Security, Compliance and Privacy

1. **Objectives:** CloudPost shall implement data security measures that are consistent with industry best practices and standards such that CloudPost:

    a. Protects the privacy, confidentiality, integrity, and availability of all data which is disclosed by Customer to or otherwise comes into the possession of CloudPost ("Data"), its affiliates or sub-contractors, directly or indirectly as a result of this Agreement, including but not limited to Customer's Confidential Information and any Customer personally identifiable information;

    b. Protects against accidental, unauthorized, unauthenticated, or unlawful access, copying, use, processing, disclosure, alteration, transfer, loss or destruction of the Customer Data including, but not limited to, identity theft;

    c. Complies with all federal, state, and local laws, rules, regulations, directives and decisions (each, to the extent having the force of law) that are relevant to the handling, processing, storing or use of Customer Data in accordance with this Agreement;

    d. Manages, controls and remediates any threats identified in the Risk Assessments findings that could result in unauthorized access, copying, use, processing, disclosure, alteration, transfer, loss or destruction of any of the Customer Data, including without limitation identity theft; and

    e. Complies with and implements the risk policies listed in this document, together with the data protection and confidentiality obligations of the Agreement.

2. **Organization Security Measures:**

    a. **Environment:** CloudPost shall provide assurance that it sets the foundation for the necessary tone, discipline, and structure to influence the control consciousness of its people necessary, and for the services provided to Customer, and/or Customer's customers.

    b. **Responsibility:** CloudPost shall assign responsibility for information security management to appropriate skilled and senior personnel.

    c. **Qualification of Employees:** CloudPost shall implement and maintain appropriate security measures and procedures, including background checks following industry best practices, to restrict access to information systems used in connection with this Agreement or to Customer information to only those personnel who are reliable, have sufficient technical expertise for the role assigned, and have personal integrity.

    d. **Obligations of Employees:** CloudPost shall implement and maintain appropriate security measures and procedures in order to verify that any personnel accessing the Customer Information or information systems used in connection with this Agreement knows his or her obligations and the consequences of any security breach, and have read and agree to comply with all applicable Customer Information Security Policies and Standards.

    e. **Segregation of Duties:** CloudPost shall provide reasonable assurance the organization of personnel provides adequate segregation of duties between incompatible functions.

3. **Physical Security Measures:**

    a. Physical Security and Access Control – CloudPost shall ensure that all systems hosting Customer Data and/or providing services on behalf of Customer are maintained consistent with industry best practices and standards in a physically secure environment that prevents unauthorized access, with access restrictions at physical locations containing Customer Data, such as buildings, computer facilities, and records storage facilities, designed and implemented to permit access only to authorized individuals and to detect any unauthorized access that may occur, including without limitation 24 x 7 security personnel at all relevant locations ("Customer Secure Area").

    b. **Physical Security for Media** – CloudPost shall implement and maintain appropriate security measures and procedures consistent with industry best practices and standards to prevent the

unauthorized viewing, copying, alteration or removal of any media containing Customer Data, wherever located.

c. Media Destruction – CloudPost shall implement and maintain appropriate security measures and procedures consistent with industry best practices and standards to destroy removable media and any mobile device (such as discs, USB drives, DVDs, back-up tapes, laptops and PDAs) containing Customer Data where such media or mobile device is no longer used, or alternatively to render Customer Data on such removable media or mobile device unintelligible and not capable of reconstruction by any technical means before re-use of such removable media is allowed.

4. Computer System Access Control Measures:

a. Access Controls – CloudPost shall implement and maintain appropriate security measures and procedures consistent with industry best practices and standards to ensure the logical separation such that access to all systems hosting Customer Data and/or being used to provide services to Customer shall: be protected through the use of access control systems that uniquely identify each individual requiring access, grant access only to authorized individuals and based on the principle of least privileges, prevent unauthorized persons from gaining access to Customer Data, appropriately limit and control the scope of access granted to any authorized person, and log all relevant access events. These security measures and procedures shall include, but shall not be limited to:

b. Access Rights Policies – CloudPost shall implement appropriate policies and procedures regarding the granting of access rights to Customer Data in CloudPost's possession or control, in order to ensure that only the personnel expressly authorized pursuant to the terms of the Agreement or by Customer in writing may create, modify or cancel the rights of access of the personnel. CloudPost shall maintain an accurate and up to date list of all personnel who have access to the Customer Data and shall have the facility to promptly disable access by any individual personnel. For purposes of this Schedule, the term "personnel" as to Customer or CloudPost shall mean such Party's employees, consultants, subcontractor or other agents.

