Exhibit (C)

Operational Policy & Procedures Manual

TABLE OF CONTENTS

1 EMPLOYEE AND SUBCONTRACTOR SCREENING

1.1 Non-Access and Access Employee Paperwork

Management will maintain on file the following documentation for all employees, whether their position grants them physical access ("Access Employee") to confidential material or not ("Non-Access Employee"):

- I-9 or similar documentation verifying an employee's legal right to work in a particular country.
- Confidentiality Agreement attesting to the employee's understanding that they will be exposed to confidential material and that they agree to maintain and protect the confidentiality of all information taken into custody by the company.
- Copy of a current driver's license (drivers only)
- Acknowledgement of Operational Policies
- CCW (if applicable)

1.2 Access Employee Criminal Background Checks

Prior to being granted access to confidential material, all Access Employees will have an initial criminal background investigation completed by a third party to verify that the employee has not been convicted of a theft-related felony in the last 7 years. The criminal background investigation is to include the following:

- Social Security Trace (or Social Security Header Search): A report of all names and addresses associated with a social security number
- Federal records search for all Federal Districts in all states on the Social Security Header Search reported within the last 7 years
- Statewide records search for all states on Social Security Header Search reported within the last 7 years
- County records search for all counties on Social Security Header Search reported within the last 7 years

In addition to initial screening, all Access Employees are subject to ongoing criminal background investigation checks. Any employee convicted of a theft-related felony during their employment with the company will be removed from a position where they have access to confidential material.

1.3 Access Employee Drug Screening

Prior to being granted access to confidential material, all Access Employees must have an initial drug screening. In addition to this initial screening, 50% of all Access Employees are subject to random drug screenings on an annual basis.

1.4 Access Employee Prior Employment Verification

Prior to being granted access to confidential material, all Access Employees will have the previous 7 years of employment history verified by management.

1.5 Subcontractor Screening

NAID Certification requires that the Company maintain secure control over all material from the moment the custody of the material is transferred from the customer, throughout all stages of the process, i.e. transportation, staging and destruction, until the material is destroyed and responsibly disposed. It may become necessary from time to time to subcontract all or a portion of this process to other organizations, of which the Company has no immediate or direct control. In order to ensure that our customers continue to receive a secure certified service when fiduciary responsibility is transferred to a subcontractor, management will adhere to the following procedures for all situations in which a subcontractor is used:

- Customer notification:
    - Notify customers in writing of the use of a subcontractor. This notification must identify the parties destined to accept custody, the exact location of destruction and the method of destruction.
    - This written notification will be included in all bids or proposals, whenever applicable, if this information is known at the time of the bid or proposal, as well as prior to or at the time the service is rendered.
    - If the subcontractor performing destruction services is not NAID Certified, this will also be included in the customer notification.

- Obtain the following written acknowledgments from the subcontractor(s):

    - All individuals of the subcontractor companies or agents in the chain of custody, including third party transporters, understand that the media they come into contact with may be confidential and the subcontractor accepts fiduciary responsibility of the material.
    - All employees and individuals in the subsequent chain of custody submit to the same background screening required for NAID Certification.
    - All agents subsequently accepting custody of media must meet the current NAID Certification specifications for all applicable criteria.

2 PLANT-BASED DESTRUCTION FACILITY PROCEDURES

2.1 Access to Facility

This company desires to keep a secure environment for all employees with the following rules and regulations:

- Only Management and designated employee representatives will be allowed to have keys to the facility.
- Employees are not allowed on the company's property after hours without prior authorization from Management. **See Section 2.7**

2.2 Security Measures at the Facility

In addition to the access limitations, the company utilizes the following security measures:

- Perimeter doors to the company should be secured at all times. Visitors and employees that do not have the security lock combination will be advised by signage to alert the occupants of their presence by pushing a doorbell.
- The use of cameras at the company in areas where confidential materials are located is prohibited without prior authorization from Management. This includes mobile phone cameras.
- Employees may possess firearms, provided a current, state issued CCW permit is maintained in the employees file and with the employee, at the time of "concealed carry", unless prohibited by law or while inside a customer's facility. Any employee found violating this policy may be dismissed. Any employee found violating this policy will be dismissed.

