SmartSort Technologies, Inc.

Business Continuity & Security Measures

Business Continuity Plan (BCP)

1. Introduction

SmartSort's Business Continuity Plan (BCP) outlines the strategies and procedures our organization uses to ensure the continuity of operations.

SmartSort leverages Microsoft Azure's robust cloud infrastructure and services, to minimize downtime and maintain critical business functions, during normal business conditions and in the event of a disaster.

2. Objectives

- Ensure the availability of critical applications and data.
- Minimize the impact of disruptions on business operations.
- Provide a clear framework for disaster recovery and business continuity.

3. Risk Assessment

SmartSort has identified potential risks that could lead to outages, including natural disasters, cyber-attacks, hardware failures, and human errors – and - assessed the likelihood and impact of each risk to prioritize mitigation efforts.

4. Azure Services Utilized

- **Azure Site Recovery**: Enables seamless replication of virtual machines (VMs) and physical servers to Azure, ensuring quick recovery in case of an outage.
- **Azure Backup**: Provides secure and reliable backup solutions for critical data, ensuring data integrity and availability.
- **Azure Virtual Network**: Facilitates secure and scalable networking solutions, allowing for seamless connectivity between on-premises applications and cloud environments.
- **Azure Load Balancer**: Distributes incoming traffic across multiple VMs, ensuring high availability and reliability of applications.
- **Azure Monitor**: Offers comprehensive monitoring and diagnostics capabilities, enabling proactive identification and resolution of potential issues.

5. Disaster Recovery Strategy

- **Data Replication**: Implement Azure Site Recovery to replicate critical VMs and data to a secondary Azure region. This ensures that data is always available, even in the event of a regional outage.
- **Automated Failover**: Configure automated failover mechanisms to switch to the secondary region seamlessly, minimizing downtime and ensuring business continuity.
- **Regular Testing**: Conduct regular disaster recovery drills to test the effectiveness of the failover process and ensure that all team members are familiar with their roles and responsibilities.

6. Backup and Restore Procedures

- **Scheduled Backups**: Utilize Azure Backup to schedule regular backups of critical data and applications. Ensure that backups are stored in geographically redundant locations to protect against regional disasters.
- **Restore Process**: Define clear procedures for restoring data and applications from backups. Ensure that the restore process is regularly tested to verify its effectiveness.

7. Communication Plan

- **Internal Communication**: Establish a communication plan to keep all employees informed during a disaster. Use Azure Communication Services to facilitate real-time communication and collaboration.
- **External Communication**: Inform customers, partners, and stakeholders about the status of operations and any potential impact on services. Use Azure's communication tools to ensure timely and accurate updates.

8. Roles and Responsibilities

- **BCP Team**: Designate a Business Continuity Planning team responsible for developing, implementing, and maintaining the BCP.
- **IT Team**: Ensure the proper configuration and maintenance of Corporate IT Assets and Azure services used for disaster recovery and business continuity.
- **All Employees**: Participate in regular training and drills to stay prepared for potential disasters.

9. Continuous Improvement

- **Review and Update**: Regularly review and update the BCP to reflect changes in the business environment, technology, and potential risks.
- **Feedback Loop**: Establish a feedback loop to gather insights from disaster recovery drills and actual incidents. Use this feedback to improve the BCP continuously.

By leveraging Microsoft Azure's comprehensive suite of cloud services, SmartSort can ensure the continuity of operations and minimize the impact of disasters on our business.

SECURITY MEASURES

SmartSort makes all reasonable efforts to comply with appropriate Privacy Laws and, when applicable, the Data Protection Agreement ("DPA"), which may require additional security controls. These Security Measures are intended to supplement the Business Continuity Plan, as an internal goal and means of protecting shareholder value.

Given that the SmartSort Systems are connected via a cellular router, and not connected to the customers LAN, our security measures are disclosed in this brief as a means of conveying understanding and a commitment to secure SmartSort's infrastructure and applications, including our intellectual property, not as a means of protecting integration amongst Customer related infrastructure and applications.

The Edge Device - Smart Bin, known as an Intelligent Processing Unit (IPU), or a lower-end Connected Processing Unit (CPU), is synced with a Microsoft Azure Cloud environment, which hosts SmartSort's proprietary Material Information Exchange (MIE) Platform.

Encryption occurs locally, on the edge device, between the Computer Vision Application capturing waste item images during object detection, which are stored locally on an encrypted database, generated what is known as a Material Disposal Event (MDE), which is then synced and encrypted with the MIE application in the Azure environment, associating the MDE with Customers and Stakeholders.

All Covered Data / Personal Data resides in the Microsoft Cloud environment, encrypted at rest and in transit.

1. Cybersecurity

This Section identifies SmartSort's cybersecurity requirements.

