YELLOW CORPORATION INFORMATION SECURITY AND PRIVACY POLICY FOR VENDORS AND SUPPLIERS

This Information Security and Privacy Policy for Vendors and Suppliers ("Policy") governs whenever a Supplier is granted physical or logical access to Yellow Information Systems, is Processing Confidential Information or where Supplier Information Systems interact with Yellow Information Systems, as part of their contract(s). If any terms in this Policy conflict with the terms contained in any Agreement between Supplier and Yellow, the provisions providing the greatest protections to Confidential Information prevail and control.

1. Definitions

1.1. "Affiliate" means (1) all business units and divisions of a party or its parents and (2) any entity controlled by, controlling, or under common control with such party. Such entity shall be deemed to be an "Affiliate" only so long as such control exists.

1.2. "Agreement" means a contract, agreement, statement of work, task order, or purchase order governing the services and/or deliverables provided by Supplier to Yellow.

1.3. "Back-up Media" means a physical device or other physical storage media that contains Confidential Information. Back-up Media may include but is not limited to disks, drives, tapes, and hard copy.

1.4. "Confidential Information" means Yellow Critical Infrastructure Information, Customer Proprietary Network Information, Personally Identifiable Information, information defined as confidential in an Agreement, Sensitive Confidential Information, and any other sensitive, private, proprietary or legally-protected data that is owned, controlled, or processed by Yellow or a third party.

1.5. "Critical Infrastructure Information" or "CII" means information regarding Yellow's network architecture and key network assets, including but not limited to, the location and capability of central offices, network points of presence and other critical network sites, network elements and equipment within them, and any other information Yellow designates as critical infrastructure information.

1.6. "Device(s)" means a piece of mechanical or electronic equipment used for computing or storing data and information, including Mobile Devices.

1.7. "Encryption" or "Encrypted" means protecting information or data by converting it into a code using strong cryptographic protocol and hashing algorithm types and key management processes consistent with the highest-level industry practice.

1.8. "Location" means the location where Confidential Information resides or can be accessed, including but not limited to, a Device, physical location, hosting jurisdiction, or other jurisdiction.

1.9. "Location Move" means (a) moving Confidential Information from one hosting jurisdiction to a different hosting jurisdiction; (b) provisioning remote access to Confidential Information from a location other than the Yellow-approved hosting jurisdiction or other Yellow-approved jurisdiction; or (c) moving Confidential Information from a physical location or jurisdiction to a different physical location or jurisdiction.

1.10. "Mobile Device(s)" means portable computing and storage devices such as laptops, personal digital assistants, cell phones, tablets, and smartphones running mobile operating systems (e.g., iOS, Blackberry OS, Android, or Windows Mobile operating systems).

1.11. "Personally Identifiable Information" or "PII" means any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

1.12. "Privileged Account(s)" or ("PA") means accounts with (a) system-level administrative or super-user access to devices, applications or databases; (b) administration access to accounts and passwords on a system; or (c) ability to override system or application controls.

1.13. "Process" or "Processing" means the performance of any operation or set of operations upon data (including, but not limited to, Confidential Information), whether or not by automatic means, including, but not limited to, collecting, recording, organizing, storing, adapting. altering, retrieving, accessing, consulting, using, disclosing by transmission, disseminating, making available, aligning, combining, blocking, erasing, or destroying data.

1.14. "Security Incident" means any actual or suspected event in which Confidential Information is or may have been lost, stolen, improperly altered, improperly destroyed, improperly disclosed, used for a purpose not permitted under an Agreement or this Policy, or accessed by any unauthorized person.

1.15. "Security Notice" means any written communication, notice, filing, press release, or report related to a Security Incident.

1.16. "Security Standards" means commercially reasonable security features in all material hardware, software, systems, and platforms that Supplier uses to access, Process and/or store Confidential Information.

1.17. “Sensitive Confidential Information” means Confidential Information that involves racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership, health and financial matters, sexual preferences, Social Security Numbers, credit cards and any other account numbers, customer data, or other Confidential Information which Yellow identifies as Sensitive Confidential Information, whether the information pertains to consumer, business, or employment activities.
1.18. “Services” means the services, materials, products, deliverables Yellow engaged Supplier to produce or perform which necessitate the Processing of Confidential Information.
1.19. “Supplier” means the entity and any Affiliate of such entity that provides Services to Yellow that Processes or has access to Confidential Information or has access to Yellow Information Systems or data.
1.20. “Supplier Information System(s)” means any Supplier systems, applications, computers, network equipment, hardware and Mobile Devices used to Process Yellow Confidential Information pursuant to the Agreement and/or as part of the Services, which includes laptops and network connected devices.
1.21. “Supplier Personnel” means Supplier’s employees, as well as its Affiliates, suppliers, subcontractors, and agents, and their respective employees.
1.22. “Yellow” means Yellow Corporation and its Affiliates.
1.23. “Yellow Information System(s)” means any networks, databases, applications, computers, hardware and/or Mobile Devices managed by Yellow, including laptops and network connected devices.