- The outside lights are to be automatically set to be on from dusk to dawn, and inside security lights are to be left on whenever the facility is unattended. It is the responsibility of the Shift Supervisor to control the lighting and to see that all the lights are in working order.
- The fire and burglary alarm shall be activated whenever the facility is left unattended. The contact individual at the company, when an alarm is activated, is a Management/Access individual.
- The company has installed closed circuit internal video security to monitor the ingress and egress from the secured areas of the building. In addition, recorded closed circuit video monitoring with sufficient clarity to identify people and their activity is used at the company in the secured area of the building during the working hours. All monitoring data or tapes will be saved for a minimum of 90 days. **See Section 2.7**
- The company has ensured that there is a secure area within the building devoted only to destroying media. No baling of non-shredded paper may take place in this area except cardboard. OR If a secured area within the building is required, it meets the following specifications:
    - There must be enough space within this area to stage all materials to be destroyed.
    - The wall or fence securing this area must be a minimum of six feet tall and have a lockable gate or door.
    - If the wall or fence does not go all the way to the ceiling, then it must have a ceiling mounted sensor alarm inside and over the perimeter of the secure destruction area (or similar, suitable device) to detect if and when individuals have climbed over or come through a section of the secured area fence/wall.
- Management will complete an Operational Security Maintenance Log to check, record and maintain the facility's operational security functions, Door Locks, Alarms, Lighting and Visitor Logs on a monthly basis. The CCTV system log will be completed on a weekly basis. The company will maintain the Operational Security Maintenance Logs for a minimum of one year.

2.3 Handling Incidents of Unauthorized Access

Every employee at the company should be on guard for unauthorized access to the facility. Any employee noticing a visitor who is not being escorted by an appropriate agent of the company and/or not wearing a current visitor badge,(**See Section 2.7**), should immediately contact Management. The unauthorized visitor should then be escorted to the main reception area to have them sign in and be properly escorted in the facility. At the slightest resistance to cooperation, notify the police immediately. Do not physically restrain the individual in any case. If they leave in a vehicle and the license of that vehicle is discernible, it should be noted for further investigation.

2.4 Reporting Breaches in Security & Safety

All employees at the company are to notify the Management of any breach in the security or safety policies of the company, regardless of its source. Any employee found to have knowledge of a breach in safety or security as stated in the company's policy manual that does not report it may be dismissed. This would also include reading confidential material entrusted to the company.

2.5 The "Nothing Leaves" Policy

As a security measure, employees at the company may take nothing into or out of the destruction area without the permission of Management. As a rule, these materials should be left in the employee's locker. Any employee found taking materials into or out of the destruction area without the knowledge and permission of Management may be terminated without any previous disciplinary action having been taken.

2.6 Daily Facility Preparations/Inspections

The daily operations of the company are the backbone of our success. The following operations procedures are in place at the company to ensure that our success continues:

- Management will complete a visual inspection of the facility at the beginning and end of each shift.
- Management will look for breaches in security, make sure that the floor is completely clean of paper debris and that all conveyors, balers, shredders and other equipment are in proper working order. In the event of any equipment not being operational, Management will be responsible for arranging all necessary repairs as warranted.
- Management will inspect all collection containers used by the company to transport between client, vehicles and facility to make sure the equipment protects confidential materials from loss due to wind or other atmospheric conditions.
- Management is responsible for making sure that all Drivers and Helpers are within the dress code policy and that Identification Badges are utilized.
- Management will inspect the forklifts, checking battery and/or fluid levels. All electrically operated forklifts should be charged during the night, as well as the propane supply for fueled units.
- Management will inspect the company's vehicles to ensure road worthiness and verify that all proper paperwork for the vehicle's most recent inspection comply with the time frames stated in the applicable state law regarding the nature and frequency of inspections.
- Management will inspect the company's vehicles to verify that all cab doors and truck boxes are lockable and that locks work properly.
- Management will assist the Drivers in their preparations for the day. Management can use any or all employees to expedite the departure of the Drivers on a timely basis.

2.7 Operational Security Maintenance Logs

Management will conduct **monthly** checks of the following operational security systems of the plant-based destruction facility and/or transfer processing station:

- Alarm System
    - Motion Detectors: Visually inspect and walk check each sensor. Observe light diodes – blinking indicates motion is detected. Check that the sensor catches movement at appropriate distance – sensor can be adjusted to allow more/less steps before alarm.
    - Door Contacts: Visually inspect for functionality and test for alarm.
    - Key Pads: Visually inspect for functionality and test all circuits, i.e. opening/closing reports. Consider if access code needs to be replaced.
    - Battery Backup: check that battery is still good by removing electrical supply.
    - Monitoring Service: Run an alarm test and confirm with monitoring service and/or attach copy of alarm reports from monitoring service since last reporting.

- Lighting
    - Visually check that all lighting is working properly (including lighting at night for CCTV system).
- Door Locks
    - Check that all doors and fence gate locks into and within facility are working properly.
- Visitor Logs
    - Visitor In/Out Logs: Visually check that logs are being completed properly (both check in and check out are recorded) and filed.
    - Visitor Badges: Ensure sufficient visitor badges are available based on average demand in a day.

Management will conduct **weekly** checks of the following operational security system of the plant-based destruction facility and/or transfer processing station:

- Closed Circuit Television (CCTV)
    - Cameras: Visually inspect for functionality. Check correct field of view so that all individuals and activity can be seen. Clean lenses.
    - Visually check recorder for functionality – no recognizable delay should be seen between each frame/shot on each camera in system.
    - Check most recent seven day records for replay standard. Verify library contains the last 90 days of recording and spot check several dates.
    - Check to see that storage capacity will not be exceeded before 90 day capacity is reached.
    - Notify NAID within 48 hours of any problems related to data storage.

