Cyber Security Agreement

The purpose of this Agreement is to establish the minimum network security standards and practices that Suppliers, Vendors, Customers, and anyone who either directly or indirectly interfaces with our digital information or infrastructure, must adhere to when providing services, products, or access to ND Paper's network, systems, or data. This Agreement outlines specific measures to ensure the protection of NDP's information assets and to mitigate potential risks associated with network insecurity, data breaches, and other cyber threats.

Therefore, in consideration of the mutual covenants and promises contained herein, the parties agree as follows:

1. NETWORK SECURITY

Supplier/Vendor/Customer agrees to regularly detect and promptly notify ND Paper of any insecure network settings within its own systems or those directly impacting ND Paper's network. This includes, but is not limited to, identifying unauthorized access points, weak passwords, and misconfigured firewall rules.

2. DNS HEALTH

Supplier/Vendor/Customer shall maintain DNS configurations that are secure and free from vulnerabilities or risks. Supplier agrees to promptly investigate and address any insecure DNS configurations or vulnerabilities detected by ND Paper or its designated security team.

3. PATCHING CADENCE

Supplier/Vendor/Customer commits to maintaining a timely patching cadence for all company assets, including software, hardware, and firmware, to minimize the risk of vulnerabilities or exploits.

4. ENDPOINT SECURITY

Supplier/Vendor/Customer shall ensure that all employee workstations used in the provision of services to ND Paper meet or exceed industry standards for endpoint security. This includes, but is not limited to, anti-virus software, firewalls, and regular security updates. Supplier agrees to cooperate with ND Paper in measuring and improving the security level of these workstations.

5. IP REPUTATION

Supplier/Vendor/Customer shall monitor its own IP reputation and promptly investigate any suspicious activity, such as malware or spam, originating from its network that may impact ND Paper's reputation or operations. Supplier agrees to share relevant information with ND Paper and take corrective actions as necessary.

6. APPLICATION SECURITY

Supplier/Vendor/Customer undertakes to maintain the security of any web applications or services provided to ND Paper, including regular assessments for common vulnerabilities and timely remediation of identified issues. Supplier shall provide ND Paper with access to vulnerability reports and remediation plans if necessary.

7. HACKER CHATTER

Supplier/Vendor/Customer agrees to monitor hacker forums, chat rooms, and other relevant sources for chatter or discussions related to ND Paper's network, systems, or

data. Supplier shall promptly notify ND Paper of any such activity and work with ND Paper to mitigate potential threats.

8. INFORMATION LEAK

Supplier/Vendor/Customer undertakes to maintain strict confidentiality of all ND Paper information and to promptly notify ND Paper of any potential information leaks, whether intentional or inadvertent. Supplier/Vendor/Customer shall cooperate fully with ND Paper in investigating and containing any such leaks.

9. SOCIAL ENGINEERING

Supplier/Vendor/Customer agrees to regularly train its employees on social engineering and phishing attack awareness, and to measure the effectiveness of these efforts. Supplier shall share its training materials and awareness metrics with ND Paper upon request.

COMPLIANCE AND ENFORCEMENT

Supplier/Vendor/Customer acknowledges that failure to comply with the terms of this Agreement may result in immediate termination of the business relationship between the parties, as well as potential legal action for any damages suffered by ND Paper.

GOVERNING LAW

This Agreement shall be governed by and construed in accordance with the laws.