2. Minimum Periodic Review Requirements

2.1. Annual Review
- 2.1.1. Vulnerability and Penetration assessments (See Section 5)
- 2.1.2. Supplier Personnel Training (See Section 4)
- 2.1.3. Security Standards Audit (See Section 10)

2.2. Semi-Annual Review
- 2.2.1. Authorized connections and rule sets (See Section 6)

2.3. Quarterly Review
- 2.3.1. Physical access rights (See Section 5)
- 2.3.2. Privileged Account access rights (See Section 5)
- 2.3.3. Security Incidents (See Section 9)

3. Minimum Retention Requirements

3.1. Security Camera Recordings: 30 days
3.2. Physical access logs: 1 year
3.3. Security Incident logs: 1 year

4. Security Requirements

4.1. Supplier must review this Policy before accepting or Processing any Confidential Information. Supplier must protect Confidential Information from unauthorized Processing, disclosure, or loss. At all times that Supplier Processes Confidential Information, Supplier must:
- 4.1.1. Meet all Security Standards, as applicable, of this Policy.
- 4.1.2. Meet the terms of the Security Requirements section, and Additional Security Requirements Section, as applicable, of this Policy.
- 4.1.3. Maintain written physical and technological safety and data security procedures (“Safety Procedures”) to safeguard against the destruction, loss, unauthorized access, or alteration of Confidential Information, reflecting best practices for information security.
- 4.1.4. Maintain and follow written Security Standards and Safety Procedures, including any requirements specified in the Agreement, regarding backup and recovery of data to prevent loss of data in the case of a systems outage or Security Incident.
- 4.1.5. Require that all Supplier Personnel review and sign an attestation to follow and comply with the Safety Procedures.
- 4.1.6. Conduct Safety Procedures training for all Supplier Personnel at least annually.
- 4.1.7. Create and implement a tailored and appropriate due diligence process to continually verify Supplier and Supplier Personnel compliance with this Policy, the Safety Procedures, and additional security requirements contained in any applicable Agreement.
- 4.1.8. Assume ultimate responsibility and liability for Supplier Personnel compliance with this Policy and any additional security requirements contained in an applicable Agreement.
- 4.1.9. Maintain a privacy policy on Supplier’s website.

4.1.10. Cooperate in good faith to modify its business practices to accommodate any future changes in the parties' hardware, software, or services, or in legal or industry standards regarding the treatment of Confidential Information that may affect the reasonableness or effectiveness of the protections under this Policy.

4.2. In the event of separation, termination, or transfer of Supplier Personnel, Supplier shall undertake prompt and reasonable measures to:
   4.2.1. Terminate Supplier Personnel access to Confidential Information, whether physical or logical, no later than the date of personnel separation or personnel transfer.
   4.2.2. Where Supplier Personnel have been assigned Yellow sign-on credentials, Supplier must notify Yellow of any such separation or transfer immediately, but no later than the day of that event.

4.3. Unless prohibited by applicable law or regulation, Supplier shall notify Yellow promptly and act only upon Yellow's instruction, upon any request by a third party, including without limitation law enforcement, governmental authority, or in connection with litigation or other court process for disclosure of Confidential Information or for information concerning the Processing of Confidential Information.

4.4. Supplier and Supplier Personnel are expressly prohibited and not authorized to Process Confidential Information on personal accounts (e.g., individual email or cloud services accounts such as Gmail, Yahoo, Dropbox, Google Drive, etc.) or on personally owned Devices.

4.5. Supplier is authorized only to Process Confidential Information on Supplier Information Systems to the extent necessary to perform the Services. Processing Confidential Information on Supplier Information Systems beyond the extent necessary to perform the Services is expressly prohibited.

4.6. Yellow prior approval is required for all Locations and Location Moves.

4.7. Supplier is prohibited from Processing any Confidential Information at any location outside the United States or through entities that are not incorporated or organized in the United States. Any exceptions require prior written consent from Yellow.

4.8. Encryption is required for the following instances:
   4.8.1. At rest for any Device containing Confidential Information.
   4.8.2. When electronically transferring Confidential Information over public networks (such as the Internet) or across non-U.S. territory.

4.9. Supplier Information Systems must have security controls that can detect and prevent attacks and must be continuously monitored. For example, network layer firewalls and intrusion detection/prevention Systems (IDS/IPS) between the Internet and DMZ, and between DMZ and internal servers containing Confidential Information. IDS/IPS high and critical priority alerts must be responded to as soon as reasonably practicable but in no case more than 24 hours.