Operational Security Maintenance Check logs must be initialed with any notes or corrective actions recorded. Logs are to be kept for a minimum of one year.

2.8 Receiving Destruction Materials

The company's business is media destruction. The following standards are in place to ensure that the company's facility and employee's provide secured destruction for their clients at all times.

- All materials to be destroyed are always attended by an Access employee or physically secured from unauthorized access while in the custody of the company before they are destroyed. Collection containers with confidential media must never be left unattended, even if they are locked, unless they are secured in a locked company vehicle.
- Company vehicle cabs and boxes must always be secure during transport.
- Management controls the receipt, inspection, weighing, and staging of all materials delivered to the destruction facility.
- All materials are to be weighed/checked in immediately upon delivery to the destruction facility. The material will be unloaded from the truck and separated by client. The containers will be weighed/received and that weight will be submitted to Management. Management will confirm the weight and transfer it onto the client's Receiving Ticket. The receiving ticket should be completed upon receipt of the materials, documenting the name of the client, date, weight of the material, and the driver. Management should also note if the materials are to be staged for other than the standard destruction process or to be destroyed with no sorting. In the event that materials are delivered to the destruction facility during non-operational hours, Management should weigh the materials as soon as possible. Materials should be clearly labeled by the Driver who left them. The associated receiving ticket should be left in the designated location.
- All materials from routine, regular service will enter the destruction process immediately upon arrival at the destruction facility. Incoming service bins will be emptied and rotated among those regularly serviced customers. Exceptions would include acts of God, breakdowns, or client instructions to retain the media for a longer period. The Access employees that are responsible for sorting incoming materials will stage materials in the designated area by the order in which they arrived at the facility.
- At time of media pick-up, the customer must be provided with a receipt or certificate of destruction indicating type and quantity of media being collected and the destruction services being provided for the media/materials collected. This must include the type of service operations (Mobile or Plant-based) and destruction (paper shredding, micro media, computer hard drive, or non-paper media) being provided to the customer. (See Section 3.9)
- Since customers of NAID Certified companies assume that all services provided to them are Certified, the Company must have written notification to the customer when any destruction services rendered are not NAID Certified. This notification should be contained on a materials receipt, certificate of destruction or another written agreement between the service provider and customer. (See Section 1.5)

2.9 Staging Destruction Materials

After materials have been received at the company, proper care should be taken by Access employees in preparing for the physical destruction of the materials. The following steps should be utilized.

- Sorting is to be performed according to the material type designations posted at the sorting station(s). When the materials have been completely sorted, they should be moved to the designated secure holding area.
- Non-information bearing material (unmarked binders, plastic file inserts, among other things) should be placed into the designated bin for storage until Management approves their disposal. If confidential materials are found in the non-information bearing trash, they should be immediately removed and placed in the proper pre-destruction area.

2.10 Destroying of Materials

Efficiency and care should be used once materials are ready for destruction at the company. All destruction of confidential materials received at the company will take place within 3 business days of receipt.
Exceptions to this would have to be made between Management and the client through a written agreement. Guidelines for proper destruction of each specific material are as followed:

- Paper materials should be destroyed by shredding and baled by grade if possible. The specifications for particle sizes should be no larger than those listed below:
    - Continuous Shred: 5/8 inch Width (max) & Indefinite Length
    - Cross Cut or Pierce & Tear: 3/4 inch Width (max) & 2.5 inches Length (max)
    - Pulverized (Equipment w/ Screens): 2 inch diameter (max) Screen holes If adjustable screens are used, Management will be responsible for ensuring that a Screen Changing Log is kept on or near each machine. The log will record the starting point of the log and the pertinent information regarding any screen changes thereafter. The company will maintain the Screen Changing Logs for a minimum of one year. Microfiche or Microfilm can be destroyed by either a disintegrator or by equipment/process which produces a particle size of 1/8 inch maximum dimension or less. Destroyed materials should be properly discarded.
- Computer Hard Drives or CPUs will be recorded by serial numbers and then physically destroyed according to the separate written method provided by management. After the destruction service is completed, management will complete the following
    - A list of recorded serial numbers of destroyed drives will be returned to the customer, unless the client has opted out of serial number recordation by signing a NAID-approved opt-out agreement.
    - Logs of recorded serial numbers, a log of customers that have opted out of serial number recordation, and executed copies of any opt-out agreements will be retained for a period of **three (3) years** after the completion of the service.

