IT Policy Carbon Check (India) Pvt Ltd

Effective Date: [1st July, 2023]

Purpose The purpose of this IT Policy is to establish guidelines and standards for the use of information technology resources within Carbon Check (India) Pvt Ltd This policy aims to ensure the security, confidentiality, integrity, and appropriate use of IT systems, networks, and data, as well as to promote responsible and ethical behavior by employees and authorized users.

Scope of this policy applies to all employees, Interns, contractors, consultants, volunteers, and any other individuals who have access to CCIPL's IT resources, including but not limited to computer systems, networks, software, data, and communication tools.

General Guidelines

➢ 3.1 - Acceptable Use

- **3.1.1 -** All IT resources provided by CCIPL are to be used for legitimate business purposes in accordance with the organization's goals, objectives, and policies.
- **3.1.2** - Users must not engage in any activity that violates local, national, or international laws or regulations, including but not limited to unauthorized access, distribution of malicious software, infringement of intellectual property rights, or harassment.
- **3.1.3** - Users should exercise caution and good judgment when accessing external websites, downloading files, or opening email attachments to prevent security breaches or the introduction of malware.

➢ 3.2 Information Security

- **3.2.1 -** Users must protect confidential and sensitive information, including personally identifiable information (PII) and financial data, from unauthorized access, disclosure, alteration, or destruction.
- **3.2.2** - Users must not share their login credentials or passwords with others or use another person's account without explicit authorization.
- **3.2.3 -** All devices, including laptops, smartphones, and tablets, should be protected with strong passwords or PINs, encrypted if possible, and promptly reported if lost or stolen.
- **3.2.4** - Users should be aware of and comply with CCIPL's information classification and handling guidelines to ensure data is appropriately protected.

3.3 Data Privacy

- **3.3.1** - CCIPL is committed to protecting individuals' privacy rights and complying with applicable data protection laws and regulations.
- **3.3.2** - Users must handle personal data in accordance with CCIPL's Privacy Policy and obtain proper consent when collecting, using, or sharing personal information.
- **3.3.3** - Personal data should only be accessed by authorized personnel on a need-to-know basis, and adequate security measures should be implemented to prevent unauthorized access, loss, or disclosure.

3.4 Software Usage

- **3.4.1** - Only authorized software obtained through legal and legitimate channels should be installed and used on CCIPL's IT resources.
- **3.4.2** - Users must comply with software licensing agreements and refrain from making unauthorized copies, modifications, or distribution of software.
- **3.4.3 -** Software updates and patches should be installed in a timely manner to address security vulnerabilities and protect against potential threats.

3.5 Network and System Security

- **3.5.1 -** Users must not attempt to gain unauthorized access to any part of CCIPL's network or systems or engage in any activity that disrupts the network or system integrity.
- **3.5.2 -** Any identified vulnerabilities, system errors, or security incidents must be promptly reported to the IT department or designated IT security personnel.
- **3.5.3 -** Users should be aware of and adhere to CCIPL's network and system usage guidelines, including restrictions on bandwidth usage, file sharing, and network access from external sources.

Compliance and Consequences

- **4.1 -** Compliance Monitoring: CCIPL reserves the right to monitor and audit the use of its IT resources to ensure compliance with this policy and applicable laws. Monitoring activities may include but are not limited to network traffic analysis, system logs review, and occasional user assessments.
- **4.2 -** The official electronic messaging system used by the employees is the property of the CCIPL and not the employee. All emails, chats and electronic messages stored, composed, sent and received by any employee or non-employee in the official electronic messaging systems are the property of the CCIPL.
- **4.3** - CCIPL reserves the right to intercept, monitor, read and disclose any messages stored, composed, sent or received using the official electronic messaging systems.

- **4.4 -** CCIPL reserves the right to alter, modify, re-route or block messages as deemed appropriate.
- **4.5 -** IT Administrators can change the email system password and monitor email usage of any employee for security purposes.
- **4.6 -** Consequences of Non-Compliance Failure to comply with this IT Policy may result in disciplinary action, up to and including termination of employment or contract, and legal consequences as allowed by law.

Confidentiality

- **5.1 -** Proprietary, confidential and sensitive information about CCIPL or its employees should not be exchanged via electronic messaging systems unless pre-approved by the Reporting Manager(s) and/or the Management.
- **5.2 -** Caution and proper judgment should be used to decide whether to deliver a message in person, on phone or via email/electronic messaging systems.
- **5.3 -** Before composing or sending any message, it should be noted that electronic messages can be used as evidence in a court of law.
- **5.4 -** Unauthorized copying and distributing of copyrighted content of the organization is prohibited.

Policy Review

This IT Policy will be reviewed periodically by the IT/Admin department and revised as necessary to reflect changes in technology, regulatory requirements, and organizational needs. Users will be notified of any updates or changes to the policy.

By using CCIPL's IT resources, users acknowledge their understanding of and commitment to comply with this IT Policy and related procedures.