Creative Services Limited (CSL)
Duty of Care and Security Policy
(Version-1, Effective from January 01, 2024)

1. Introduction

Creative Services Limited (CSL) is committed to protect employees, contractors, clients, and stakeholders. This policy aims to ensure their health, safety, and well-being, as well as safeguard assets and information. It also maintains a secure operational environment and protects against risks and threats.

2. Scope

This policy applies to all employees, contractors, clients, visitors, and stakeholders of CSL. It covers all activities and interactions, both within our premises and external environments where our business operates.

3. Principles

CSL is committed to the following principles:
- Safety: Providing a safe and secure environment for all individuals.
- Health: Promoting physical and mental well-being.
- Security: Protecting assets, information, and intellectual property.
- Compliance: Adhering to all relevant laws, regulations, and industry standards.

4. Responsibilities

4.1 Management
- Ensure the implementation and enforcement of this policy.
- Allocate resources and support necessary for security measures.
- Conduct regular risk assessments and security audits.

4.2 Employees
- Comply with security protocols and procedures.
- Report any security concerns or incidents promptly.
- Take personal responsibility for their safety and the safety of others.

4.3 Security Team
- Develop and implement security plans and procedures.
- Monitor and assess security risks and threats.
- Respond promptly to security incidents and emergencies.

5. Health and Safety

5.1 Workplace Safety
- Provide a safe working environment through regular inspections and risk assessments.
- Ensure compliance with health and safety regulations.
- Conduct safety training for employees and contractors.

5.2 Emergency Preparedness
- Develop and maintain emergency response plans for various scenarios.
- Conduct drills and simulations to prepare employees for emergencies.
- Provide necessary equipment and resources for emergency situations.

6. Physical Security

6.1 Access Control
- Implement access control measures to secure CSL premises and facilities.
- Monitor and restrict access to sensitive areas as necessary.
- Maintain records of access and visitors.

6.2 Asset Protection
- Secure company assets, equipment, and resources from theft, damage, or misuse.
- Implement inventory controls and tracking systems for valuable assets.
- Ensure proper storage and handling of sensitive information and intellectual property.

7. Information Security

7.1 Data Protection
- Protect confidential and sensitive information from unauthorized access, disclosure, or loss.
- Implement cybersecurity measures, including firewalls, encryption, and access controls.
- Train employees on data protection practices and awareness.

7.2 IT Security
- Maintain secure IT infrastructure and networks.
- Regularly update software and systems to protect against vulnerabilities.
- Monitor and respond to cybersecurity threats and incidents.

8. Travel Safety

8.1 Travel Policies
- Establish travel policies and guidelines to ensure employee safety during business travel.
- Provide travel security briefings and resources for employees traveling to high-risk areas.
- Partner with reputable travel agencies and providers for secure travel arrangements.

8.2 Crisis Management
- Develop and communicate crisis management plans for incidents affecting employee safety or business continuity.
- Provide support and assistance to employees affected by crises or emergencies.
- Coordinate with local authorities and emergency services as needed.

9. Reporting and Investigation

9.1 Reporting Procedures
- Establish clear channels for reporting security incidents, concerns, or breaches.
- Encourage open communication and whistleblower protections.
- Maintain confidentiality and handle reports promptly and professionally.

9.2 Investigation
- Investigate security incidents and breaches thoroughly and impartially.
- Identify root causes and implement corrective actions to prevent recurrence.
- Comply with legal and regulatory requirements during investigations.

10. Training and Awareness

10.1 Security Training
- Provide regular security training for employees, contractors, and stakeholders.
- Cover topics such as threat awareness, emergency response, and crisis management.
- Offer specialized training for roles with specific security responsibilities.

10.2 Awareness Programs
- Conduct awareness campaigns on security best practices and procedures.
- Distribute security guidelines and resources to promote a culture of vigilance and preparedness.
- Engage employees in security initiatives and encourage active participation.

11. Compliance and Review

11.1 Compliance
- Monitor compliance with this policy through audits, assessments, and performance reviews.
- Ensure alignment with relevant legal, regulatory, and industry standards.
- Address non-compliance issues promptly and effectively.

11.2 Review
- Review and update this policy periodically to reflect changes in security risks, technology, or operational requirements.
- Seek feedback from employees and stakeholders to improve the effectiveness of security measures.