- Non-Paper Media (CD's, DVD's, tapes, flash electronic storage devices, x-rays) will be destroyed using the standard method of shredding. If it becomes necessary to deviate from this standard method of destruction for any reason, management will notify the customer in writing of the actual method of destruction.
- Management will decide the appropriate method to use to destroy atypical media or non-media materials that require destruction.
- On a (daily/weekly/monthly) basis, Management will inspect the destroyed materials prior to disposal, to ensure that the destroyed information is within the original equipment manufacture specifications and within certification specifications. (**See Section 3.9**)

2.11 Visitor Sign-in Procedures

All visitors entering the secure destruction building, Transfer Processing Station or Collection Facility must sign a log with their name, time in, affiliation, and time out. Visitors must be issued a visitor badge and escorted or under the supervision of an Access Employee (i.e. an employee, who has full access to the secure destruction area(s)), at all times while in the building. Visitor logs will be maintained for a minimum of one year. (**See Section 2.7**)

2.12 Witnessed Destruction Process

Occasionally a client will need to witness the destruction of materials at the company. Management has the authority to agree to an appointment for witnessed destruction. The company will do its utmost to accommodate the client's needs in scheduling the appointment. Management is responsible for handling all witnessed destruction projects. Materials will be delivered to the facility either by a Driver or by the client. If delivered by the Driver, the materials should be securely stored until the client's representative arrives. The witness must sign the visitor's log and be escorted by an Access employee to the Witnessing Area to watch the destruction process. The process should be conducted as close to the time of the client's arrival as possible.(See Section 2.7)

2.13 Post Destruction Process

Once materials have been properly destroyed, Management will review that all procedures have been followed and that the job has been completed. Management will use the following procedures:

- Management will record the date the materials are destroyed, whether in a batch or singularly, on the receiving ticket.

- Management will inspect containers, boxes or security receptacles to verify they are free of the materials to be destroyed. If confidential materials are found, Management will remove the materials and immediately destroy them. Receptacles or boxes to be returned to clients will be returned on the next scheduled pick-up. The emptied and inspected boxes that are not to be returned to the client will be processed into bales. Security containers owned by the company that are used by the clients will be rotated through a service plan agreed upon by the client and the company. Any unused security receptacles will be stored in the holding area.
- Management will instruct individuals to stack the bales of destroyed media in rows designated by grade and in rows in the inventory storage area. No weak or mushy bales should be stacked. Weak or mushy bales must be reprocessed.
- Management will weigh bales and record the weight on appropriate documents before they are shipped to a disposal agent. The company's policy is to have destroyed materials be disposed of in a responsible manner which does not include any type of reuse (for purposes such as animal bedding or packing materials.)
- Management will oversee all bales and upon achieving threshold inventory levels, will determine the destination of all baled materials and schedule all shipments.
- Management will record the tallied total weight of the shipment on the Bill of Lading. Management will be responsible for completing the Bill of Lading compiled from the shipping information and the tallied bale weights.

2.14 Closing Procedures

The destruction process is not complete at the company until these final steps have been done.

- At the end of a shift, an Access employee/individual(s) should sweep the entire exposed floor and pass the sweepings through the destruction process.
- Management will check waste receptacles and areas directly outside of the information destruction building/area to see that no unshredded, confidential information has been deposited in waste receptacles or that no loose information-bearing materials are scattered around or near the destruction building.
- Management is responsible for relieving employees of duty at the end of each shift. At this time, employee identification badges should be returned and any company-related items.
- Once all employees have been relieved from a shift, Management is responsible for touring the facility and completing a visual security check.
- Management will ensure that all processed receiving tickets are placed in the appropriate holding box located in the business office.

2.15 Collection Facility Procedures

This destruction facility utilizes an offsite Collection Facility at (Address) to collect and store customer material awaiting transport to the destruction facility. Following are procedures and policies related to the use of this Collection Facility:

- The Collection Facility is used only to store material in preparation for transfer to the destruction facility; no destruction is to take place at the collection facility.
- Bins are to remain closed and locked until transferred to the destruction facility. The bins will not be tipped, and material is not to be processed in anyway.
- Bins/material intended for destruction will be transferred via secure transport to the destruction facility within 3 business days of arriving at the Collection facility. If material cannot be transferred within this timeframe, the customer will be notified in writing of the actual timeframe.
- Building security requirements:
    - Only screened access employees may enter the secure storage area.
    - All visitors must sign the visitor log, and logs will be kept for 12 months.
    - I.D. Badges are to be worn by employees and visitors at all times.
    - Building perimeter is protected by a third party monitored alarm system, which is to be armed at all times during which the building is unattended.
- Media is to be brought to the designated secure storage area immediately upon arriving at the Collection Facility. Other material, which is not intended for eventual destruction, is never to be staged or processed in this designated area.

