SmartFile Security Standards

1. **Information Security Program.** SmartFile will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the SmartFile Network, and (c) minimize security risks, including through risk assessment and regular testing. SmartFile will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

    a. **Network Security.** The SmartFile Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. Smartfile will maintain access controls and policies to manage what access is allowed to the SmartFile Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. SmartFile will maintain corrective action and incident response plans to respond to potential security threats.

    b. **Physical Security**

        i. **Physical Access Controls.** Physical components of the SmartFile Network are housed in nondescript facilities (the "**Facilities**"). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

        ii. **Limited Employee and Contractor Access.** SmartFile provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of SmartFile or its affiliates.

        iii. **Physical Security Protections.** All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are

monitored by video surveillance cameras designed to record all individuals accessing the Facilities. SmartFile also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion- detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

2. **Continued Evaluation**. SmartFile will conduct periodic reviews of the security of its SmartFile Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. SmartFile will continually evaluate the security of its SmartFile Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.