1.1. Information Security

1.1.1. SmartSort must implement policies and procedures to provide a data protection policy consistent with the requirements of Applicable Law, these Security Measures and the DPA.

1.1.2. SmartSort shall identify a person or organization responsible for managing information security risks.

1.2. Network Security

1.2.1. SmartSort must implement policies and procedures to ensure that network systems are well designed and properly configured to ensure that only authorized network traffic is transmitted over networks. These policies and procedures must include:

1.2.1.1. Controls to permit passing of only approved types of network traffic and block unapproved traffic;

1.2.1.2. Network segmentation and isolation;

1.2.1.3. Monitoring to ensure the controls and configurations of network devices comply with these Security Measures;

1.2.1.4. Strict access control to any physical or wireless networks, with access restricted to authorized personnel only;

1.2.1.5. Prevention of the deployment of unauthorized wireless networks; and,

1.2.1.6. Policies and controls regarding the access of personally owned computing devices to SmartSort's corporate network and other IT infrastructure.

1.3. Physical Security

1.3.1. Physical and environmental security controls are in place to prevent unauthorized physical access, damage and interference to SmartSort's processing facilities hosting Covered Data. SmartSort or SmartSort's third-party data center service Suppliers adhere to the following controls.

1.3.1.1. **Data Center Security.** Data centers hosting Customer Data have physical security controls in place to prevent unauthorized access, including, but not limited to, perimeter controls such as fencing, walls, security staff, video surveillance, and intrusion detection systems.

1.3.1.2. **Environmental Security**. With respect to Customer Data, data centers maintain power, fire detection, fire suppression, climate and temperature controls to limit the risk related to environmental interference, including but not limited to second floor flood protection, dual UPS, generator power backup systems, redundant telecommunications routing and multiple HVAC environmental systems.

1.3.2. **Physical Storage Device Decommissioning**. Where SmartSort is managing the physical media, SmartSort has established rules for the safe and permanent destruction of Customer Data stored on physical media. When a storage device has reached the end of its useful life, decommissioning processes are designed and in place to prevent Customer Data from being exposed to unauthorized individuals.

1.4. Encryption

1.4.1. With respect to Customer Data, all data transmission supporting business with SmartSort Customers must be encrypted, at a minimum using 256-bit encryption per NIST 800-131Ar2 as provided by native encryption solutions supported on the storage platform or using secure communication channels such as IPSEC VPN, industry accepted implementations of TLS, etc.

1.4.2. With respect to Customer Data, applications, data storage and network devices must use cryptographic algorithms defined per NIST 800-131Ar2 or NSA Suite B as provided by native encryption solutions supported on the storage platform or using secure communication channels such as IPSEC VPN, industry accepted implementations of TLS, etc.

1.4.3. Wireless networks connected to SmartSort networks shall implement strong encryption for authentication and transmission.

1.4.4. An encrypted VPN or other equivalent secure remote access solution is required for SmartSort personnel to remotely access production systems containing Customer Data.

1.5. Anti-Malware, Secure Patch and Vulnerability Management

1.5.1. SmartSort must have industry standard tools and processes in place to prevent, detect and contain any attacks on, or unauthorized access to, its IT network infrastructure devices and client devices (e.g., Smart Bins, including computers, cellular routers, power distribution systems, and displays). SmartSort must review and update its threat identification processes on a yearly basis. Vulnerability remediation efforts must be tracked, monitored, and verified.

1.5.2. SmartSort must have a vulnerability reporting program in place for the safe and timely internal remediation of vulnerabilities, threats, and exploits.

1.5.3. To the extent applicable to the device, all devices used for the management of Solutions related to SmartSort's business must have an active and up-to-date anti-malware solution installed.

1.5.4. Web and email traffic processed by the SmartSort infrastructure must be scanned with anti-malware solutions.

1.5.5. To the extent applicable to the infrastructure or applications, Security patches that affect SmartSort infrastructure and applications supporting Solutions must be deployed as soon as available, and in any case within the recommended timeframe of 30 days for high-risk vulnerabilities and 90 days for medium and low-risk vulnerabilities.

1.5.5.1. Applications and infrastructure under the direct control of SmartSort and used for storing and/or processing Covered Data must be maintained to the latest security patching levels, including minimum version levels (to the extent this is not client dependent).

1.5.5.2. Deployment of patches must follow a formal change management process.

1.5.5.3. Exceptions to patching must be communicated to SmartSort via email to the SmartSort Cyber Security Team (infosec@smartsortai.com), and simultaneously documented with patch testing results, a short-term remediation date and acceptance of risk in writing by the SmartSort official or organization responsible for managing information security risks.