2.16 Transfer Processing Station Procedures

This destruction facility utilizes an offsite Transfer Processing Station at (Address) to collect, process and store customer material awaiting transport to the destruction facility. Following are procedures and policies related to the use of the Transfer Processing Station:

- The Transfer Processing Station is used only to store and/or process material in preparation for transfer to the destruction facility, no destruction is to take place at the Transfer Processing Station.
- Material intended for destruction will be transferred via secure transport to the destruction facility within 15 business days of arriving at the Transfer Processing Station. If material cannot be transferred within this timeframe, the customer will be notified in writing of the actual timeframe.
- Building security requirements:
    - Only screened access employees may enter the secure storage/processing area.
    - All visitors must sign the visitor log, and logs will be kept for 12 months.
    - I.D. Badges are to be worn by employees and visitors at all times.
    - Building perimeter is protected by a third party monitored alarm system, which is to be armed at all times during which the building is unattended.
    - A closed circuit camera system (CCTV) is maintained with 90 days of recording, monitoring all ingress/egress points into the secure building/area and processing activity with sufficient clarity to identify people and their activities. (**See Section 2.7**)
- Media is to be brought to the designated secure storage area immediately upon arriving at the Transfer Processing Station. Other material, which is not intended for eventual destruction, is never to be staged or processed in this designated area.

3 DRIVER PROCEDURES

3.1 Access to Vehicles

The company wants to ensure that the utmost security precautions are taken by all employees. The company's access rules and regulations are as follows for those employees whose job duties involve driving:

- Only Management and designated employee Drivers will be allowed to have keys to vehicles.
- Two sets of keys will be issued to each driver.
- Employees are not allowed to utilize the company's vehicles for personal use without prior authorization from Management.
- Drivers are to follow the management-designated routes in providing services.

3.2 Security and Safety Measures for Vehicle Usage

In addition to the access limitations, the company utilizes the following security and safety measures for all drivers:

- Driver's Manual will be kept in every vehicle for reference purposes.
- Each driver has been provided with a readily accessible two-way communication device. The device should be kept on at all times unless it is prohibited while inside a customer's facility.
- All doors to the vehicles must be locked at all times, whether it contains confidential materials or not.
- All drivers should exercise extreme caution in all phases of vehicle operation. At no time should any employee put themselves or others at risk for accessing a loading area or loading materials.
- The use of cameras in or around vehicles where confidential materials are located is prohibited without prior authorization from Management.
- Employees may possess firearms, provided a current, state issued CCW permit is maintained in the employees file and with the employee, at the time of "concealed carry", unless prohibited by law or while inside a customer's facility. Any employee found violating this policy may be dismissed.

3.3 No Unauthorized Access to Truck

Under no circumstances are there to be any unauthorized persons permitted to have access to the cab, body, box, payload or tail-lift of the truck. Similarly, no unauthorized person shall be transported as a passenger in the truck at any time. Only Management can authorize access to the truck or permission to provide transportation to any Non Access employee or visitor.

3.4 Driver Demeanor

The company's mission to provide professional and prompt service requires that all company employees, particularly drivers, be polite and conduct themselves without excessive interaction with the client's personnel. The goal is to provide superior service with a minimum of distraction to their production.

3.5 Vehicle Preparation

Prior to driving to a client's location, all drivers must ensure that they are properly prepared for travel. Drivers must do the following prior to departure:

- Drivers must be certain that all vehicle paperwork required by the state is in the vehicle and up-to-date. This also includes any driver's license required.
- Drivers must make sure the truck is loaded with any security containers, carts, or pallets that are required to execute the assigned work orders.
- The driver should have a Receiving Ticket for each customer. The driver is also responsible to make sure there is a sufficient supply of the company's business cards in the truck.
- Drivers must make certain that the truck has adequate fuel to complete the route. There is no excuse for running out of fuel. Such incidents will be noted and considered in employee evaluations.
- If a vehicle is in need of repair, the driver should complete a Maintenance Request form and notify Management.

3.6 Driver Authority

Unless it is stipulated otherwise, while completing assignments the driver is the company's sanctioned authority and is responsible for instructing any other assistants in order to execute their assignments and duties safely, securely and as efficiently as possible. The driver is the lead representative and in charge of all client communications and interactions, unless a higher company authority is present.

In the event that a destruction facility is unattended when a driver arrives or departs, the driver will be responsible for its security. The driver should relock any doors and set the alarm before they leave the building unattended. If no security procedures have been established with the client prior to arrival, the driver must either contact the client or the company's management to determine how to handle the situation.

