**Rue Password Policy**

**1. Scope**

This policy applies to all users, including standard and administrative accounts, as well as any service accounts used within Rue's IT environment.

**2. General Password Requirements**

* All passwords must be at least **12 characters long** and should be **strong**, using a mix of letters, numbers, and symbols.
* Users must **not reuse** old passwords across different accounts or services.
* Passwords must be **stored securely** using a strong hashing algorithm.
* Multi-Factor Authentication (MFA) must be enabled for all privileged accounts and recommended for standard users.
* Passwords **must not** be shared, written down, or stored in an unencrypted format.
* Users should use a **password manager** to securely generate and store passwords.

**3. Administrator and Privileged Account Passwords**

* Admin passwords should be **strong and unique**, not shared between accounts or systems.
* Privileged accounts must use **Multi-Factor Authentication (MFA)**.
* Passwords for privileged accounts should be changed **only when necessary**, such as:
	+ A suspected compromise.
	+ Staff role changes or departures.
	+ When required due to security policies or audits.
* Privileged access should be limited using **role-based access control (RBAC)** and temporary privilege escalation when required.

**4. Service Accounts and API Keys**

* Service account passwords must be **unique and complex**.
* Use machine-generated passwords or keys wherever possible.
* Store service account passwords in a **secure vault**.
* Rotate API keys and credentials **only when required**, ensuring secure rollout mechanisms.

**5. Incident Response**

* If a password is suspected to be compromised, it must be changed **immediately**, and an investigation must follow.
* Any security incident related to credential exposure must be reported to IT Security.

**6. Monitoring and Compliance**

* Regular audits will be conducted to ensure compliance with this policy.
* Automated tools should be used to monitor for leaked credentials.
* Employees will receive periodic **security awareness training** on password security best practices.

This policy is aligned with **Cyber Essentials** and **NCSC guidance** to ensure best-practice password security within Rue.

**Version: V\_1.0**

**Date Created: 24/02/2025**