

# National Association for Information Destruction, Inc.



## **NAID<sup>®</sup> Certification** **Electronic Media Sanitization** *January 2012*

**World Headquarters**  
**1951 W. Camelback Rd., Suite 350, Phoenix, AZ 85015**  
**Phone: (602) 788-6243 & Fax: (602) 788-4144**  
**E-mail: [certification@naidonline.org](mailto:certification@naidonline.org)**

# ABOUT THE CERTIFICATION OF COMPUTER HARD DRIVE SANITIZATION

## OVERVIEW OF THE SANITIZATION PROGRAM

- 1) The overwhelming majority of the security elements for this Certification are the same as our current Certification Program, i.e., employee screening, access control, unannounced audits, etc.
- 2) This will be a separate certification process/program as opposed to an endorsement on the current one.
- 3) The current auditors will be used to conduct the sanitization audits. However, it may utilize a limited number of auditors specifically for the Sanitization audits.
- 4) NAID will request that all sanitization applicants identify key points within their operation that serve as audit points and supply those to the auditor in advance via the *Sanitization Process Questionnaire*. With this information, the auditor will be prepared to thoroughly inspect the applicant's unique process, including but not limited to:
  - a. Staging
  - b. Acceptance and Identification of Items Prior to Processing (requiring logging of serial numbers)
  - c. Stages of the Sanitization Process (including quality control or redundant verification sampling)
  - d. Identification and Separation/Isolation of Sanitized Hard Drives after Processing
  - e. The Recordkeeping/Paper Audit Trail through the entire Sanitization Process
- 5) Besides verifying all record keeping and procedural elements common among all NAID Certifications, the auditor will verify the effectiveness of the applicant's sanitization process during the audit utilizing the following methodology:
  - a. The auditor will provide two (2) control hard drives to the applicant containing a known amount of control data which must be sanitized and returned to the auditor prior to his departure. These will be sent to a data recovery service to verify that the data is not conventionally retrievable.
  - b. The auditor will also remove two (2) hard drives randomly from among the hard drives in the applicants processed inventory, each within the 80-120 GB size range. These too will be sent to the data recovery service for analysis. (These hard drives would then be returned to the applicant.)

The applicant will acknowledge on the application that they understand the process, and while errors may occur, they will not be NAID Certified if any of the hard drives contain recoverable information when using a conventional recovery process.

The applicant will also acknowledge on the application that they agree NAID is not responsible for damage to any hard drives utilized in the process.

# **ABOUT THE CERTIFICATION PROGRAM**

## **PROGRAM OVERVIEW**

The NAID Certification Program is offered on a voluntary basis to all NAID member companies providing information destruction services. Through the program, NAID members may seek annual certification audits for both Mobile and Plant-based operations in paper or printed media, micro media or computer hard drive destruction. The NAID Certification Program establishes standards for a secure destruction process including such areas as operational security, employee hiring and screening, the destruction process, responsible disposal and insurance.

Applicants are required to submit the most current Certification Application and associated fees to NAID Headquarters on a yearly basis. Once the application is received complete by NAID Headquarters, an auditor is assigned to the location to perform the audit. All audits are performed by security professionals with the Certified Protection Professional (CPP) accreditation. The CPP accreditation is issued by the American Society for Industrial Security.

When a NAID Member has had a successful audit, they are issued a certificate, showing their company name, type of operations and the specific media destruction performed at their location. The NAID Member is also listed on the NAID website as certified.

Under the above program, the certification application and associated fees cover only individual locations. If a NAID member operates in multiple locations, each location must pass the audit to be certified. NAID members who receive certification must specify the location certified in company literature when referencing the NAID Certification Program.

The following packet is designed to help further familiarize applicants with the NAID Certification Program and clarify the specific information required to have a successful audit and maintain certification status. Included are commonly used terms or definitions used in the Certification Program, forms/templates required to be used and be available to the auditor conducting the NAID Certification audit, and the Certification Application. All forms can also be found at [www.naidonline.org](http://www.naidonline.org). NAID is committed to maintaining the integrity of the Certification Program and is here to assist your company in achieving Certification status. Any questions or concerns can be directed to [certification@naidonline.org](mailto:certification@naidonline.org).

## **CERTIFICATION APPLICATION AND SCHEDULED AUDIT PROCESS**

The following is the process that is adhered to by NAID Headquarters in order for a NAID member to obtain Certification status:

1. A NAID Member applies for NAID Certification by submitting a completed Certification Application to NAID Headquarters. This includes the Additional Required Materials requested on page 2 as well as the application fee.
2. NAID Headquarters assigns and faxes a copy of the application to the regional auditor.
3. The auditor contacts the applicant to schedule the audit appointment.
4. The auditor then completes and faxes the "Audit Confidentiality Agreement," verifying the date and time of the audit, to the applicant and NAID Headquarters.
5. The audit will take place as scheduled and at the end of the audit process, the auditor will report his/her findings on the Auditor Report form to NAID Headquarters for acceptance by Certification Review Board.

6. After reviewing the auditor's findings and recommendation, the Certification Review Board will approve, deny or request further information/action on the applicant's Certification. NAID Headquarters will notify the NAID member of the results. If the audit has been approved, NAID Headquarters will provide the NAID member with appropriate Certification documentation, including posting successful Certification on the NAID website [www.naidonline.org](http://www.naidonline.org).

### **CERTIFICATION REVIEW BOARD**

The Certification Review Board, composed of several NAID member representatives and outside professionals in security and records management, will make final outcome decisions on all audits (scheduled and unannounced), including review of any special considerations before audits and indicate required corrections before, during or after the Certification application and audit process.

### **UNANNOUNCED AUDITS**

As an integral part of the Certification Program, Unannounced Audits will be randomly chosen by NAID's Certified Public Accountant and conducted for approximately 25% of all Certified locations annually. Auditors will have full latitude to check any and all criteria of the Certification Program, but will focus on security measures and observable operations that occur on a daily basis at the member's site. Any problems or issues found during an Unannounced Audit will be referred to the Certification Review Board for review. The Certification Review Board may require necessary actions take place by the member to rectify problems immediately and can revoke their Certification Status during that period.

## **CERTIFICATION PROGRAM DEFINITIONS**

The following are definitions of words or terms used in regards to the NAID Certification Program.