3.7 Enroute

The success of the company's business is dependent upon the knowledge and reliability of its drivers while completing an assignment. Drivers should familiarize themselves with all aspects of the company's business and the expectations of their drivers. Specifically, drivers should ensure that the following are adhered to while traveling to or from an assignment:

- Follow scheduled and designated routes to, from and between clients.
- It is driver's responsibility to inform Management of all developments that affect the timeliness and efficiency of executing the route. Drivers are required to notify the Management in advance of any period of time that they will be unable to be reached via the company-issued two-way communications device.
- The driver must always make sure that any confidential materials on the vehicle are secure at all times.
- In the event of a breakdown, the driver should immediately contact Management of the company and inform them of the situation. The driver or a representative of the company should then contact any client(s) that will be affected by the delay. Arrangements to service the vehicle should then be made. The driver should stay with the truck until help arrives. The driver should never leave a disabled truck unattended for any reason other than their safety or the safety of others. The driver should keep Management informed of the estimated time required for repairs.
- In the event of a collision or other accident, the driver should contact any emergency authority required first. If able, the driver should then notify Management or a representative of the company of the situation and if the vehicle will be operational. The driver or a representative of the company should then contact any client(s) that will be affected by the delay. The driver should also make sure the materials in the truck are secure. If they are not secure, the driver and any assistants should do their best to secure them. Management may need to dispatch help if required to secure the materials. Except for the police, the driver and any assistants should not engage in a dialogue with anyone regarding the accident, unless otherwise directed by Management.
- If a driver arrives at a loading area that is occupied, the driver should assess how long the delay will be. If it will be a long delay (more than 15 minutes) or if the length of the delay is indeterminable, the driver should locate an alternate loading area. If no alternative is available, the driver should notify the client to make alternative arrangements.

3.8 While at Client's Facility

Upon arrival at the client's facility, all drivers and any assistants of the company should remember to be professional and courteous at all times. The following guidelines should also be used:

- There may be instances where a client makes a request outside of the scope of the assignment that will need to be dealt with immediately. If the request is reasonable and does not seriously delay the route, then the driver should comply with the request and notify Management of the company later. (Management will inform the client of the problem with such requests later or assess a charge for the extra service.) If a client makes a request that is unreasonable, delays the route, compromises security, or is otherwise inappropriate, the driver should notify Management of the company immediately. Once apprised, Management will advise the driver regarding how to proceed.
- While at the client's facility, if a vehicle is required to be left unattended, the cab and box must be locked, whether it contains confidential materials or not. No materials in the company's custody should be left unattended ever.

- Collection containers with confidential media must never be left unattended, even if they are locked, unless they are secured in a locked company vehicle.
- If destruction of confidential material is not performed at the client's facility, then the driver should secure all containers before moving them. No person, not even an employee of the client, is allowed to examine or retrieve materials taken into the company's possession. If a situation requires that a client look through the materials or retrieve something from them, then the driver should contact Management first to get approval.
- If a customer expresses a complaint about a driver or the company, the driver should offer to convey their dissatisfaction or give them the company's business card.

3.9 Collecting, Receiving and Destroying Confidential Materials for On-site, Mobile Destruction

The company adheres to the following general policies in the collection, receipt and destruction of materials for on-site, mobile destruction:

- All materials taken into the company's custody are to be destroyed at the customer's site before proceeding to the next client, unless otherwise prearranged.
- All materials to be destroyed are always attended by an Access employee while in the custody of the company before they are destroyed. Collection containers with confidential media must never be left unattended, even if they are locked. If a vehicle is left running and unattended while collecting media at the client site, the driver should use duplicate keys to lock the vehicle cab and box.
- At time of media pick-up, customer must be provided with a receipt or certificate of destruction that indicates the type of service provided, a description of the material destroyed, and the quantity.

The driver should use the following steps in receiving/collecting and transporting confidential materials for destruction:

- At time of media pick-up, customer must be provided with a receipt indicating type and quantity of media (paper, micro media, computer hard drives, non-paper media – CDs, DVDs, tapes, etc.) being collected and that mobile destruction services are being provided for the media/materials collected and whether or not such services are NAID Certified. Management will instruct driver as to proper recording of this information on the receipt.
- The driver should complete the Receiving Ticket, have it signed by the client's representative, and leave the receipt with the client. The driver must return the work order to Management.

The company's destruction process procedures are as follows:

- Paper materials should be destroyed by shredding and baled by grade if possible. The specifications for particle sizes should be no larger than those listed below:
    - Continuous Shred: 5/8 inch Width (max) & Indefinite Length

- Cross Cut or Pierce & Tear: 3/4 inch Width (max) & 2.5 inches Length (max)
- Pulverized (Equipment w/ Screens): 2-inch diameter Screen Size holes (max)

  If adjustable screens are used, Management will be responsible for ensuring that a Screen Changing Log be kept on the truck denoting the starting point of the log and the pertinent information regarding any screen changes. The company will maintain the Screen Changing Logs for a minimum of one year.