5. **Intrusion Detection/Prevention and Malware**:

a. CloudPost shall use appropriate security measures and procedures (i) to ensure that Customer Data in CloudPost's possession and control, and /or systems being used to provide Services, is protected against the risk of intrusion and the effects of viruses, Trojan horses, worms, and other forms of malware, and (ii) to monitor and record each and every instance of access to the CloudPost's assets and information systems and to Customer Data to detect the same, and to promptly respond to the same. If any malicious code is found to have been introduced by CloudPost or any third party into any of CloudPost's information systems handling or holding Customer Data, CloudPost shall take appropriate measures to prevent any unauthorized access or disclosure of any Customer Data and in any case (wherever such code originated), CloudPost shall, at no additional charge to Customer, remove such malicious code and eliminate the effects of the malicious code. If such malicious code causes a loss of operational efficiency or loss of data, CloudPost shall monitor such losses and restore such lost data in accordance with the terms of the Agreement. Unless, and to the extent, prohibited by law enforcement authorities, CloudPost shall immediately notify Customer's Chief Information Security Officer if it knows or reasonably suspects that there has been an actual instances of unauthorized access to the Customer Data and/or systems holding or handling Customer Data and shall cooperate fully in assisting Customer as necessary to enable Customer to comply with its statutory and other legal breach notice requirements, if any.

6. **Incident Response Measures** – CloudPost shall implement and maintain appropriate incident response measures and procedures for systems that handle or hold Customer Data, including, but not limited to:

a. Operational problems and security incidents are detected, reported, logged, and resolved in a timely manner.

b. Processing is appropriately authorized, scheduled, and that deviations from scheduled processing are detected, reported, logged, and resolved in a timely manner.

c. System availability, performance and capacity are routinely monitored to help ensure potential issues are detected, reported, logged, and resolved in a timely manner.

d. Networks are routinely monitored for availability and response times to help ensure potential issues are detected, reported, logged, and resolved in a timely manner.

7. <u>Data Management Controls Measures:</u>

a. **Customer Data** - Customer Data must only be used by CloudPost for the purposes specified in this Agreement.

b. **Customer Production Data** - Where access is given to Customer Data on any Customer production system, unless otherwise agreed to in writing by Customer, CloudPost must not and shall procure that its personnel and sub-contractors shall not copy, download or store such Customer Data on any desktop, server or other device at any Location, in CloudPost's or its personnel's possession or otherwise.

c. **Data Integrity Controls** – Implementing and maintaining appropriate security measures and procedures to protect the integrity of the Customer Data in CloudPost's possession or control, to prevent the unauthorized recording, alteration or erasure of such Customer Data, and to ensure that it is subsequently possible to determine when, by whom and which Customer Data were recorded, altered or erased.

d. **Data Destruction –** Implementing and maintaining appropriate security measures and procedures to destroy Customer Data in CloudPost's possession or control when appropriate and in accordance with the Agreement. At the request of Customer at any time, CloudPost will: (i) promptly return to Customer, in the format and on the media reasonably requested by Customer, all or any part of Customer Data; and (ii) erase or destroy all or any part of Customer Data in CloudPost's possession, in each case to the extent so requested by Customer.

e. **Software Patching** – Implementing and maintaining appropriate security measures and procedures in order to ensure the regular update and patching of all computer software on systems that handle or hold Customer Data to eliminate vulnerabilities and remove flaws that could otherwise facilitate security breaches. Patching schedule and regular verification access and/or reporting shall be mutually agreed upon by Customer and CloudPost.

f. **Virus Management** – CloudPost shall implement and maintain appropriate security measures and procedures designed to provide antivirus and spyware software protection to CloudPost's systems that handle or hold Customer Data, using the most recently distributed version of software.