**ACCESS INDIVIDUALS** – Individuals who have access to, or who can grant or authorize access to the Confidential Customer Media to be destroyed at the Company's location, including but not limited to 1) employees, 2) agents of "sub-contractors" as defined herein, or 3) others providing any type of services to the applicant company that allows access to any area in which Confidential Customer Media is accessible. For NAID Certification, Access Individuals also include officers, directors, owners, partners of the company or other individuals who have access to, can grant access to, or authorize access to the Confidential Customer Media to be destroyed at the Applicant Company's location.

**ACCESS NON-EMPLOYEES** – Access Individuals who are not employees. This subset of Access Individuals is distinctly identified because of background screening requirements that apply to this category.

**BRANCH/LOCATION** – Any facility or place operated by a Company where 1) Confidential Customer Media is destroyed; or 2) stand-alone support is provided for Mobile Operations.

**CONFIDENTIALITY AGREEMENT** – An Agreement in which all Access Individuals acknowledge they will keep any customer media and information secure and confidential. A Confidentiality Agreement having concepts substantially similar to the sample document available to all NAID members must be signed by all Access Individuals and Non-Access Employees, and the Agreement must be kept on file by the Company. Where it is not practical to have such an Agreement directly with an individual, a letter from the Subcontractor, verifying that such an Agreement has been executed by any of their agents who would be provided as an Access Individual, would be acceptable.

**CONFIDENTIAL CUSTOMER MEDIA** – Documents, papers, records, or other media received by the Company from customers for destruction.

**CONVENTIONAL COMPUTER HARD DRIVES** – Standard, conventional PC hard drives; this does not include micro chips, micro processors or storage devices typically found in PDAs, cell phones, or USB storage devices.

**EMPLOYMENT HISTORY VERIFICATION** – A verification of all prior employment held by an employee of the Company over the past 7 years; the verification may be conducted by whatever means best suit the Company (i.e., in-house or third-party).

**MEDIA** – Any form of confidential or protected information-containing mediums to be destroyed, including but not limited to paper, microfilm, microfiche, X-rays, ID badges, credit/debit cards, computer hard drives, magnetic or digital tapes, disks or cartridges.

**MOBILE OPERATION** – Secure destruction activities carried out using mobile commercial-grade destruction equipment that destroys Confidential Customer Media within an enclosed and securable vehicle (truck or trailer) at the customer's site.

**NAID Certification, Certified, Certification, AAA Certification, Certification Program, Program** - words used interchangeably throughout the NAID Certification Program information referring to NAID Certification or to identify a facility or company that meets all NAID standards regarding security and other operational characteristics.

**NON-ACCESS EMPLOYEES** – Employees of the Company who are restricted from access to secure destruction areas and other areas where Confidential Customer Media is accessible or who have not been through, or cannot be fully vetted for the NAID Certification employee screening requirements. These employees must be accompanied, supervised, or escorted by an Access Employee at all times when in presence of Confidential Customer Media to be destroyed. Also see Visitors.

**NON-CITIZEN EMPLOYEES** – Employees who are not citizens of the country in which the Company location is operated.

**PLANT-BASED OPERATION** – Secure destruction activities carried out using fixed-location commercial-grade destruction equipment that conducts the entire process, including the staging, destruction, baling and storage of destroyed materials, within a secure building environment.

**SANITIZATION/WIPING** - The process of masking information recorded on a computer hard drive by overwriting with random, meaningless data.

**SECURE ERASE** – A process of permanently removing information from a computer hard drive by activating a preexisting protocol hard wired into the hard drive by the manufacturer. This process is not accessible directly through the bios functions of any computer so that it cannot be inadvertently activated. It must be activated by physically accessing the hard drive directly with the proper equipment and software.

**SUBCONTRACTOR** - Any entity the Company uses to provide services that are an integral part of the Company's destruction service program and whose employees or agents have access to Confidential Customer Media to be destroyed. Examples include providers of temporary staffing, transportation, etc. *Use of another destruction company for remote locations, projects or other special circumstances must be represented to the Company's clients as NOT NAID-Certified, unless such company is currently NAID Certified for the work being performed - these destruction companies do not need to be submitted as Subcontractors.*

***VISITORS*** - All individuals who may enter the secure destruction area/facility or enter an area/facility with Confidential Customer Media for destruction and who are 1) not employed by the Company, 2) working as (or for) an independent contractor for the Company, 3) otherwise providing services for compensation to the Company, &/or 4) employees from another division or Company location who have not met all of the NAID Certification Employee Screening requirements and are not wearing a Photo ID badge, are considered Visitors. All Visitors must sign in a Visitor log maintained by the Company, be provided a Visitor badge and be escorted or under the supervision of an Access Individual at all times while in the secure destruction building or area with Confidential Customer Media for destruction. This includes, but is not limited to, current or prospective clients, service providers such as vending machine distributors, mechanics or technicians, or employees as noted above

# NAID<sup>®</sup> Certification Application

## Electronic Media Sanitization

### January 2012

**Company Name:** \_\_\_\_\_ **Audit Contact:** \_\_\_\_\_  
**Physical Address:** \_\_\_\_\_ **Unit/Ste:** \_\_\_\_\_  
**City:** \_\_\_\_\_ **State:** \_\_\_\_\_ **Postal Code:** \_\_\_\_\_  
**Phone:** \_\_\_\_\_ **Fax:** \_\_\_\_\_ **Email:** \_\_\_\_\_

**Profile Information**

Year Sanitization/Wiping Business Established: \_\_\_\_\_ Total Number of Access & Non-Access Individuals for this Location: \_\_\_\_\_  
 Normal Hours of Operation: \_\_\_\_\_ Number of Collection Vehicles/Trucks in Fleet: \_\_\_\_\_

Are any of your Collection Vehicles stored at a location other than address above?  
 No  Yes, at the following address: \_\_\_\_\_

Typically, the First Truck of the Day is Dispatched at (Indicate time): \_\_\_\_\_

Do you arrange for or subcontract with common carriers for transport of media from the client to your facility?  
 No  Yes; all companies used within the last year are listed in the additional materials as a subcontractor

**Application is for:**

**PLANT-BASED** – Commercial sanitization process is conducted within a secure building environment, including the receiving, staging, record-keeping, sanitization, destruction, and storage of media. *This Endorsement for Electronic Media Sanitization requires that this location have a standard method for the physical destruction of Electronic Media.*

*What type of sanitization is being NAID Certified for Plant-based Operations? (check all that apply)*

- Conventional Hard Drives  SSD-Computer (Beta)  SSD-Memory Cards (Beta)
- Mobile Phones (Beta)  Physical Destruction of Electronic Media
- Other (please indicate): \_\_\_\_\_

*What other operations take place within the building? (check all that apply)*

- Degaussing  Physical Destruction of Electronic Media
- Resale or Storage of Sanitized Media  Electronics Recycling
- Other (please indicate): \_\_\_\_\_

**ONSITE** (check all that apply)

- Physical destruction (not overwriting or wiping) of Electronic Media performed at the Client's premises.
- Sanitization of Electronic Media performed at the Client's premises.

