Cloud Password Requirement Policy

This document outlines the password requirements for the Notify Cloud platform. Why do we need a password policy? To ensure the security and integrity of our platform, customer data, and user accounts. Here are the key reasons why our policy is essential:

Protects Sensitive Data

Passwords are the first line of defence against unauthorised access. A strong password policy reduces the risk of data breaches by making it harder for attackers to guess or brute-force user credentials.

Safeguards User Accounts

Without a robust password policy, users may choose weak or common passwords. This can lead to account compromises, affecting both individual users and our customers.

Meets Compliance and Regulatory Standards

Many industries are subject to compliance standards (e.g. GDPR, HIPAA, ISO 27001, SOC 2) that require companies to implement strong authentication practices. A formal password policy helps meet these requirements and demonstrates a commitment to information security.

Minimises Operational Disruptions

Account compromises can lead to downtime, data loss, or emergency incident responses. A password policy helps proactively prevent such disruptions, saving time and resources.

Password Requirements

Below are the password requirements for the Notify Cloud platform:

Item	Requirement
Length	Passwords must be a minimum of 12 characters in length
Complexity	Passwords must have at least one non-alphanumeric or special character Passwords must have at least one digit ('0'-'9'). Passwords must have at least one uppercase ('A'-'Z') Easily guessable passwords, e.g. commonly used words, re-use of username etc. is blocked
Age	Maximum password age is 1 year
Lockout	A user will be locked out of their account following 5 consecutive failed attempts
History	The same password cannot be used more than once