Assured Data and Information Security Policy (Recital 49, Article 32, Article 34)

Document Number: NGPSPL-WEB-2020-006
Document Version: 1.1

NOTE: Meant for employees within the organization, external staff associated with business operation & customers

REQUESTS: For information requests or for obtaining permission for the use of this work, please submit a written request to: Sales & Marketing, Next Gen Paper Solutions Pvt. Ltd., Plot No - 424, First Floor Udyog Vihar, Phase-IV, Gurgaon (Haryana) - 122016 India.

Revision History

S. No	Version	Date	Author	Approval by	Remarks
1.	1.0	30 November, 2018	Nandita Saxena	Naresh Chand	Draft, Supersedes the earlier documented versions and updated with respect to current practices.
2.	1.1	07 February, 2020	Nandita Saxena	Naresh Chand	Minor changes to make it ready for implementation phase
3.					
4.					
5.					

Table of Contents

1. Purpose

Effective measures for data and information security are essential conditions for a reliable and unwavering outsourcing clients, partners, associates and employees. Aware of client concerns for data breaches and misuses; Next Gen Paper Solutions Pvt. Ltd., (NGPSPL) offers to make assured data and information security an integral component of outsourcing contracts to generate client confidence. Our stringent security policies fully compliant to project information criticality, pace, and scale of outsourcing aim at improving vendor-client collaboration, mutual trust, and ethical business practices.

We use a variety of technologies, data formats, and measures that eliminate the risk of information breaches, secure data from becoming privy to unintended recipients, and allow full control and use of data only for specified purposes. NGPSPL is also certified for ISMS (ISO 27001:2013) and maintains all processes and procedures laid down as per ISMS policy and procedure manuals. This document defines overlapping additional procedures and controls.

2. Policy

NGPSPL is committed to ensuring that all data including employee data and data / documents from NGPSPL clients, secure at all times, and have implemented appropriate technical and organizational measures against the unauthorized or unlawful disclosure of such information, and so as to prevent its accidental loss, destruction or damage.

NGPSPL Information Security Policies includes the following features:

- Data protection and controlling at transmission, supplier/vendor premises, and workstations.
- Comprehensive information security before, during, and after the project completion.
- Compliance to information security in all data formats.
- Use of latest technology for data security.
- In-house professionals and data processing to prevent information breaches.
- Effective regulatory framework in place to fully meet present security threats.
- Provision for additional security as per client/ project requirements.
- Regular security audit of Information Systems and data privacy usage at every level.
- Implementation of integrated and unit-wise steps for client data and information security.
- Identification of possible breaches for every project and creating and enforcing effective mechanism to prevent the same.

3. Data Security Safeguards at NGPSPL:

We have strict security practices at a number of levels to counter Information Systems and data security breaches. These are as follow:

- **Confidentiality & Non-Disclosure Agreement:** NGPSPL is ready to sign Non-Disclosure Agreement with clients as and when it is requested for. This testifies our willingness to convert the data security commitment into a legal binding instrument guaranteeing top-level information security practices. Our professional employees are bound by Confidentiality & NDA terms and security practices explicitly mentioned in their employment terms.
- **Backup & Restore Process:** We backup the files regularly and keep them in secure zones with restricted access.
- **Cleanup Process:** We do not backup data for completed projects or where clients have terminated the contracts without explicit client request. The data was either destroyed or returned back.
- **Data Encryption:** Wherever applicable, encrypted email, folders, and files assure data confidentiality and eliminate the risk of breaches during the sharing processes.

- **Data Sharing:** Only authorized employees are allowed to share data and that too within set information security guidelines. NGPSPL does not allow sharing of source files.
- **Storage and Encryption:** By leveraging the benefits of Cloud Computing all NGPSPL Data is stored on highly secure systems. These utilize the latest encryption and security technologies – we specifically use LUKS File System supported by Linux to keep documents and database encrypted on servers.

4. Data and Information Security:

We use Secure VPN and Network empowered with latest security upgrades. It helps to constantly supervise and overcome unwarranted accesses and firewall breaches. Secure Switches are installed to secure information transformation through reliable VPN Tunnel and block HTTP, UDP port, and other security threats.

5. Employee Access Control:

Personal access to NGPSPL's information systems will only be via a secure username and password. The username and password for each individual is unique and only allows access to their own personal information. Only certain authorized staff, who are required to have access to the personal information of other employees and client data for the purposes of their job role, will be authorized and will have the necessary access rights to do so. They will receive relevant training and will be asked to agree to abide by the terms of this Data Privacy and Protection Statement.

We restrict information inflow at various individual employee levels that prevent unauthorized access, data misuse, and information breaches. These include the following measures.

- Protected system access only for employees working on the project
- Network logins protected by password.
- No remote access is allowed.
- Access Card for common office and workstation areas.
- Client documents and database is encrypted for enhanced data protection as per client requirements.
- Password protected systems and enterprise applications.
- 24x7 security camera surveillance and advanced technology for monitoring.
- Separate security and administrative monitoring.
- USB ports, CD, and other storage devices are not allowed.
- Regular system auditing.
- Latest anti-virus programs for every work station.
- Centralized backup management.

For more information on NGPSPL' Information Security Systems; contact naresh.chand1@kleeto.in (dpo) and / or Nandita.saxena@kleeto.in (cpo)

6. Incident Reporting

If an account or password is suspected to have been compromised, incident shall be reported through an Incident Management System and a consistent process shall be followed for identifying, reporting and investigating the issue until closure. All incidents are adequately documented along with its occurrences and mitigation techniques.

7. References

- Information Security Policy
- Information Security Incident Management Policy

- Information Security Incident Management Procedure