*What type of sanitization is being NAID Certified for Onsite Operations? (check all that apply)*

- Conventional Hard Drives  SSD-Computer (Beta)  SSD-Memory Cards (Beta)
- Mobile Phone (Beta)  Physical Destruction of Electronic Media
- Other (please indicate): \_\_\_\_\_

**Application Fee: \$2620** (Fee will increase, on a case-by-case basis, for overwrite methods using random characters instead of 1's and/or 0's)

**Payment Info & Amount:** \$ \_\_\_\_\_

Enclosed Check (Payable to "NAID") Check No.: \_\_\_\_\_  
 Mastercard  Visa  Discover  AmEx Card# \_\_\_\_\_ - \_\_\_\_\_ - \_\_\_\_\_ - \_\_\_\_\_ Expires (mo/yr): \_\_\_\_/\_\_\_\_  
 Name on Card: \_\_\_\_\_ Signature: \_\_\_\_\_

NAID Use Only			
New or Recert:	Auditor:		
Audit #: _____ - _____	Received: ____/____/____	DBS Updates: ____/____/____	Packet Sent: ____/____/____
Audit Appt.: ____/____/____	Auditor Rec: ____/____/____	CRB Approval: ____/____/____	Expires: ____/____/____
Funds given to Finance: ____/____/____	Payment Processed: ____/____/____		

**Employment Information Disclaimer**

All organizations applying for NAID Certification are expected to comply with any and all national, state, local, or other laws regarding the collection, maintenance and disclosure of employee information, and all laws regulating employment practices, in the jurisdiction governing the location for which the applicant Company is applying for NAID Certification or does business. NAID is not responsible for the compliance of its individual NAID Certified members. Therefore, if the applicant Company believes that anything in this Application or the audit process is, or may be, violative of any laws applicable to the applicant Company, such Company must notify NAID, concurrently with the submission of its NAID Certification Application or during the audit, as applicable, of the practices or disclosures which are believed by the applying organization to be in conflict with or violative of any relevant laws. In addition, such notification must include a statement of and citation to the applicable law, code, ordinance or other legal authority. NAID will then analyze the law, code, ordinance or other legal authority to determine whether the applicant Company may be exempted from the particular criteria, practice or disclosure. NAID will notify the applicant Company in writing of such determination.

Also, a particular requirement of this application, although permissible under applicable laws and regulations, may violate applicable laws and regulations if applied in an impermissible manner, particularly in regard to hiring and retention practices. You should consult your own legal counsel to determine whether your hiring and retention policies and practices comply with all applicable laws and regulations.

**Additional Required Materials:** (to be submitted with application)

- 1) **Access Individuals and Non-Access Individuals list** - A list of all employees/individuals broken down by "Access Individuals" and "Non-Access Individuals" indicating title/position/responsibility (driver, owner, manager, processing, etc) and for "Non-Access Individuals" the reason the individuals have been classified this way. Also, the Applicant must indicate any employees who are not citizens of the employer's country.  
(See the Definitions document for detailed descriptions of Access Individuals and Non-Access Individuals).
- 2) **List of Collection Vehicles** – A List of all collection vehicles, including Vehicle make & model, VIN, License Plate Number and State vehicle is licensed in.
- 3) **List of Recipients of Physically Destroyed Media/Materials** – List should include all companies receiving destroyed media/materials from Applicant within the last year and ultimate responsible disposition of materials (materials recycling, metals recovery/smelting, landfill, etc.)
- 4) **Subcontractor list** (if applicable) – A list of all companies or agents used within the last year to subcontract any part of the information destruction process indicating what aspects of the process for which they are responsible and accept custody (See Definitions page); this must include any third party or common carriers used within the last year.
- 5) **Sanitization Process Questionnaire** (see attached form) – Applicant must submit responses to all questions, including reference to how and where in their Policies and Procedures these items are addressed.
- 6) **Special Consideration Letter** (only applicable for hardship or extreme circumstances) – Letter requesting a temporary or conditional qualification for a specific NAID Certification criteria; Only considered under extreme or special circumstances, applicant must submit this written request (on Company letterhead & signed by an official Company representative) with their NAID Certification Application. The letter must identify the specific criteria, detail the hardship or special circumstance for consideration, and state how the applicant will achieve the intent of the criteria given their circumstances. The NAID Certification Review Board will review and respond to all requests.

**We agree with and are bound to the following:** (Please initial each item and sign on bottom)

1.  NAID Certification is optional and is not required for NAID membership.
2.  The Company is a member of NAID in good standing and with no outstanding debt to the association. In order to gain or maintain NAID Certification, the Company must be a NAID member in good standing.
3.  Owners or Senior management of the Division of the Company that conducts the secure destruction operation has read and understands the NAID Certification Audit Methodology, which makes clear the documentation, facilities and equipment that each location will be required to have available and immediately accessible to the Auditor.
4.  Any failure to make accessible for inspection all documentation, facilities, and equipment on the date, time and location identified on the Auditor Assignment & Confidentiality Agreement (Appointment) Form may result in failure to be NAID Certified, forfeiture of the application fee, additional fees for the failures, re-auditing or other expenses, and/or require that we reapply if we want to pursue this credential. Also, failure to meet the criteria for the type(s) indicated on this application may be considered a failure of the audit.
5.  **If the Company is applying for NAID Certification of Onsite Sanitization Operations**, only those individuals who are verified to be on the Company's payroll, and who are direct employees of the Company (NOT contract or temporary) perform Onsite Sanitization services.
6.  The Company understands the NAID Certification requirements contained herein and that conventional recovery testing is part of auditing the sanitization process. If any information is recovered during the testing of the control Electronic Media devices or sample sanitized Electronic Media devices from the Company "stock," this will be considered a failed audit and the Company will not be NAID Certified. Also, all sample "stock" Electronic Media devices will be returned, but the Company acknowledges that NAID and/or its agents are not responsible for damage that may occur to the Electronic Media during this recovery testing.