1.5.5.4. To the extent applicable to SmartSort and as commercially reasonable, SmartSort must replace all system components when support for the components are no longer available from the developer, vendor or manufacturer.

1.5.6. SmartSort has one or more of the following executable restrictions in place:

1.5.6.1. Windows Security Settings: Software Restriction Policies

1.5.6.2. Other technology in place to prevent unauthorized executables from running

1.5.6.3. Organization has macros turned off into the policies

1.5.7. SmartSort has email protective measures in place that include:

1.5.7.1. Custom filtering,

1.5.7.2. Anti-Spam, and

1.5.7.3. Anti-Phishing

1.5.7.4. Anti-Spoofing

1.6. Vulnerability Management

1.6.1. **Vulnerability Scanning.** Information security personnel perform vulnerability assessments on the Cloud Solution's production infrastructure on at least a quarterly basis. Upon Customer's request, SmartSort shall provide to Customer the results of the most recent network and infrastructure vulnerability scans of its systems and environments used to develop, host, or interact with the Cloud Solution.

1.6.2. **Penetration Testing.** Internal or external penetration tests are performed on the Cloud Solution production infrastructure on at least an annual basis. For the avoidance of doubt, the scope of SmartSort's penetration tests will test the security controls at an infrastructure-wide level, and not at the level of each customer instance of the Cloud Solutions. The penetration test will include but not be limited to tests to detect vulnerabilities listed in the SANS Critical Security Controls for Effective Cyber Defense or the Open Web Application Security Project ("OWASP") current at the time of the penetration test. SmartSort will perform appropriate mitigations to address issues identified and provide a summary of the most recent penetration test and security evaluation to the Customer's Security Team upon request. Upon Customer's request, SmartSort shall provide to Customer the results of any penetration tests of its systems and environments used to develop, host, or interact with the Cloud Solution.

1.6.3. **Vulnerability Response.** SmartSort shall comply with all applicable provisions of the Security Measures - with respect to its identification, management, and disclosure of vulnerabilities in the Software.

1.7. Segregation of Duties

1.7.1. SmartSort organizations that are responsible for architecting, designing, developing, managing and/or supporting systems that store and/or process Customer Data must be structured such that no one individual has the ability or access necessary to solely perform every key aspect of a transaction, event or process.

1.7.2. Where segregation of duties and system access cannot be consistently maintained by an organization or team, the SmartSort must have a formal governance process in place that will rank the risk of non-adherence.

1.8. Internal Access Controls for SmartSort Employees and Subcontractors

1.8.1. Access to Covered Data must be controlled in accordance with these Security Measures, SmartSort company policies, and all standards, procedures and Applicable Law, and all applicable legal, contractual restrictions set forth by Customers in the Agreement. Such controls must protect against any unauthorized access.

1.8.2. Business users must be granted appropriate access based on their role, following the principles of "least privilege" and "need to know". Role-based access lists (i.e., group profiles) should be used whenever possible.

1.8.3. Access credentials may not be group-based or team-based. Each individual user must have auditable user account credentials.

1.8.4. All user and administrator accounts must have an auditable trail of request, approval, creation, modification, recertification, and removals actions.

1.8.5. Access privileges must be reviewed at least quarterly to determine if access rights remain appropriate for a user's job duties.

1.8.6. SmartSort Employee User accounts must be disabled immediately, but no later than 24-hours, upon the user's termination of employment. Access must be modified immediately, but no later than 24-hours, as appropriate upon any modification of a user's employment role. Customer User accounts and Stakeholder User accounts must be disabled immediately, but not later than 72-hours, after notification, as appropriate upon any modification of a Customer or Stakeholders User's employment role. Customer and Stakeholder must provide notification to said employee's change in role or termination.

1.8.7. Systems used in the provision of the Cloud Solution are configured to authenticate Customer and Stakeholder personnel with a unique user ID and password, including multifactor authentication (where supported, provided that multifactor authentication must be implemented for all remote access by SmartSort, Customer, and Stakeholder personnel). Memorized secrets and passwords must meet the guidelines set out in NIST Special Publication 800-63B or, at a minimum, the requirements listed below when they are created, changed, or handled:

1.9. Passwords must not be shared between users or accounts;

1.9.1. Passwords must be a minimum of 14 characters, or 16 characters for privileged/ administrator accounts;

1.9.2. Passwords must contain 3 of the following: uppercase, lowercase, numeric, non-alphanumeric and any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase;

1.9.3. Passwords must be changed upon a user's first login, or after any password reset, but only by the account owner;

1.9.4. Passwords must be changed at least every 90 days. The number of unique new passwords a user must select before an old password can be reused is 10; and,

1.9.5. Default passwords must be changed upon system implementation.

1.9.6. In addition to a valid user ID, users accessing SmartSort applications outside of the SmartSort's network require a second form of authentication to log in to his/her account (e.g., a Two-Factor Authentication ("2FA") token).