4.10. Any Supplier Personnel remotely accessing Supplier Information Systems must be authenticated using at least a two-factor authentication method and such transmissions must be secured using Encryption.

4.11. Supplier agrees that all Yellow data residing on Supplier Information Systems is the property of Yellow. Supplier must return to Yellow all Yellow data upon dissolution of the Agreement or business relationship between Yellow and Supplier, regardless of cause.

4.12. Supplier must remove Confidential Information from Supplier Information Systems prior to disposal or reuse in a manner that ensures that the Confidential Information may not be accessed or readable. Supplier's removal process must be an auditable process (e.g., certification of destruction).

4.13. Upon dissolution of the Agreement or business relationship between Yellow and Supplier, and after returning Yellow data to Yellow, Supplier must remove Confidential Information from Supplier Information Systems in a manner that ensure the Confidential Information may not be accessed or readable. Supplier's removal process must be an auditable process (e.g., certification of destruction).

4.14. Yellow reserves the right to audit Supplier and Supplier Personnel for compliance with this Policy.

5. Additional Security Requirements for Sensitive Confidential Information

In addition to the above Security Requirements, the following additional measures and controls are required with respect to Sensitive Confidential Information, Supplier shall:

5.1. Perform vulnerability and penetration assessments on Supplier Information Systems. For Supplier Information Systems that are internet facing, Supplier must engage an independent external party to perform a vulnerability and penetration assessment at least annually and shall remediate as required and identified by Audits.

5.2. Have or implement hardening and configuration requirements consistent with highest level industry practices.

5.3. Implement and maintain appropriate data loss prevention ("DLP") controls consistent with highest level industry practices (e.g., disabling of USB ports, DLP software, URL/Web filtering) to detect and prevent unauthorized exfiltration of Confidential Information from Supplier Information Systems.

5.4. Support the secure creation, modification, and deletion PAs.

5.4.1. Supplier must review and update PA access rights at least quarterly.

5.4.2. Supplier shall continually review PA usage logs.

5.4.3. Supplier shall use Encrypted mechanisms (e.g., secure shell) to establish PA access.

5.5. Monitor, record, and control all physical access with physical access rights.

5.5.1. Limit physical access to Supplier Information Systems to approved, authorized Supplier Personnel

5.5.2. Unless prohibited by applicable law, Supplier must create physical access logs detailing access.

5.5.3. If Supplier is not staffed with physical security 24 hours per day, it must install and maintain alarms and entry point security cameras for off-hours access monitoring.

6. Technical Controls on Supplier Information Systems

6.1. Unless otherwise expressly agreed in the Agreement, development and testing environments must not contain Confidential Information and shall only go "live" upon Yellow Information Security's review and approval, as appropriate.

6.2. Back-up Media stored at Supplier's site must be kept in a secure location (e.g., locked office or locked file cabinet) and be Encrypted to a standard consistent with industry practice. Off-site Back-up Media storage must employ a check-in/check-out process with locked storage for transportation. Back-up Media must be given the same level of physical and environmental protection as the level of protection applied to "live" Confidential Information.

6.3. Supplier must implement network layer security devices to allow only authorized connections and rule sets.

6.4. Use of Mobile Devices to Process Confidential Information is authorized only in compliance with this Policy and only as needed to provide the Services. If so needed, Confidential Information contained on or processed through Mobile Devices must be Encrypted. Supplier must ensure that Mobile Devices used to Process Confidential Information (including emails) must have strong mobile device security controls, including required passcode, minimum passcode length, inactivity lock, and a process in place to immediately remotely wipe lost or stolen devices.

7. Compliance

7.1. Supplier represents and warrants that it shall comply with all laws and regulations applicable to Supplier's activities concerning Confidential Information.

8. Data Collection

8.1. Unless and except to the extent expressly provided in the Agreement, Supplier must, in each case, seek and obtain Yellow's prior written approval regarding the scope of any PII to be collected by Supplier, as well as any notices to be provided and any consent language to be used when collecting such information from or about an individual. In the case of PII collected directly from individuals by Supplier, Supplier shall comply with applicable data privacy laws and regulations, including those concerning notice, consent, access, correction, and deletion.

9. Security Incident

9.1. Supplier must develop and maintain an up-to-date incident management plan designed to promptly identify, prevent, investigate, and mitigate any Security Incidents and perform any required recovery actions to remedy the impact.

9.2. Security Incidents on Suppliers Information Systems must be logged, reviewed on a periodic basis, and securely maintained.