7.  The stated application fees are only applicable for control Electronic Media devices and sample Electronic Media devices from the Company "stock" that have been sanitized using the method of overwriting with ones and/or zeros. The application fees will increase for the testing of Electronic Media devices that have been overwritten with random characters. These fees will be determined on a case-by-case basis and the Company will be contacted with a description of those fees.
8.  All application fees are non-refundable, except in the instance where the Auditor fails to conduct the audit on the date, time and location indicated on the *Auditor Assignment & Confidentiality Agreement* (Appointment) form; and when, in such circumstance, the Company decides to withdraw their application.
9.  At no time will the label "NAID Certification" or "NAID Certified" be applied, referenced or inferred to facilities or operations of the Company where 1) the location and operating details related to the facility or operation have not been specifically and formally provided to NAID for participation in the NAID Certification program, or 2) the facility or operation does not have any involvement related to the collection, transport, processing, wiping/sanitization and/or destruction of Electronic Media.
10.  The Company must reapply for NAID Certification on an annual basis, prior to the expiration of the current NAID Certification. If the Company chooses not to reapply and/or not to submit to the required audit, it will result in loss of NAID Certification. Loss of NAID Certification will not affect NAID membership.
11.  The Company will hold NAID harmless from any claim of damage or loss as a result of the Company's failure to achieve NAID Certification.
12.  The location applying for the Sanitization endorsement for NAID Certification must provide physical media destruction as a component of this process.
13.  The Company understands and agrees that at least 90 days of CCTV recordings must be maintained and the Company must be able to produce them during the time of an audit. If the Company is unable to produce the 90 days of recordings at an audit, the Company may be subject to a reaudit, including associated costs for this reaudit.
14.  The Company understands that the specifications and fees for NAID Certification are subject to change at the discretion of the NAID Board of Directors.
15.  All of the Company's employees are legally registered to work in the country to which this Application applies, and the Company has all necessary documentation to confirm this (see the Employment Information Disclaimer).
16.  The Company understands that it is responsible for ensuring that background checks of current and prospective employees and any use of consumer reports for employment purposes comply with the mandates of the Fair Credit Reporting Act, 15 U.S.C. 1681 et seq.
17.  If restrictive employment agreements are in place that would prevent the Company from conducting drug screening and/or criminal record searches, the Company will provide a detailed description of such restrictions with this application.
18.  The Company understands that random Unannounced Audits are part of the NAID Certification Program. Only if asked and not a hardship, the Company will allow access to a NAID Certification Auditor for purposes of conducting such Unannounced Audits. Discrepancies discovered during any unannounced audit may result in the issuance of fines and/or sanctions against the Company.
19.  **If the Company is applying for NAID Certification of Onsite Sanitization Operations**, copies of all Quality Control Logs and Client documentation are stored at the Headquarters Office, for review during scheduled and unannounced audits.
20.  The Company understands and agrees that the NAID Certification Auditor may inspect and test its access control systems related to the facilities, containers and vehicles used to provide secure destruction services during announced and unannounced audits and will not consider such inspection and testing to be a violation of the law, provided such inspection and testing does not result in property damage or the risk of personal injury and is undertaken solely for the purpose of ascertaining compliance with NAID Certification.
21.  At any time during the application and/or audit process or after NAID Certification, the Company acknowledges that NAID, its agents and/or the NAID Certification Auditor may investigate or require additional information or documentation from the Company in order to verify information on this Application or the NAID Certification criteria.
22.  The Company understands and agrees that all of its employees and agents will refrain from any false or misleading claims, suggestions or references regarding NAID Certification, including but not limited to such claims used in advertising produced in advance and/or in anticipation of NAID Certification at some future date.
23.  If the Company has a change in address, ownership, or the operations/services it offers to Clients any time during a pending NAID Certification application or audit, or while the Company is NAID Certified, the Company must notify NAID in writing within 15 business days of this status change. **Failure to do so may result in fines, sanctions and/or revocation of NAID Certification.**

Company Name: \_\_\_\_\_

24.  The Company agrees that if any location for which it is seeking NAID Certification becomes NAID Certified, then if at any time during the audit process or NAID Certification the Company elects to discontinue any or all NAID Certification operations or endorsements for such location, the Company must notify NAID in writing within 30 days of this status change and has an ethical responsibility to inform clients (aware of the Company's NAID Certification status) of the change.
25.  The Company understands that ALL NAID certifiable services/operations being offered to the Company's Clients must be NAID Certified in order to gain and maintain NAID Certified status. If the Company adds a certifiable operation after NAID Certification has been approved, it has 6 months in which to apply for NAID Certification of the new operation. **Failure to apply for and/or successfully pass an audit of all certifiable operations may result in the removal of all NAID Certifications.**
26.  The Company understands that the NAID Auditor does NOT approve or deny NAID Certification. The Auditor's findings will be submitted to the NAID Certification Review Board for approval, determination of remedial or corrective actions and/or additional fees necessary to approve a NAID Certification, or denial of application.
27.  The Company has 14 business days (as determined by the date on the notice sent to the Company regarding the results of an audit) to submit to the NAID Certification Review Board in writing any protest of the results of an audit. The Company understands that the protest should clearly state the perceived reason of the failure to achieve NAID Certification and why the finding is incorrect. The Company understands that the NAID Certification Review Board will rule on the dispute within one month from receiving it. The Company will accept the ruling of the NAID Certification Review Board as final and seek no further remedy, legal or otherwise, except to reapply for NAID Certification at the Company's discretion.
28.  This Application is truthful and accurately represents the daily operating procedures of the Company's Sanitization and Physical Destruction operations. If any of the Company's representatives willfully deceive NAID or a NAID Certification Auditor, the Company could be immediately removed from NAID, or the NAID Certification may be revoked.
29.  Indications of the signatory's initials above and the signature below acknowledge that they are an owner, corporate officer or official representative of the Company submitting this Application. The undersigned has full authority to request this audit, with full knowledge of the Company's operations to accurately complete the application, and the authority to execute this agreement.