1.9.7. If SmartSort allows third parties to access its network remotely, then (a) the Supplier must have policies and controls in place to secure such access and (b) network traffic between the remote client and the Supplier's network must be encrypted.

1.10. Logging and Alerting Controls

1.10.1. SmartSort must record and retain access and system logs from infrastructure host and server operating systems, network perimeter access control systems, databases and critical applications for a minimum of ninety (90) days.

1.10.2. Logs must provide enough details to assist in the identification of the source of an issue and enable a sequence of events to be recreated. Logs must record the date, time and source location (e.g., Internet Protocol address/hostname) for all network access attempts. Logs must capture system and network security event information, alerts, failures, events and errors.

1.10.3. Logs must be stored in a central location to preserve the integrity and security of the logs. The integrity of log files must be maintained and protected from tampering by restricting access to systems that store log information.

1.10.4. Monitoring requirements must be considered during the implementation of new IT resources and should be designed to reflect the classification of the asset and the criticality of the services it provides.

1.10.5. SmartSort shall maintain an IPS and/or IDS system.

1.10.6. SmartSort shall maintain evidence that the IDS/IPS is actively managed.

1.10.7. IDS/IPS software shall be updated to the most recent patch levels.

1.10.8. IDS/IPS signatures must be updated to the most recent patch levels.

1.10.9. IDS/IPS custom signatures must be implemented by the SmartSort.

1.10.10. SmartSort must maintain an automated IDS incident notification.

1.11. Incident Management and Reporting

1.11.1. SmartSort must maintain data privacy and cyber risk insurance coverage with a minimum of one million United States dollars ($1,000,000 USD) per occurrence and a minimum of one million United States dollars ($1,000,000) aggregate.

1.11.2. SmartSort must maintain an incident response policy and procedures compliant with Applicable Law. The incident response policy and procedure should be reviewed on an annual basis to ensure the appropriate roles and teams are up to date.

1.11.3. To the extent SmartSort has any knowledge of such Security Incidents, SmartSort must inform Customers and Stakeholder of any Security Incidents as soon as possible and under no circumstances later than 96 hours from the time of SmartSort's awareness thereof. Security Incidents include, but are not limited to, the following (but this list specifically excludes Unsuccessful Security Incidents for which SmartSort is under no reporting obligation):

1.11.3.1. Virus/Malware/Ransomware infection;

1.11.3.2. Verified phishing/scam which yields harvested credentials from SmartSort employees or contractors;

1.11.3.3. A breach of Covered Data;

1.11.3.4. Deliberate attempted password misuse;

1.11.3.5. Suspicious/inappropriate handling of Covered Data;

1.11.3.6. Suspected server/workstation compromise;

1.11.3.7. Denial of service; and,

1.11.3.8. Malicious internal or external intrusion.

1.11.3.9. Product vulnerabilities (software/firmware)

1.11.4. Logs must be maintained for all observed or suspected information Security Incidents in compliance with applicable Privacy Laws and must be made available to Customer upon request.

1.11.5. Following the occurrence of a Security Incident, SmartSort will permit Customers to perform a virtual and an on-site assessment (subject to SmartSort's discretion) of the administrative, physical and logical security controls used at SmartSort's business facilities in order to assess the impact to Customer and Stakeholder of the security event even if an assessment has been completed within the year. Customer, Stakeholder and SmartSort will each bear its own costs for security assessments resulting from security events.

2. Security Management Systems

2.1.1. Critical Security Systems and Processes

2.1.2. SmartSort shall implement and maintain a comprehensive security program with defined roles and responsibilities that ensures security requirements are identified and implemented to protect the confidentiality, integrity and availability of SmartSort, Customers, and Stakeholders resources, information and materials. The security program must include processes and allocated responsibility to ensure security risks are identified and mitigated and ensure that a formal risk assessment is conducted at least annually. The program must ensure audits and assessments are conducted to ensure security requirements are being maintained and managed, and that any identified nonconformities are remediated in a timely manner.

2.1.3. SmartSort must have a documented risk management program which evaluates organizational and administrative risks and performs ongoing risk identification, prioritization and mitigation efforts quarterly.

2.1.4. Information Security Policy: SmartSort shall maintain an Information Security Policy that is communicated to employees, contractors and vendors and approved annually and is aligned with industry standard leading practices (e.g., ISO 27001). This documentation must include current emergency customer and local management contacts to be contacted in case of security incidents.

