Creative Services Limited (CSL)
Data Security Policy
(Version-1, Effective from January 01, 2024)

1. Introduction

Creative Services Limited (CSL) is committed to maintaining the highest standards of data security and privacy to protect the confidentiality, integrity, and availability of data assets. By implementing effective data security controls and procedures of Data Security Policy, CSL assures clients, partners, and stakeholders about trustworthy data handling practices. Recognizing the significance of safeguarding data and information assets, CSL commits to maintaining measures to prevent unauthorized access, disclosure, alteration, and destruction.

2. Policy Statement

CSL is committed to:

- Ensuring compliance with relevant data protection laws, regulations, and industry standards governing the collection, storage, processing, and transfer of data.
- Implementing robust technical, administrative, and physical safeguards to protect data from unauthorized access, misuse, or loss.
- Establishing clear roles, responsibilities, and accountability mechanisms for data security management across the organization.
- Promoting awareness and training programs to educate staff about their responsibilities for data security and privacy.
- Regularly assessing and monitoring the effectiveness of data security controls and procedures and making continuous improvements to mitigate emerging threats and vulnerabilities.
- Responding promptly and effectively to data security incidents and breaches to minimize the impact on individuals and the organization.
- Maintaining transparency and accountability in data handling practices, including providing individuals with clear information about how their data is collected, used, and protected.

3. Data Classification

CSL classifies data into categories based on its sensitivity, criticality, and regulatory requirements. The following classifications are used:

i) **Confidential Data:** Data that requires the highest level of protection due to its sensitive nature, including personally identifiable information (PII), financial records, proprietary information, and trade secrets.

ii) **Sensitive Data:** Data that, if compromised, could cause harm to individuals or the organization, such as health information, intellectual property, and strategic business plans.

iii) **Internal Data:** Data used for internal operations and decision-making, including employee records, internal communications, and operational documents.

iv) **Public Data:** Data that is intended for public consumption and does not contain sensitive or confidential information.

4. Data Security Controls

CSL implements the following data security controls to protect data assets:

i) **Access Controls:** Limiting access to data based on the principle of least privilege, implementing strong authentication mechanisms, and regularly reviewing access permissions to ensure they are appropriate and up to date.

ii) **Encryption:** Encrypting data both at rest and in transit using industry-standard encryption algorithms to prevent unauthorized interception or access.

iii) **Data Loss Prevention (DLP):** Implementing DLP technologies and policies to prevent the unauthorized transfer or disclosure of sensitive data, including monitoring and blocking unauthorized data transfers.

iv) **Network Security:** Implementing firewalls, intrusion detection and prevention systems (IDS/IPS), and other network security measures to protect data from external threats.

v) **Endpoint Security:** Installing and regularly updating anti-malware software, endpoint encryption, and other security controls on all devices used to access organizational data.

vi) **Physical Security:** Securing physical access to data storage facilities, server rooms, and other areas where sensitive data is stored or processed.

vii) **Incident Response:** Establishing incident response procedures to detect, contain, and mitigate data security incidents and breaches in a timely manner, including notifying affected individuals and regulatory authorities as required by law.

viii) **Training and Awareness:** Providing regular training and awareness programs to educate staff about data security best practices, including safe handling of data, recognizing phishing attempts, and reporting security incidents.

5. Data Privacy

CSL respects individuals' privacy rights and adheres to applicable data protection laws and regulations when collecting, processing, and storing personal data. This includes obtaining explicit consent for data processing activities, providing individuals with access to their data, and implementing measures to ensure data accuracy, integrity, and confidentiality.

6. Compliance and Monitoring

CSL regularly monitors compliance with this Data Security Policy through audits, assessments, and reviews of data security controls and procedures. Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contractual relationship.