Date: \_\_\_\_\_

Signed: \_\_\_\_\_

Print Name: \_\_\_\_\_ Title: \_\_\_\_\_

Company: \_\_\_\_\_

	Initial	Criteria	Audit Methodology
<b>EMPLOYEE REQUIREMENTS</b>			
1.1	Applicant Claims <hr/> Auditor Verifies <hr/>	<p><b>All Access Individuals and Non-Access Employees</b> must sign a Confidentiality Agreement prior to gaining access to Confidential Client Media and employees must be legally Registered to work at the Company:</p> <ul style="list-style-type: none"> <li>• <b>Confidentiality Agreement</b></li> <li>• <b>I-9</b> for US employees hired after November 7, 1986 or proper work registration for non-citizens</li> </ul> <p><i>(See Employment Information Disclaimer.)</i></p>	<p>Based on the list of <b>Access and Non-Access Employees</b> submitted with the Application, Auditor will request evidence of the appropriate documentation in the individual files of this operation location as follows:</p> <p>Where applicant Company has 7 or fewer Access and/or Non-Access Employees, Auditor will request verification of applicable documentation for all Access and Non-Access Employees.</p> <p style="text-align: center;">OR</p> <p>If the applicant Company has more than 7 Access and/or Non-Access Employees, Auditor will request verification of applicable documentation for a random sample, totaling 25% of the entire Access and Non-Access Employees List, with a minimum of 7 individuals and a maximum of 15 individuals to be selected.</p>
1.2	Applicant Claims <hr/> Auditor Verifies <hr/>	<p><b>Access Individuals*</b> are subject to the employment screening restriction requirements of NAID Certification, including criminal background check, initial employment drug-screening and previous employment verification.</p> <p>Screening for <b>Access Individuals*</b> must include:</p> <ul style="list-style-type: none"> <li>• <b>7 Year Criminal Record Search:</b> <ul style="list-style-type: none"> <li>○ Social Security Header Search (must be conducted prior to the criminal background investigation to ensure all states and counties of residence and employment have been included (and verified) in the investigation)</li> <li>○ Federal Records Search for all Federal Districts in all states on SS Header Search</li> <li>○ Statewide records search for all states on SS Header Search</li> <li>○ County records search for all counties on SS Header Search</li> </ul> </li> <li>• <b>Pre-hire or Initial Drug Screening</b></li> <li>• <b>7 Year Employment History Verification</b> must minimally include the following for each place of prior employment:                             <ul style="list-style-type: none"> <li>○ Name of the previous employer</li> <li>○ Dates of employment, as reported by the employee</li> <li>○ Date of verification (or attempted verification if the previous employer cannot be reached)</li> <li>○ Indication of whether or not the previous employer was able to verify the dates of reported employment.</li> </ul> </li> </ul> <p>A <b>Criminal Record Search</b> must be conducted for each place of residence and employment during the previous 7 years and obtained through a third-party background search service. <b>For all places in the U.S.</b>, federal, statewide and county-by-county searches must be conducted for any record searches conducted after January 1, 2012. Prior to that date, only statewide and county-by-county searches were required. If federal, statewide and/or county searches are not available in a particular state, the applicant may do the ones available and provide documentation to support the unavailability of the other.</p> <p><i>For all places in Canada</i>, searches must be done on a province/territory and National basis and obtained through a third-party background search service or Canadian Police Information Centre (CPIC).</p> <p>When searches are being conducted in <b>places outside of the U.S.</b> every effort should be made to have the searches done at a level comparable to the statewide and county-by-county searches done in the U.S.</p> <p><i>(See Employment Information Disclaimer.)</i></p> <p>This location has <b>Restrictive employee agreements</b> in place that prevents drug screening and/or criminal record searches for certain individuals</p> <p><input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes and attached is a letter stating who and what employee screening restrictions are in place.</p>	<p>When randomly selecting individuals' files, the Auditor should attempt to choose individuals from each category of Access Individual, i.e. driver, processor/sorter, driver helper, etc. Auditor to identify which files were checked so that these individuals' files may be exempted from the random selection process during future audits.</p> <p>If Auditor finds any missing documentation in representative sampling, s/he may request applicable documentation for additional Access and/or Non-Access Employees.</p> <p>Auditor must inspect applicable documentation for all Non-Citizen Employees and Access Individuals who are owners, partners or senior managers (of destruction division) of the Company.</p> <p>*Access Individuals who are exempt from the employment verification, drug screening requirements, and I-9 requirements are:</p> <ol style="list-style-type: none"> <li>1) officers, directors, owners and/or partners of the applicant Company not engaged in the day-to-day operation of the applicant Company; or</li> <li>2) others who have access to, can grant or authorize access to the Confidential Client Media to be destroyed at the applicant's location but are not engaged in the day-to-day destruction operations; and/or</li> <li>3) independent contractors, Subcontractors or employees thereof.</li> </ol> <p>Any Access Individuals representing the Headquarters of the Company's information destruction division, minimally the President/Vice President of area &amp;/or Audit Coordinator, whether at the location listed on this application or at another location, must have criminal background searches conducted.</p> <p>For independent contractors, subcontractors, and/or employees thereof, the Company may have a written agreement or certificate issued by such contractor stating that the current NAID Certification employee screening requirements are being met, in lieu of the actual records.</p> <p>The criminal record search must be current, meaning that it was conducted within the last seven years from the current date.</p> <p>No person subject to a felony conviction in the last seven years for any crime involving theft (of tangible or intangible property), fraud, burglary or larceny may be employed in a capacity where they may come in contact with Confidential Client Media. This applies to all Access Individuals.</p> <p>The employment screening is applicable to all Access Individuals (other than those exempt from these requirements as mentioned above) regardless of length of service or pre-existing employment status, except where there is a restrictive employment agreement in place. Access Individuals whose employment or relationship predates the implementation of NAID Certification policies, must be retroactively screened, and, if necessary, restricted from access to Confidential Client Media.</p>