2.1.4.1. Cloud Security: SmartSort must have a cloud security policy in place that ensures that the use of cloud services is managed, which at a minimum must include the following:

2.1.4.2. SmartSort must encrypt all information and/or data by using current industry-standard strong encryption, key management and related standards (NIST 800-53 Rev 4), when processing, transmitting and/or storing Covered Data in any public cloud infrastructure; provided, that this requirement shall not apply to

any data transmission between the Cloud Solution and the Customer's public/private cloud Supplier to the extent that Faction provides interconnection services to the Customer in support of such transmissions.

2.1.4.3. SmartSort must ensure that subcontractors providing cloud services adhere to the most recently published version of ISO/IEC 27001.

2.1.5. Backup & Restore: SmartSort will maintain a secure backup of any critical data for purposes of SmartSort's business continuity and will also maintain backups of Customer Data as required or requested by Customer. Further, SmartSort represents and warrants that it has a business continuity plan in place which is commercially reasonable for the products and services provided, and which at least meets industry standards. and will also maintain backups of.

2.2. Access to backups should be limited to a small group of users which is monitored and reviewed monthly.

2.3. SmartSort must prevent the unauthorized disclosure of computer files containing product keys when operating computer backup equipment.

2.4. Security systems and tools, including, but not limited to, security access control systems and Closed-Circuit Television (CCTV), must have functioning failover and backup capability such that required records, images and video, and data are not lost by SmartSort.

2.4.1. SmartSort has an audit program which prescribes the frequency, methods, responsibilities, planning requirements and reporting for the Cloud Solution SmartSort will conduct audits of the security of the systems, networks, computing environment and physical data centers that it uses in the provision of the services to Customer. Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually. The types of audits will depend on the applicable Cloud Solution and may include ISO 27001, SOC1, SOC2, HIPAA, PCI, FedRAMP and other industry assessments and certifications. Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework. Each audit will be performed by qualified, independent, third-party security auditors at SmartSort's selection and expense. Each audit will result in the generation of an audit report ("Audit Report"). The Audit Report will be SmartSort's Confidential Information and will clearly disclose any material findings by the auditor. SmartSort will endeavor to remediate issues raised in the relevant Audit Report. Upon Customer's reasonable request, SmartSort will provide Customer with the relevant Audit Report(s). Customer may provide SmartSort's Audit Report(s) to its Customers, so long as such SmartSort Audit Reports are covered by a confidentiality agreement between SmartSort's Customer and Customer's Customer protecting such information. Customer's right to provide SmartSort's Audit Report(s) will cease when Customer is able to achieve and provide equivalent Customer audit reports to Customer's Customers.

2.4.2. SmartSort continually improves the suitability, adequacy and effectiveness of the information security management system. As a part of the continual improvement process, SmartSort uses internal and external audit results as a means to measure the design and

effectiveness of the information security controls. As findings are identified, remediation plans are developed and then implemented.

2.5. Secure File & Data Deletion:

2.5.1. Upon notification by Customer, and if SmartSort has proper access and is responsible for handling such deletions, SmartSort will ensure that computer files and/or other media devices containing Customer Data / Personal Data or customer-specific Covered Data are deleted from computer systems in a secure manner once the Cloud Solutions have been terminated.

2.5.2. If SmartSort is responsible for deletions pursuant to Section 2.5.1 above, then it will provide a certificate of data destruction signed by the executive or officer who has oversight of the team or department responsible for such destruction.

2.6. Personnel Security

2.6.1. SmartSort performs screening/background checks on employees who have access to Covered Data in accordance with applicable law and SmartSort policies.

2.6.2. SmartSort ensures that any person authorized by SmartSort to process Covered Data is subject to an obligation of confidentiality.

2.6.3. Training for the topics identified in this section must occur at least annually, or as specific items change (such as new lines of business, equipment or process changes, disclosure changes, or other changes that may impact how security is implemented at the site).

2.6.4. SmartSort must document all training it conducts in accordance with these Security Measures, including the content provided, the dates conducted, and the personnel trained. SmartSort must retain such documentation for a minimum of four (4) years.

2.6.5. Information Security Training: All SmartSort employees must receive privacy, data protection and information security training at the time of hiring and onboarding (within 90 days of each) and repeated on an annual basis. Training must address the following as described in the DPA:

2.6.5.1. Information security threats and best practices;

2.6.5.2. Phishing and awareness campaigns,

2.6.5.3. Information security and data privacy policies, procedures and controls in place to protect Covered Data; and

2.6.5.4. Each representative's roles and responsibilities in the protection of Covered Data**.**

2.6.6. Incident Response Training: All SmartSort personnel with access to products sold to Customer, including those with indirect access by means of administrative privilege, must receive annual training on the Standards, as well as on information security principles that, at a minimum, review the following:

2.6.6.1. Incident response processes, including when to implement such processes, and any related and required actions that must be taken in relation thereto;

2.6.6.2. Simulated events and automated mechanisms to facilitate effective response by personnel in crisis situations; and,

2.6.6.3. Methods that prevent various security incidents, such as identifying and understanding the risks of downloading malicious software**.**

2.6.7. SmartSort must provide and communicate a means for all SmartSort personnel to anonymously report illegal or suspicious activity relating to any products sold to Customer or Covered Data.

