Information Security Policy

At Century Paper, we are deeply committed to safeguarding our information assets and ensuring the integrity, confidentiality, and availability of our information. As stewards of our digital resources, we prioritize robust information security measures to mitigate risks and protect against potential threats. Our Information Security Policy outlines our steadfast dedication to maintaining a secure environment for our employees, customers, and stakeholders.

- **Responsibility and Governance:** Senior Manager Information Security holds overall responsibility for information security, while users are accountable for safeguarding IT resources. Clear lines of responsibility ensure comprehensive oversight and management of security measures.

- **Data Management:** Data backup policies are rigorously followed, encompassing remote storage for disaster recovery and defined retention periods. Regular reviews of backup functionality uphold data integrity and availability.

- **Endpoint Security:** Licensed antivirus utilities are deployed across all devices, with proactive measures for updates, scans, and policy enforcement. Ensuring endpoint security safeguards against potential threats and vulnerabilities.

- **Software Governance:** IT-managed software installations adhere to approved lists, ensuring compliance with licensing, updates, and security configurations. Departmental responsibilities are delineated for software security maintenance.

- **Email Protection:** Policies are in place to prevent misuse and mitigate risks associated with email communications. Rigorous controls, including whitelisting and anti-spam measures, safeguard against unauthorized access and data breaches.

- **Internet Access Management:** Internet access is restricted to official purposes only, with comprehensive controls and monitoring mechanisms to prevent unauthorized use. Strict enforcement mitigates potential security risks and preserves network integrity.

- **User Access Control:** Robust procedures govern user account creation and deletion, with stringent password policies and authentication mechanisms. Regular reviews ensure access rights align with organizational needs and security standards.

- **Network Infrastructure Security:** Physical access controls and device configurations are implemented to safeguard network infrastructure. These measures include secure server room access and customized configurations to reduce attack surfaces.

- **Media Handling and Encryption:** Stringent protocols govern the handling and disposal of media, with emphasis on data encryption and secure storage. Compliance ensures data confidentiality and integrity across all IT assets.

- **Incident Response and Compliance:** Compliance with legal and regulatory requirements underscores our commitment to maintaining a secure operating environment.

Prepared By : _____ **Version No :** 01

Approved By : _____ **Effective From :** 25-03-2024