	Initial	Criteria	Audit Methodology
1.3	Applicant Claims _____  <input type="checkbox"/> <b>Not Applicable</b>  Auditor Verifies _____	<p><b>APPLIES TO ONSITE CERTIFICATION ONLY</b></p> <p>Only those individuals who are verified to be on the Company's payroll, and who are direct employees of the Company (NOT contract or temporary) perform Onsite Sanitization services.</p>	<p>The Auditor will review the Company's payroll records to verify that all field technicians /employees listed on the employee list (provided with this application) are directly employed by the Company, and not contracted or temporary.</p>
1.4	Applicant Claims _____  Auditor Verifies _____	<p><b>Access Individuals</b>, other than those exempted from the drug screening requirements as discussed in Section 1.2 herein, are monitored for drugs/substance abuse by one of the following methods (applicant to check the option used):</p> <p><input type="checkbox"/> Option #1: On a random basis, 50% of employees are drug-screened annually.</p> <p style="text-align: center;"><b>OR</b></p> <p><input type="checkbox"/> Option #2: The local management has been trained in a qualified (pre-approved by NAID) "Substance Abuse Recognition Awareness Program."</p> <p><i>(See Employment Information Disclaimer.)</i></p>	<p>Auditor will look to see evidence of the method indicated on the Application:</p> <p>Option #1: Invoices/results from drug testing lab for random sampling drug screening of 50% of employees</p> <p style="text-align: center;"><b>OR</b></p> <p>Option #2: Documentation showing Program approval from NAID and proof that on-site management has completed this Substance Abuse Recognition training within the last year.</p>
1.5	Applicant Claims _____  Auditor Verifies _____	<p>All <b>Access Employees</b> have ongoing criminal record searches in accordance with one of the following methods (select only one):</p> <p><input type="checkbox"/> Option #1: One-third of Access Individuals have been randomly selected and criminal record searches conducted annually.</p> <p><input type="checkbox"/> Option #2: One-third of all Access Individuals are screened the first year, a different 1/3 are screened the following year, and the remaining 1/3 are screened in the third year.</p> <p><input type="checkbox"/> Option #3: All Access Individuals have Criminal Record searches conducted every three years.</p> <p style="text-align: center;">Year of most recent search: _____.</p> <p><i>(See Employment Information Disclaimer.)</i></p>	<p>Auditor to see documentation from an outside agency or source which verifies that one-third of the Access Individuals have had criminal record searches annually or that all Access Individuals are screened every three years.</p>
1.6	Applicant Claims _____  <input type="checkbox"/> <b>Not Applicable</b>  Auditor Verifies _____	<p>Drivers meet all licensing requirements of the governmental jurisdiction.</p> <p><i>(See Employment Information Disclaimer.)</i></p>	<p>The applicable law or regulation for commercial driver licenses will be made available and examined by the Auditor. Auditor will request driver license verification, and any other items required by law for all drivers listed on the Access and Non-Access Employees List.</p>

	Initial	Criteria	Audit Methodology
<b>OPERATIONAL SECURITY</b>			
2.1a	Applicant Claims _____ Auditor Verifies _____	The firm has written policies and procedures for drivers and destruction processing employees.	Auditor to inspect copy of policies and procedures manuals
2.1b	Applicant Claims _____ Auditor Verifies _____	Prior to gaining access to confidential material, all drivers and destruction processing employees must sign an acknowledgement indicating that they have received and read the Company's current written policies and procedures. A new acknowledgment must be signed by employees on an annual basis.	Auditor to inspect employee files for a signed acknowledgement of the Company's current written policies and procedures. This form must reference the version of the written policies and procedures that it applies to. A new acknowledgment must be signed by employees on an annual basis.
2.1c	Applicant Claims _____ Auditor Verifies _____	The Company has a written policy in place, stating that it will notify any Client of a potential release of, or unauthorized access to, that Client's Confidential Client Media that poses a threat to the security or confidentiality of that information as soon as reasonably possible.	Auditor will check procedures manual to ensure that there is a written policy stating that it will notify any Client of a potential release of, or unauthorized access to, that Client's Confidential Client Media that poses a threat to the security or confidentiality of that information as soon as reasonably possible.
2.1d	Applicant Claims _____ Auditor Verifies _____	The Company has a written policy in place, instructing and requiring employees to notify management of a potential release of, or unauthorized access to, Confidential Client Media that poses a threat to the security or confidentiality of the information.	Auditor will check procedures manual to ensure that there is a written policy, instructing and requiring employees to notify management of a potential release of, or unauthorized access to, Confidential Client Media that poses a threat to the security or confidentiality of the information.
2.1e	Applicant Claims _____ Auditor Verifies _____	The Company has a written policy that addresses the procedures for employees to follow during an unannounced audit. This policy must name at least one person or position of contact, which is to be contacted in the event of an unannounced audit at the destruction plant or the office.	Auditor will review the Company's written policies and procedures for their written policy instructing employees in the procedures to follow during an unannounced audit.
2.2	Applicant Claims _____ Auditor Verifies _____	<b>Access Individuals</b> display Company-issued photo I.D. badges at all times while on duty. Badges must minimally include a photo, employee name and Company name.	Auditor to inspect employees present to see that all are wearing appropriate photo I.D. badges.
2.3	Applicant Claims _____ <input type="checkbox"/> Not Applicable Auditor Verifies _____	While at Client's location, drivers and other employees of contractor must wear a specific uniform (minimum of Company shirt) to improve recognition by Clients.	Auditor to inspect uniform of at least one driver and confirm that wearing a uniform is specified in policies and procedure manual(s).

	Initial	Criteria	Audit Methodology
2.4	Applicant Claims _____ Auditor Verifies _____	<p>At the time that media is transferred from the Client’s custody to the custody of the Company’s employees or a third party carrier or other subcontractor, the Client must be provided with a receipt or certificate of destruction indicating type and quantity of media and an acknowledgement of the services rendered. An electronic receipt is acceptable, provided there is a verifiable electronic audit trail and the ability to provide the Client with the printed information.</p> <p>If services rendered by the Company after NAID Certification are not NAID Certified, but such services could be NAID Certified (plant-based or offsite services, onsite operations, and/or destruction endorsements for Paper/Printed Media, Micro Media or Electronic Media) and/or are recycling services of unshredded/intact paper, then the recipient of the services must be notified in writing that such service is NOT NAID Certified. This written notification may be contained on a materials receipt, certificate of destruction, current Client Agreement/contract or another written notice (including e-mail or another electronic method that may be printed) delivered by the Company to the Client /recipient of services.</p>	<p>Auditor will inspect the Company policies and procedures manual to ensure that client documentation process contains the requisite information and will inspect a copy or sample of the client documentation.</p> <p>If a subcontractor is used for transport prior to destruction, the subcontractor must provide the Client and the applicant Company with the Client receipt documentation. Auditor to verify documentation has been provided by the subcontractor and is being utilized by inspecting a copy of a past Client receipt.</p>
2.5	Applicant Claims _____ Auditor Verifies _____	<p>All media are always attended by a Company employee or physically secured from unauthorized access while in the custody of the destruction contractor or subcontractor before they are destroyed.</p>	<p>The Auditor will verify that containers used in the field to transport loose or small confidential media from the client’s facility to the destruction provider’s vehicle have operable locks and are locked when unattended. Non-contained media (i.e. on pallets or gaylords) must never be unattended during transport from client to collection vehicle and must be locked within vehicle when unattended by Company employee or subcontractor.</p> <p>Auditor will inspect the Company policies and procedures manual to assure that secure custody of the media prior to sanitization or destruction is addressed.</p> <p>For plant-based operations, Auditor will determine that there is a secured area designated for holding media when unattended until that media can be sanitized or destroyed.</p>
2.6	Applicant Claims _____ <input type="checkbox"/> <b>Not Applicable</b> Auditor Verifies _____	<p>All media are securely contained during transfer from Clients’ custody to transportation vehicle to prevent loss from wind, tipping/spillage or other atmospheric conditions.</p>	<p>Auditor to inspect collection equipment used by the contractor in the field to make sure it protects the media from loss due to wind, tipping/spillage or other atmospheric conditions.</p>
2.7	Applicant Claims _____ <input type="checkbox"/> <b>Not Applicable</b> Auditor Verifies _____	<p>All vehicles used for transfer of client media will have the applicable government inspection for roadworthiness on file.</p>	<p>Auditor will review paperwork from the most recent inspection of all Company’s commercial vehicles within the time frame stated in the applicable state law regarding the nature and frequency of these inspections. If there is a jurisdiction that does not require an inspection of commercial vehicles, Auditor will require a copy of the government statement saying so. Three vehicle records will be checked.</p>