2.7. Operational Security

2.7.1. **Asset Inventory.** Where applicable, SmartSort maintains an inventory of all media on which Customer information is stored. Access to the inventories of such media is restricted to SmartSort personnel authorized in writing to have such access.

2.7.2. **Asset Handling.** SmartSort classifies Customer information to help identify it and to allow for access to it to be appropriately restricted. Where applicable, SmartSort imposes restrictions on printing Customer information and has procedures for disposing of printed materials that contain Customer information. SmartSort personnel must obtain SmartSort authorization prior to storing Customer information on portable devices, or remotely accessing Customer information.

2.7.3. **Change Management Process**. Change management processes are in place to ensure appropriate reviews and authorizations are in place prior to implementing any new technologies or changes within the production environment of the Cloud Solution.

3. Audit

3.1. Notwithstanding any otherwise applicable limitations on the frequency of audits, in the event of a material breach of these Security Measures by SmartSort or upon the request of a regulatory entity, Customer may initiate an audit by providing at least 7 days advance notice prior to such audit to SmartSort.

3.2. In connection with any audit of SmartSort's compliance with these Security Measures, SmartSort shall provide Customer with written remediation plans, including specific action and target timescales for any non-compliance identified against the requirements hereof.

3.3. SmartSort shall provide independent assurances over its business and information technology controls applicable to the Cloud Solution, by providing a Service Organization Report based on the Statement of Standards for Attestation Engagement No. 18 (SSAE 18) ("SOC Report") or equivalent information security certification report (e.g., ISO 27001), Such SOC Report(s) shall cover all controls and security processes and procedures that SmartSort and its subservice organizations perform in accordance with the Agreement including without limitation these Security Measures and be in the form of a SOC I Type II and SOC 2 Type II report, as applicable. The reporting period for the SOC Reports shall be for SmartSort's standard yearly period and SmartSort shall provide Customer or its authorized external auditor with copies of such relevant reports upon Customer's request; provided, however, SmartSort shall use reasonable efforts to deliver such SOC Report(s) no later than November 15th of each year, if Customer has requested the report. To bridge any gap between the audit end date and December 31st of each year, SmartSort shall provide Customer additional affirmation

of ongoing control operating effectiveness. If a SOC Report from SmartSort's retained third-party auditors yields deviations, SmartSort shall communicate an action plan within 30 days of the date of issuance of such SOC Report and provide Customer with periodic updates until such deviations have been remediated, retested and deemed resolved by such third-party auditors. The audit shall be at SmartSort's expense as part of SmartSort's ongoing information security program to evaluate SmartSort's general security controls.

4. Definitions

4.1. **"Covered Data":** any data or information (such as electronic files, materials, data, text, audio, video, images, etc.) uploaded, transmitted, stored, retrieved, processed, submitted, or otherwise made available by Customer in connection with the services or products provided by SmartSort. This includes any Personal Data or personally identifiable information provided to SmartSort in connection with the Agreement.

4.2. **"De-Identified Data":** De-Identifiable Data" refers to data that has been processed to remove or obscure Covered Data / Personal Data, so that the remaining information cannot be used to identify an individual or legal entity. This process is known as de-identification. The data resulting in de-identification is owned exclusively by SmartSort.

4.3. **"Intellectual Property"** or "**IP**": Any and all intellectual property rights worldwide arising under statutory or common law, including, without limitation, that which is acquired or obtained under a contract with a Customer, Stakeholder, or any third party, and whether or not perfected, comprised of any of the following: (a) copyrights, copyright applications, copyright registrations; (b) mask work rights and mask work registrations; (c) designs, inventions, discoveries and rights arising from or related to all classes or types of patents, utility models and design patents (including, without limitation, originals, divisions, continuations, continuations-in-part, extensions or reissues) issued or issue-able thereon, and applications for these classes or types of patent rights; (d) any trade secrets and any know-how; (e) any right analogous to those set forth herein in foreign jurisdictions; and (f) any renewals or extensions of the foregoing (as and to the extent applicable) now existing, hereafter filed, issued or acquired.

4.4. **"IDS"**: intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. A system that monitors important operating system files is an example of an HIDS, while a system that analyzes incoming network traffic is an example of a NIDS.

4.5. **"IPS"**: An intrusion prevention system (IPS) is a system that monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, and then log information, attempt to block the activity, and then finally to report it.