- Microfiche or Microfilm can be destroyed by either a disintegrator or by equipment/process which produces a particle size of 1/8 inch maximum dimension or less. Destroyed materials should be properly discarded.
- Computer Hard Drives or CPUs will be recorded by serial numbers and then physically destroyed according to the separate written method provided by management. After the destruction service is completed, management will complete the following
  - A list of recorded serial numbers of destroyed drives will be returned to the customer, unless the client has opted out of serial number recordation by signing a NAID-approved opt-out agreement.
  - Logs of recorded serial numbers, a log of customers that have opted out of serial number recordation, and executed copies of any opt-out agreements will be retained for a period of **three (3) years** after the completion of the service.
- Non-Paper Media (CD's, DVD's, tapes, flash electronic storage devices, x-rays) will be destroyed using the standard method of shredding. If it becomes necessary to deviate from this standard method of destruction for any reason, management will notify the customer in writing of the actual method of destruction.
- Management will decide the appropriate method to use to destroy atypical media or non-media materials that require destruction.
- On a (daily/weekly/monthly) basis, Management will inspect the destroyed materials prior to disposal, to ensure that the destroyed information is within the original equipment manufacture specifications and within certification specifications.
- Paperwork verifying destruction should be returned and signed by an authorized agent of the client, preferably the person that witnessed the destruction process.
- Prior to leaving a client's facility, the driver should ensure that no confidential materials or trash are left on the ground where the loading or destruction took place.
- When leaving equipment at a client's facility, the driver should make sure it is in reasonable condition considering the environment in which it is located. Containers that are to be left in an office area require a much better appearance than those to be left in a warehouse. The driver should never leave equipment that does not function properly.

3.10 Collecting and Receiving Confidential Materials for Plant-based Destruction

- All materials to be destroyed are always attended by an Access employee or physically secured from unauthorized access while in the custody of the company before they are destroyed. Collection containers with confidential media must never be left unattended, even if they are locked, unless they are secured in a locked company vehicle.

- At time of media pick-up, customer must be provided with a receipt indicating type (paper, micro media – microfiche, microfilm, computer hard drives, non-paper media – CDs, DVDs, tapes etc.) and quantity of media being collected and that Plant-based destruction services are being provided and whether or not such services are NAID Certified. Management will instruct driver as to proper recording of this information on the receipt.

3.11 Reporting Damage to a Client's Facility

The company takes pride in providing efficient and honest employees. In the event that any accidental damages occur during an assignment, the driver must notify the client immediately about any damages to their property. The client should be assured that the company takes responsibility for actions that caused the damages and will pay for any damages resulting from those actions. The driver or assistant should notify Management at the company of such an occurrence as soon as possible. Management will be responsible for inspecting the damage and reconciling the issue with the client.

3.12 Ending the Destruction Assignment

Upon completion of an assignment, the driver and any assistants will unload all materials at the designated secure location. Each client's material should be individually staged and weighed. The driver will inspect and accept the materials, as they are unloaded from the truck. The driver will turn the Receiving Ticket over to Management upon verification that all materials have been removed from the vehicle.

Management is responsible for materials once they are unloaded at the designated secure location. Management will weigh bales and record the weight on appropriate documents before they are shipped to a disposal agent. The driver and any assistants will return their ID Badge to Management or the designated location in the office upon completion of the shift.

4 QUALITY CONTROL

4.1 Frequency of QC

On a (daily/weekly/monthly) basis, Management will inspect the destroyed materials prior to disposal, to ensure that the destroyed information is within the original equipment manufacture specifications and within certification specifications. (**See Section 3.9**)

4.2 Method of QC (See Section 2.7 and 3.9)

Daily/Weekly/Monthly Log will include the following:

- Date
- Name/Initials of individual performing the check
- Items checked:

    - Particle size (paper and micro media shredders). Is the equipment performing according to OEM and certification specifications?
    - Quality of physical hard drive destruction. Are the internal discs destroyed in a manner that prevents them from being put back on the hard drive mechanism to spin?
    - Non-paper media destruction. Does the standard method of destruction adequately destroy the material so that it would be impossible to retrieve the data using standard/traditional methods?
    - Paperwork control
        - Weekly/monthly logs
        - Visitor logs
        - Recordation of serial numbers
    - Length of time undestroyed material is held.
- Results
- Corrective Actions, if any

4.3 Corrective Actions

Management will be responsible for directing any Corrective Actions to be executed in the event of a failed quality control check. These actions may include the following:

    - If the particle size is too large and/or the equipment is underperforming:
        - Management will arrange for maintenance of the blades and/or other components, as recommended by the equipment OEM.
    - If material has been staged for more than 72 hours, or for a longer period of time than previously agreed upon with the customer:
        - Management will notify the customer in writing (email is acceptable) of the actual/revised timeframe.
        - If the reason for the delay is due to employee error or oversight, management will retrain employees on proper destruction procedures and the training will be documented.
    - If Visitor Logs, Operational Security Maintenance Logs and/or Serial Number logs are not being filled out in accordance with NAID Certification standards:
        - Management will retrain employees on proper Certification procedures.
        - Management will document the training, including a roster of the employees who were trained.