	Initial	Criteria	Audit Methodology
2.8	Applicant Claims _____ <input type="checkbox"/> <b>Not Applicable</b>  Auditor Verifies _____	All vehicles used for transfer of client media will have lockable cabs and lockable fully enclosed boxes. The vehicle cab and box must be locked during transport and when unattended by an Access Individual.  _____ Number of Media Collection Vehicles / Trucks in fleet	Auditor will inspect trucks made available by the Company to verify that all cab doors and truck boxes are lockable and that locks work properly. Auditor will inspect the Company policies and procedures manual to assure that vehicle cab and box locking is addressed.  <b>Note:</b> If there are 3 trucks or less, all trucks must be made available for inspection. If there are 4 or more trucks, 75% of the fleet must be made available for inspection. If trucks are not made available, the Company must provide written testimony that those trucks not presented for inspection are of equal or superior condition of roadworthiness and security. The testimony must be on Company letterhead and signed by an officer of the Company.
2.9	Applicant Claims _____ <input type="checkbox"/> <b>Not Applicable</b>  Auditor Verifies _____	All drivers of collection-vehicles must have readily accessible two-way communication devices.  <b>Type of Device Used:</b> <input type="checkbox"/> Radio/CB <input type="checkbox"/> Cell Phone <input type="checkbox"/> Other (please indicate): _____	Auditor to verify each driver has the stated and operable two-way communication device with them or in the vehicle.
2.10	Applicant Claims _____ <input type="checkbox"/> <b>Not Applicable</b>  Auditor Verifies _____	<b>APPLIES TO PLANT-BASED CERTIFICATION ONLY</b>  Unauthorized access to the designated sanitization and secure destruction areas and Client media is effectively prevented.	Auditor to inspect all entrances to see that unauthorized access to secured areas is effectively preventable when media are not attended.  Auditor will verify that the Company policies and procedures manual covers access control and unauthorized access interdiction measures.
2.11	Applicant Claims _____ <input type="checkbox"/> <b>Not Applicable</b>  Auditor Verifies _____	<b>APPLIES TO PLANT-BASED CERTIFICATION ONLY</b>  All visitors entering the designated sanitization or secure destruction building sign a log with their name, time in, affiliation, and time out. Visitors must be issued a Visitor Badge and be escorted or under the supervision of an Access Employee at all times while in the building. This log info/record must be maintained for one year.	Auditor will examine visitor/contractor logs and verify records maintained for one year.

	Initial	Criteria	Audit Methodology
2.12	Applicant Claims _____  <input type="checkbox"/> <b>Not Applicable</b>  Auditor Verifies _____	<p><i><b>APPLIES TO PLANT-BASED CERTIFICATION ONLY</b></i></p> <p>There is a secure area within the building devoted specifically for Electronic Media sanitization and a separate area for physical destruction of media. No media or equipment ready for resale or simple disposal may be within these areas.</p>	<p>Auditor to inspect building to determine that separate secured areas exist for Electronic Media sanitization and physical media destruction; Staging for each process must have separate secure areas if not contained within the sanitization or destruction area.</p> <p>The secured areas within the building must meet the following specifications:</p> <ol style="list-style-type: none"> <li>1. The wall or fence securing this area must be a minimum of six feet tall and have a lockable gate or door.</li> <li>2. 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.</li> </ol>
2.13	Applicant Claims _____  <input type="checkbox"/> <b>Not Applicable</b>  Auditor Verifies _____	<p><i><b>APPLIES TO PLANT-BASED CERTIFICATION ONLY</b></i></p> <p>There is a monitored alarm system in place and utilized when the secure destruction building is unoccupied.</p>	<p>Auditor is to inspect alarm system to make sure it is operational and examine alarm test reports &amp;/or invoices from alarm monitoring service.</p>
2.14	Applicant Claims _____  <input type="checkbox"/> <b>Not Applicable</b>  Auditor Verifies _____	<p><i><b>APPLIES TO PLANT-BASED CERTIFICATION ONLY</b></i></p> <p>There is a closed circuit camera system monitoring all access points into the secure buildings/areas where confidential media are stored, processed and/or destroyed. All activities are monitored with sufficient clarity to identify people and their activities. There must be enough lighting at night or during other non-business hours to ensure that all images have sufficient clarity.</p> <p><b>Recordings must be retained for 90 consecutive days in an organized, retrievable manner.</b></p>	<p>Auditor to inspect the closed circuit monitoring system to meet criteria. This includes checking that the system has sufficient cameras and image quality to identify individuals and capture the full range of motion and all activities in the secure destruction process from point of entry into the building through final destruction, including any unauthorized access to the confidential information.</p> <p><b>CCTV playback must be available at the time of the scheduled audit.</b></p> <p>Auditor to inspect recording library system and to review four 4-minute samples:</p> <ul style="list-style-type: none"> <li>• Two random samples during operational hours</li> <li>• One random sample during non-operational hours</li> <li>• One sample from the 90<sup>th</sup> day back from the current date</li> </ul> <p>Recording of operations may be suspended for playback recordings.</p>
2.15	Applicant Claims _____  <input type="checkbox"/> <b>Not Applicable</b>  Auditor Verifies _____	<p><i><b>APPLIES TO PLANT-BASED CERTIFICATION ONLY</b></i></p> <p>The following Operational Security systems are checked and maintained on a monthly basis:</p> <ul style="list-style-type: none"> <li>• Alarm System</li> <li>• Lighting</li> <li>• Door Locks</li> <li>• Visitor Logs</li> </ul> <p>In addition to monthly Operational Security system checks, <b>the CCTV system must be checked on a weekly basis, including a minimum of five minutes of playback</b> to ensure that all cameras and recording systems are working correctly.</p> <p>Monthly and Weekly Logs must be kept for one year using the NAID-issued Forms (or the information/content contained on it).</p>	<p>Auditor to review the Monthly and Weekly Operational Security Maintenance Logs used to check, record and maintain the facility's operational security functions, including CCTV (except for a Collection Facility), Alarms, Lighting, Door Locks and Visitor Logs – records must be kept for one year.</p>