4.6. **"Personal Data**": means any information relating to (i) an identified or identifiable person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws.

4.7. **"Security Incident"**: An incident or realized scenario that involves or may involve accidental, unlawful, or unauthorized destruction, alteration, disclosure, misuse, loss, theft, access, copying, use, modification, disposal, compromise, or access to any Covered Data hosted or

maintained by SmartSort, or any security-related incident which has the reasonable potential to cause harm to Customer, the Customer brand, Customer's Customer relationships, or to any Customer asset (ex. people, facility, equipment, etc.). The Parties acknowledge and agree that this constitutes notice by SmartSort to Customer of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Customer will be required. "Unsuccessful Security Incidents" include, but are not limited to, pings and other broadcast attacks on SmartSort's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of any Covered Data.

5. Systems

5.1. Any of SmartSort's electronic infrastructure, including all computer systems, software, hardware, networks, databases, electronics, platforms, servers, interfaces, applications, websites, devices, products, Cloud Solution, edge solutions, and related information technology systems and services, used, accessed by or made accessible to SmartSort or Customer.

Secure Software Development

SmartSort shall follow a documented SDL process ("**SDL Program**") based upon industry standards and best practices (i.e., SAFECode, ISO 27034, NIST Secure Software Development Framework, or equivalent). For the avoidance of doubt, all references to the Cloud Solution in this Annex include any or all non-proprietary or IP related source or build code components used or provided to Customer as part of the Cloud Solution.

1. The SDL Program shall:

    a. implement a governance structure that provides management oversight to SmartSort's SDL Program, including review and approval of the Cloud Solution's compliance with applicable Security Requirements;

    b. require SmartSort to baseline new releases (e.g., original releases, patches, and updates) of the Cloud Solution, against Customer's Security Requirements prior to release and document any gaps. Any security vulnerabilities uncovered as part of this security assessment and impacting supported products shall be addressed per the vulnerability remediation timeline set forth In 1.5. Anti-Malware, Secure Patch and Vulnerability Management, section 1.5.5.;

    c. ensure that product security is addressed throughout the development lifecycle including through security requirements review, threat modeling, static and dynamic security testing, secure code reviews, penetration testing, third party dependencies, risk assessment, vulnerability remediation and response.

    d. implement and maintain controls to identify and remediate security vulnerabilities and weaknesses in the Cloud Solution, such as static/dynamic code analysis, vulnerability scanning and penetration testing, during development, and test such software/firmware to ensure it is free of errors such as, at a minimum, those listed in "CWE/SANS Top 25" (http://cwe.mitre.org) and/or "OWASP TOP 10"

(http://www.owasp.org), as applicable, at the time of delivery and in subsequent releases;

e. ensure that all third-party components of the Cloud Solution (excluding any components provided to SmartSort by Customer) are inventoried and tracked throughout the software's life cycle;

f. at Customer's request, (i) provide a machine readable software bill of materials ("SBOM") identifying each third party component in the Cloud Solution (excluding any components provided to SmartSort by Customer) and identifying baseline information on each identified component, consistent with applicable guidance issued by the National Telecommunications and Information Administration (NTIA), or (ii) provide scan results of open source software manager and/or software composition analysis tools (e.g., BlackDuck, WhiteSource);

g. contractually require any third party that provides SmartSort with closed source components used in the Cloud Solution to implement an SDL Program that meets the requirements set forth in this Section. SmartSort must further obtain and, at Customers's written request, be able to provide a self-certification from such third party that its development practices comply with the requirements of this Section. To the extent this Section 2(g) is applicable to components provided to SmartSort by Customer, then Customer agrees that it has an SDL Program that meets the requirements set forth in this Section.

2. SmartSort shall make available, upon Customer's request, documentation of SmartSort's SDL Program sufficient to demonstrate compliance with the requirements of the Customers Agreement and these Security Measures, including but not limited to the results of SmartSort's ongoing threat modeling activities, excluding all intellectual property (i.e., data flow diagrams). Customer may further request that SmartSort self-certify that its development practices comply with the requirements of its documented SDL Program and this Section.

3. SmartSort must use reasonable efforts to ensure that the Cloud Solution does not contain malware through use of up-to-date commercial malware detection tools as part of its code acceptance and development processes prior to release.

4. SmartSort must ensure at the time of release that the Cloud Solution does not contain any undocumented methods or components that provide unauthorized access to third parties (e.g., backdoors).

5. If SmartSort uses a Customers-provided Register Transfer Level (RTL) on Complex Programmable Logic Devices (CPLD) or Field Programmable Gate Arrays (FPGA) it shall have a process to ensure the integrity of the RTL used on such devices.

6. SmartSort shall demonstrate the authenticity and integrity of the Cloud Solution's code provided to Customer by digitally signing, distributing verifiable product code from a trusted website, or other method as agreed to by the parties.