5 NOTIFICATIONS

5.1 Management Data Breach Notification to Customer

Management will report, following discovery and without unreasonable delay, to the customer any release of, or unauthorized access to the customer's confidential material that poses a threat to the security or confidentiality of that information. Any such report shall include the identification (if known) of each individual whose confidential information has been, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach. Customer notification shall occur within 60 days from the date of discovery.

5.2 Employee Data Breach Notification to Management

All destruction personnel and drivers will report, following discovery and without unreasonable delay, to management any release of, or unauthorized access to the customer's confidential material that poses a threat to the security or confidentiality of that information. Any such report shall include the identification (if known) of each individual suspected of causing the breach, as well as each individual whose confidential information has been, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach.

Any such report shall be kept confidential and management will not retaliate against any employee who has reported, in good faith, a potential or actual data breach. (**See Section** 2.4)

5.3 Notification of Subcontracted or Non-NAID Certified Services

The customer must be notified in writing by management whenever all or a portion of the destruction process is being subcontracted to another service provider, or when a destruction service is not NAID Certified, but such services could be NAID Certified. This includes advance notification to potential customers at the bid or proposal stage; as well as notification at the time of the service, either on a materials receipt, certificate of destruction, customer agreement/contract or other written notice (including email). (**See Section** 1.5)

In instances where a subcontractor will be used, the advance notification must also identify the parties destined to accept custody, the exact location of destruction and the method of destruction, if this information is known at the time of the bid or proposal. This information must always be provided prior to or at the time the service is rendered. The notification must also indicate if a subcontractor performing destruction services is not NAID Certified.(**See Section** 1.5)

6 NAID UNANNOUNCED AUDIT POLICIES

As part of our NAID Certification, we are subject to unannounced audits conducted by a NAID auditor, which may occur at any time, either in the field or at the destruction facility or company offices. The auditor has the authority to challenge our security and to review any item that would be reviewed during a scheduled audit to ensure that our practices are consistent with NAID Certification standards. The auditor may also follow company vehicles to witness collection and destruction activities at a customer's location prior to announcing his/her presence.

The NAID Certification Review Board (CRB) tracks verified reports of NAID Certification non-compliance and may issue fines and/or sanctions or recommend removal of our Certification to the NAID Complaint Resolution Council (CRC) and Board of Directors for any violations.

6.1 Unannounced Audits at the Office or Destruction Facility

The following procedures must be followed in the event that a NAID Auditor arrives at the office or destruction facility to conduct an unannounced audit:

- Ask to see the Auditor's identification. All NAID Auditors have a photo ID Badge issued by NAID.
- Verify that the Auditor has an Auditor Assignment and Confidentiality agreement, which has been signed and dated by a NAID official.
- Call the NAID office or notify company management if there is any reason to doubt the legitimacy of the audit.
- Ask the Auditor to sign the visitor log and provide the Auditor with a visitor badge.
- Contact **Keith Eriksen** to accompany the auditor during the audit. If **Keith Eriksen** is not available, contact **Clint Eriksen**.
- **Keith Eriksen** or **Clint Eriksen** will escort the Auditor throughout the audit process and will allow access to all requested areas and documentation, if such request is not a hardship and does not unreasonably disrupt daily operations.
- Only if **Keith Eriksen** and **Clint Eriksen** are ***both*** unavailable, any employee may assist and accompany the Auditor during the audit, provided that they have been cleared for access to confidential customer material.
- At the end of the unannounced audit the auditor may ask you to sign a report. This report should be signed if asked. Your signature acknowledges that the audit took place; it does NOT indicate your agreement with the report.

6.2 Unannounced Audits in the Field or at the Customer's Site

The following procedures must be followed in the event that a NAID Auditor arrives at a location where a driver or driver's assistant is picking up customer material for onsite destruction or transportation back to the destruction facility:

- Ask to see the Auditor's identification. All NAID Auditors have a photo ID Badge issued by NAID.

- Verify that the Auditor has an Auditor Assignment and Confidentiality agreement, which has been signed and dated by a NAID official.
- Call the NAID office or notify company management if there is any reason to doubt the legitimacy of the audit.
- Contact (First Company representative or position of contact) to report the audit. If (First Company representative or position of contact) is not available, contact (Second Company representative or position of contact).
- At the end of the unannounced audit the auditor may ask you to sign a report. This report should be signed if asked. Your signature acknowledges that the audit took place; it does NOT indicate your agreement with the report.

7 Red Flags Rule Procedures

7.1 Policy

It is the policy of **Reed Records Management** to fully disclose to clients all relevant details in a timely manner and to reasonably cooperate in any subsequent investigation if information, verified by management, constitutes unauthorized access to information transferred to our custody. The acceptance, transfer and processing of information transferred to our custody shall be documented and verified. Such documentation shall be made available to the customer in the course of business or upon request.

7.2 Condition of Employment

As a condition of employment, all employees are required to notify management of any actual or potential unauthorized access to information transferred to our custody for processing.