes.

Purpose
The purpose of this policy is to increase the percentage of up time and reliability of Algospark systems and solutions for clients, staff and suppliers. The goal of the change control policy is to minimize the number and impact of any related incidents. The change control policy also requires documentation, which will be important for problem resolution and contingency planning purposes.

Scope
This policy applies to workstations, laptops, devices, servers and cloud solutions owned or managed by Algospark. This includes systems that contain Algospark data owned and/or managed by Algospark regardless of physical location.

Policy
Algospark change control is co-ordinated and managed by the Data Protection Officer. There are 4 types of changes:

1. Low / minimal to no visibility to users
2. High visibility to users
3. Emergency: a change in a critical system or service that is required due to repair an urgent system, restore a network outage or where a critical application is unavailable.
4. Pre Approved: regularly scheduled changes

Out of Scope: A change that is a normal administrative function or process in a system, service or application that will not have impact.

Change Control Process
Submission of all change control requests must be sent to the Data Protection Officer, and change control email must be submitted detailing the reason for change, dependencies of change and expected timeframes.

- Low: Submitted 24 hours in advance of the change
- High: at least 5 days before required change
- Emergency: covered by Incident Management Policy
- Pre Approved: approved an annual basis.

Change Control Logs

- Held by Data Protection Officer
- Detail acceptance / rejection / exceptions.

Enforcement:
Implementation and enforcement of this policy is ultimately the responsibility of all staff at Algospark. The Data Protection Officer may conduct random assessments to ensure compliance with policy without notice.