7. SmartSort shall train developers on an ongoing basis on secure engineering practices consistent with changing practices and the then-current threat landscape.

Vulnerability Response and Disclosure

1. SmartSort shall implement and follow a documented vulnerability response program/process based upon industry standards and best practices (e.g., FIRST PSIRT Services Framework, ISO 29147, ISO 30111, or similar).

2. SmartSort shall have measures in place to continuously monitor external security advisory sources (e.g., cooperative security tests, external security research, open source and third-party disclosures) to identify and track any vulnerabilities in the non-Customer-provided components of the Cloud Solution that may impact Customer Data or the Cloud Solution, including third party components.

3. SmartSort shall remediate all identified vulnerabilities in the Cloud Solution affecting non-Customer-provided components ("**SmartSort Software Vulnerabilities**") with a CVSSv3 base score greater than or equal to 4, regardless of source of discovery (e.g., Customer, internal, third-party researcher, open source, SmartSort, pen-testing, SDL, etc.).

4. If SmartSort receives reports from Customer of a SmartSort Software Vulnerability, SmartSort shall provide to Customer:

    - within **five (5) business days** of Customer reporting the security vulnerability, confirmation of the security vulnerability or a detailed response summarizing its reasonable basis for denying the security vulnerability; and

    - within **ten (10) business days** of confirmation of the security vulnerability, a remediation plan and share information with Customer, including the applicable CVE, CVSS score and components affected.

5. For any publicly known or Customer-reported SmartSort Software Vulnerabilities with a base score greater than or equal to 4, as defined by Common Vulnerability Scoring System v3 (CVSS), SmartSort shall promptly remediate and/or implement a temporary fix, as applicable, on a timeline commensurate with risk and in accordance with the following timeframes, unless otherwise agreed to by Customer.

CVSSv3 base score	**Maximum time to provide a Temporary Fix**	**Maximum time to provide an Official Fix**
9.0-10.0	**seven (7)** calendar days	earlier of the next available release or within **thirty (30)** calendar days
7.0 - 8.9	not applicable	earlier of the next available release or within **thirty (30)** calendar days
4.0 – 6.9	not applicable	**ninety (90)** calendar days

6. SmartSort's use of third-party components shall not alter SmartSort's responsibility to identify and remediate vulnerabilities as described herein. SmartSort shall have a system to be notified of all publicly released third-party vulnerabilities in its software/firmware and components and to evaluate applicability thereof. SmartSort must also ensure that Open-Source Software & Third-Party Code included in new product releases are recent and still supported.

7. Upon remediating a SmartSort Software Vulnerability, SmartSort shall have a process to communicate the following information to Customer, as applicable:

    a. a description of the security vulnerability, including the potential scope of risk to Cloud Solutions, and the versions of SmartSort code impacted;

    b. the remedy information and location (e.g., patch, maintenance update, or product version upgrade);

    c. the Common Vulnerabilities and Exposures (CVE) ID (where applicable); and

    d. any other relevant information on workarounds or mitigating options for the security vulnerability.

8. If there is a known mitigation or workaround for a vulnerability, SmartSort agrees to notify Customer of the mitigation as soon as it is known, even if the issue is not yet publicly known.

9. To promote coordinated disclosure, SmartSort shall provide Customer with **at least ten (10) business days advance** written notice before publicly disclosing SmartSort Software Vulnerabilities. SmartSort shall coordinate with the Customer Cyber Security Team regarding the content of any such public disclosure. In the case that SmartSort must make an emergency response to a security vulnerability publicly disclosed by a third party, SmartSort shall coordinate with the Customer Product Security Incident Response Team as soon as possible. SmartSort shall provide Customer with information, which Customer reasonably requests, to identify and understand the security vulnerability and validate the remedy.

10. SmartSort shall provide Customer written notice about the impact and remediation plan for any **high-profile** (e.g., publicly acknowledged vulnerabilities, zero-day exploits, actively exploited issues, high media attention issues, "branded" issues, publicly-known issues with proof of concept attack, etc.) issue, for which advance notification was infeasible, **within five (5) business days** of public acknowledgement/media reporting. For such high-profile issues, Customer expects an expedited remediation and may request an expedited remediation timeline, as mutually agreed to by the parties.

11. If at any time SmartSort deems that a SmartSort Software Vulnerability (regardless of CVSS score) poses significant risk to Customer and cannot be addressed in accordance with SmartSort's applicable remediation timeframe, SmartSort shall provide Customer information about the issue, any known workarounds or mitigations and any options to turn off the related code.

12. SmartSort shall limit sharing of non-remediated issues and follow industry coordinated vulnerability disclosure practices.