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

1. Introduction

Creative Services Limited (CSL) is committed to safeguard its information technology (IT) resources and data from cyber threats. This IT and Cyber Security Policy guarantees the confidentiality, integrity, and availability of information. By following this policy, CSL ensures the ongoing protection of its IT resources and data, crucial for the organization's success.

2. Purpose

The purpose of this policy is to:
- Define the principles and procedures for managing IT and cyber security at CSL.
- Protect CSL's information assets from unauthorized access, disclosure, alteration, and destruction.
- Ensure compliance with legal, regulatory, and contractual obligations.
- Promote a culture of security awareness within the organization.

3. Scope

This policy applies to all employees, suppliers, and stakeholders of CSL who use or manage CSL's IT resources. It covers all hardware, software, data, networks, and other IT assets owned, leased, or operated by CSL.

4. Principles

4.1 Confidentiality- Ensure that sensitive information is accessible only to those authorized to have access.

4.2 Integrity- Maintain the accuracy and completeness of information and processing methods.

4.3 Availability- Ensure that information and vital services are available to users when required.

4.4 Compliance- Adhere to relevant laws, regulations, and standards related to IT and cyber security.

5. IT and Cyber Security Management

5.1 Risk Assessment
- Conduct regular risk assessments to identify and evaluate threats to CSL's IT assets.
- Implement measures to mitigate identified risks.

5.2 Access Control
- Use strong authentication and authorization mechanisms to control access to IT resources.
- Grant access based on the principle of least privilege, ensuring users have the minimum access necessary to perform their duties.

5.3 Data Protection
- Encrypt sensitive data in transit and at rest to protect it from unauthorized access.
- Implement regular data backup procedures to prevent data loss.

5.4 Network Security
- Use firewalls, intrusion detection/prevention systems (IDS/IPS), and other security technologies to protect CSL's networks from cyber threats.
- Segment networks to limit the spread of potential security breaches.

5.5 Endpoint Security
- Install and maintain up-to-date antivirus and anti-malware software on all devices.
- Implement device management policies to secure mobile devices and ensure they comply with security standards.

5.6 Incident Response
- Develop and maintain an incident response plan to address cyber security incidents promptly and effectively.
- Conduct regular drills and training to prepare for potential cyber incidents.

5.7 Security Awareness and Training
- Provide regular training to employees on cyber security best practices and emerging threats.
- Promote a culture of security awareness through ongoing education and communication.

6. Specific Security Measures

6.1 Password Management
- Enforce strong password policies requiring complex passwords and regular changes.
- Use multi-factor authentication (MFA) for accessing critical systems and information.

6.2 Software and Patch Management
- Ensure that all software and systems are kept up-to-date with the latest security patches and updates.
- Use automated tools to manage and deploy patches across the organization.

6.3 Physical Security
- Implement physical security controls to protect IT infrastructure, including server rooms and data centers.
- Restrict physical access to authorized personnel only.

6.4 Monitoring and Logging
- Implement logging and monitoring systems to detect and respond to suspicious activities.
- Regularly review logs and take appropriate actions in response to detected anomalies.

7. Compliance and Legal Obligations

7.1 Regulatory Compliance
- Ensure compliance with relevant regulations, including Data Protection Act 2023.
- Conduct regular audits to verify compliance with legal and regulatory requirements.

7.2 Third-Party Management
- Assess and manage the security practices of third-party vendors and service providers.
- Ensure that third-party agreements include appropriate security clauses and obligations.

8. Roles and Responsibilities

8.1 IT Department
- Implement and maintain IT and cyber security measures.
- Monitor IT systems for potential security breaches and respond to incidents.

8.2 Employees
- Adhere to the IT and Cyber Security Policy and report any suspicious activities.
- Participate in security awareness training programs.

8.3 Management
- Provide the necessary resources for effective IT and cyber security management.
- Ensure that IT and cyber security practices align with CSL's strategic objectives.

9. Training and Awareness

- Conduct regular training sessions for employees on IT and cyber security best practices.
- Promote awareness campaigns to keep employees informed about the latest security threats and measures.

10. Monitoring and Review

- Regularly monitor IT systems and networks to detect and respond to security incidents.
- Conduct periodic reviews of the IT and Cyber Security Policy to ensure its effectiveness and relevance.

11. Incident Management

- Develop and maintain an incident response plan to address IT and cyber security incidents.
- Ensure that incidents are promptly reported, investigated, and resolved.

12. Review and Updates

- This policy will be reviewed annually and updated as necessary to reflect changes in technology, legal requirements, and industry best practices.
- Feedback from employees and stakeholders will be considered in the review process.