9.3. Supplier will promptly provide notification of Security Incidents (but in no event later than 24 hours after discovery) to Yellow in writing. Supplier shall report Security Incidents to Yellow's Information Security Manager at Security.Management@myyellow.com, or by calling Yellow's Network Operations Console (NOC) at 913.344.3106 and asking to be connected with the current Information Security Manager. In any such instance, Supplier will give specific information on what Confidential Information was accessed and any other information Yellow reasonably may request concerning the details of the Security Incident, as soon as such information can be collected or otherwise becomes available. Supplier will also disclose any

remediation efforts undertaken, to the extent known and will thereafter provide regular and timely updates throughout the ongoing investigation and remediation. Supplier shall work to secure the return of any Confidential Information removed or copied. Upon reasonable request of Yellow, Supplier may be required to hire an independent, third party forensic or security firm to assist with investigation or remediation efforts. Yellow reserves the right, and is entitled, to receive the final results of the investigation, whether conducted by Supplier or a third party.

9.4. Notwithstanding and excluded from any limitations in the Agreement, Supplier shall pay for or reimburse Yellow for all costs incurred by Yellow as a result of a Security Incident, including repeated and related losses and expenses relating to any Security Incident experienced by Supplier, including without limitation, costs of forensic assessments, Security Notices, credit monitoring or other fraud alert services, and all other remedies either required by applicable law and regulation or which are required to remediate the Security Incident and prevent similar Security Incidents in the future.

9.5. If requested by Yellow, and at Yellow's direction, Supplier shall send Security Notices regarding a Security Incident.

9.5.1. Unless prohibited by applicable law or regulation, Supplier shall provide Yellow with reasonable notice of, and the opportunity to comment on and approve, the content of such Security Notices prior to any publication or communication thereof to any third party, except Yellow shall not have the right to reject any content in a Security Notice that is specifically required to comply with applicable law or regulation.

9.5.2. Should Yellow elect to send a Security Notice regarding a Security Incident, Supplier shall provide all reasonable and timely information relating to the content and distribution of that Security Notice as permitted by applicable law or regulation pursuant to the Security Notice.

9.6. Supplier may not make or permit any public statements or disclosure to any third party concerning any Yellow connection to any Security Incident without the explicit written authorization of the Yellow Legal Department.

10. Audits

10.1. Supplier shall monitor the effectiveness of its Security Standards by conducting or engaging a third party to conduct audits and risk assessments of Supplier Information Systems against the requirements of this Policy. Supplier shall be responsible for ensuring consistency of its Security Standards, including proactive monitoring and mitigation of all vulnerabilities across any Supplier Information Systems used to access or Process Confidential Information or Yellow Information Systems.

10.2. Upon Yellow request, Supplier will provide information to Yellow to enable Yellow to determine compliance with the applicable security requirements. Yellow may require Supplier to, without limitation, answer security questionnaires or conduct scans of servers, databases and other network hardware, and submit an attestation by an officer of Supplier with knowledge of Supplier's compliance.

10.3. Upon request, Supplier must provide to Yellow reports of any audits and assessments conducted on Supplier Information Systems, which reports shall include, at a minimum, the scope of the audit and/or assessment and any vulnerabilities, issues, findings, concerns, and/or recommendations in so far as they impact Confidential Information. Such reports provided by Supplier to Yellow shall be treated as confidential.

10.4. Supplier must remediate within thirty (30) days, or as soon as reasonably practicable thereafter, any items rated as high or critical (or similar rating indicating similar risk) in any audits or assessments of Supplier Information Systems. Yellow reserves the right to request remediation to be completed in less than 30 days or suspension of further activity where necessary to adequately protect Confidential Information. Where necessary to protect Confidential Information, Yellow may instruct Supplier to immediately suspend the Services without liability under any applicable Agreement.

10.5. Yellow reserves the right to conduct an onsite audit of Supplier on thirty (30) days prior written notice during regular business hours. This right shall survive termination or expiration of the Agreement so long as Supplier Processes Yellow Confidential Information provided under the Agreement. Supplier agrees to cooperate fully with Yellow or its designee during such audits and shall provide access to facilities, appropriate resources, provide applicable supporting documentation to Yellow, and complete security assessment questionnaires that may be requested.

10.6. If Yellow has a reasonable basis to believe that Supplier has breached or is likely to breach the terms of this Policy, Yellow may, upon 5 days' notice, perform a vulnerability assessment, which assessment will be in addition to any assessment in the ordinary course. At Yellow's reasonable request, Supplier will promptly cooperate with Yellow to develop a plan to protect Confidential Information from any applicable

failures or attacks, which plan will include prioritization of recovery efforts, identification of and implementation plans for alternative data centers or other storage sites and backup capabilities.

11. Material Breach

11.1. Notwithstanding anything to the contrary herein or in the Agreement, Supplier's (including Supplier Personnel) failure to comply with the obligations set forth in this Policy also constitutes a material breach of the Agreement, with such rights and remedies set forth therein or under applicable law and regulation.

11.2. Yellow and/or any Yellow Affiliate may enforce the terms of this Policy with respect to Confidential Information.