**Introduction**

The Data Protection Policy of National Cleaner Production Centre (NCPC) specifies that the organization is responsible for the protection of data and information regarding its’ clients, stakeholders, and its’ employees with the utmost confidentiality. This document defines how the data is collected, stored, controlled with transparency and confidentially. The guidelines mentioned in this document is applied regardless of the medium in which it is stored in.

**Features**

Any data that helps to identify an individual or an organization, will be gathered and processed as a crucial part of our procedure. This may include the name of the individual or the organization, physical address, email address, contact details, any form of identification number (NIC or other identification numbers).

The above mentioned information will be collected from the individual or organization with his/her/it’s full cooperation and sound knowledge. The rules mentioned below will be applied to NCPC following the availability of the information of the interested party.

* The information will be collected stating its purpose and motives.
* The data stored **WILL NOT BE** transferred to any individual, organization or stakeholder who do not have proper data protection policy guidelines.
* The data will be updated regularly.
* Storage of data **WILL NOT** surpass the total specified amount.
* The data will be processed according to its legal and ethical binds.
* It **WILL NOT BE** informally communicated to anyone.
* The data will be consisting of a protective measure to ensure it is protected from any unauthorized or illegal access due to any internal or external parties.
* When NCPC is required by law to release confidential information, the owner of the data will be notified as to what information will be provided.

General Information

* Only the employees who require the data covered by this policy for their work will be granted access.
* The employees of NCPC will have to request access to confidential information from the chief executive officer. Data **WILL NOT BE** shared informally.
* Employees who are granted access will take necessary precautions to keep the data protected. For E.g. Passwords used **WILL NOT BE** shared internally or externally.
* All employees who handle data will be subjected to formal training sessions to ensure they are well aware of their responsibilities.
* If any employee is uncertain and divided about any details, they will request help from their superiors or the chief executive officer.

**Gathering of Data**

The following terms and conditions are valid.

* Data collected from an interested party will be collected through a trustworthy and safe communication medium.
* During the collection of the data, the interested party will be advised of its purpose and the application by the employee of National Cleaner Production Centre (NCPC)
* During any point of data gathering, if the requested data is found out to be unreliable and false, the process will be suspended immediately.

**Storage of Data**

The practice of data storage is given below.

* The data, if stored in paper, will be made sure to be kept in a secure location, accessible only by the authorized personnel. It will be kept in a locked cabinet or a drawer.
* Any paper or printouts containing confidential data **WILL NOT BE** left unattended by the employees of NCPC.
* Once a hard copy containing confidential data is deemed unnecessary, it is made sure to be shredded and disposed appropriately by the employees of NCPC.
* Confidential data stored electronically will be ensured to be equipped with adequate protective measurements to make sure to prevent unauthorized access.
* Electronic data will be protected with the use of strong passwords and will be updated frequently. The passwords **WILL NOT BE** shared among employees and informal sharing of passwords is also prohibited.
* Electronic data stored in a storage device, for e.g. DVD or an external HDD, will be required to be locked away safely when not engaged in any form of use.
* NCPC laptops and computers are prohibited from transferring any electronic data using any storage device, unless access is granted through the chief executive officer.
* Electronic data will be stored in only selected devices and will be updated only through them. These devices will be protected by firewall.
* Data entering into the database of NCPC will be protected through strict security systems.

**Usage of Data**

* Data collected by the National Cleaner Production Centre will be only used for services offered by NCPC.
* The employees make sure the computer screens are locked when left unattended during the usage of personal data. They also make it a point not to save personal data into their personal computers.
* The data is encrypted before transmission of data for added protection.

**Accuracy of Data**

* Data collected will be stored in few places as possible and the access to sensitive data will be monitored
* Proven data collection procedures will be established.
* Employees handling private data will be given online privacy and security measures training.
* Secure network will be established to ensure the protection of electronic data from cyber-attacks. Proper firewall will be in place to ensure safety of data.
* Privacy breaches and misuse of data will be reported formally, and proper actions will be followed.
* Continuous updates will be carried out on personal data and any mistakes reported will be updated without any delay.
* Contract clauses on data is handled will be included.
* Tracking logs are in place to make sure to prevent data misuse.
* Data protection practices are established.

**Responsibility by outsourced entities**

NCPC is authorized to outsource certain services when necessary. In such situations, NCPC enters into a formal consultancy service agreement in which the outsourcing party is also obligated to safeguard the confidentiality of the data. The outsources entities have to ensure that

* + Data received will be only used per the agreement.
	+ Once the task is completed, the data will be erased or destroyed.
	+ If assisted or consulted by external party, necessary confidentiality obligation must be sought from the said entity.

**Subject access requests**

Individuals and organizations whose personal or other data acquired by NCPC are entitled to the following requests.

* Inquire about the information NCPC holds of them and the reason behind it.
* Inquire on how to gain access to it.
* To be informed on how to keep it updated
* Inquire how NCPC is on data protection requirements.

**Modification of Data**

Clients can contact requesting data modification through email or by post to the below address. NCPC has the responsibility to verify the identity of the personnel inquiring the data or making a data modification request.

Email - harshinincpc@gmail.com

Address – 66/1, Dewala Road, Nugegoda

**Disclosure of Data**

In specific circumstances, when needed, NCPC can disclose any data to law enforcement agencies without the consent of the client. NCPC will ensure to check the validity of the request beforehand. Once the validity of the request is ensured, the data will be handed over to the law enforcement agencies.