	Initial	Criteria	Audit Methodology
<b>SANITIZATION &amp; PHYSICAL DESTRUCTION PROCESS</b>			
3.1	<p>Applicant Claims</p> <hr/> <p><input type="checkbox"/> Not Applicable</p> <p>Auditor Verifies</p> <hr/>	<p><b>PHYSICAL DESTRUCTION OF ELECTRONIC MEDIA</b></p> <p>The Company has a written and verifiable process for the physical destruction (not wiping or overwriting) of Electronic Media. The Company also has written and verifiable processes for the following:</p> <ul style="list-style-type: none"> <li>• That prior to the destruction event the Company provides clients with a written description of the process for the physical destruction of Electronic Media.</li> <li>• That serial numbers of all Electronic Media being destroyed for each client are recorded, unless the Client has signed an agreement opting out of this requirement. And that any opt out agreement must state that the Company is obligated, under NAID Certification standards, to have the client sign the agreement if they choose to not have their serial numbers recorded.</li> <li>• That the log of recorded serial numbers of Electronic Media is returned to the Client upon the completion of the service, unless the Client has opted out of this requirement.</li> <li>• That a log of recorded serial numbers, a log of Clients that have opted out of serial number recordation, and copies of opt-out agreements are retained for a specified length of time, as documented in the Company's written policies, or in accordance with Client Agreements or contractual stipulations.</li> </ul> <p>Method of Physical Destruction:</p> <hr/> <p><input type="checkbox"/> Plant-based only</p> <p><input type="checkbox"/> Onsite only</p> <p><input type="checkbox"/> Plant-based &amp; Onsite</p> <p>If the Company sub-contracts physical destruction to another vendor, the Company meets meet all requirements for Transfer of Custody, as described in Section 3.7 herein.</p>	<p>Auditor will review the <b>Sanitization Process Questionnaire</b> and the Company's written policies and procedures for their standard physical destruction (not wiping or overwriting) of Electronic Media. Auditor will also review the Company's written policies and procedures for the following provisions:</p> <ul style="list-style-type: none"> <li>• An instruction that all clients must be provided with a written description of the process for the physical destruction of Electronic Media, prior to the destruction event.</li> <li>• An instruction that all serial numbers of sanitized or destroyed Electronic Media are logged and returned to the Client after the completion of the service, unless the Client opts out by signing an opt out agreement.</li> <li>• An instruction that if the client has opted out of having their serial numbers recorded, they must sign an opt-out agreement that clearly states that the recordation of serial numbers is a NAID Certification requirement.</li> <li>• That a log of recorded serial numbers, a log of Clients that have opted out of serial number recordation, and copies of opt-out agreements are retained for a specified length of time, as documented in the Company's written policies, or in accordance with Client Agreements or contractual stipulations.</li> </ul>

	Initial	Criteria	Audit Methodology
3.2	<p>Applicant Claims</p> <hr/> <p><input type="checkbox"/> Not Applicable</p> <p>Auditor Verifies</p> <hr/>	<p><i>APPLIES TO ONSITE CERTIFICATION ONLY</i></p> <p><b>SANITIZATION OF ELECTRONIC MEDIA (Onsite)</b></p> <p>The essential components of the Sanitization Process are defined in the <b>Sanitization Process Questionnaire responses</b>.</p> <p>The Company has a written and verifiable process for the sanitization of Electronic Media, to include the following:</p> <ul style="list-style-type: none"> <li>• Acceptance, identification &amp; recording (of serial numbers), and tagging of Electronic Media. Procedures for recording serial numbers must include the following:               <ul style="list-style-type: none"> <li>○ That serial numbers of all Electronic Media being sanitized for each client are recorded, unless the Client has signed an agreement opting out of this requirement. And that any opt out agreement must state that the Company is obligated, under NAID Certification standards, to have the client sign the agreement if they choose to not have their serial numbers recorded.</li> <li>○ That the log of recorded serial numbers of sanitized Electronic Media is returned to the Client upon the completion of the service, unless the Client has opted out of this requirement.</li> <li>○ That a log of recorded serial numbers, a log of Clients that have opted out of serial number recordation, and copies of opt-out agreements are retained for a specified length of time, as documented in the Company’s written policies, or in accordance with Client Agreements or contractual stipulations.</li> </ul> </li> <li>• Wiping Software Product used</li> <li>• Recovery or verification Software used</li> <li>• Quality Control procedures, to include the following:               <ul style="list-style-type: none"> <li>○ The quality control software manufacturer is different than the sanitization software manufacturer, and that the Company employee who performs quality control is never the same person that performed sanitization on the same drive(s). In the event that the same Company employee performs both sanitization and quality control, the Auditor will determine whether the quality control procedures that are in place effectively ensure that all information has been removed from the sanitized drive(s).</li> <li>○ A specific number or percentage of sanitized drives, as determined by the Company, is selected for quality control assessment.</li> <li>○ Quality control assessment is performed at each Client’s site, and deemed successful, prior to leaving the site.</li> <li>○ Instructions that in the event of a quality control assessment revealing recoverable data from a sanitized drive, all drives processed since the last successful quality control assessment will be reprocessed.</li> <li>○ Instructions that a log must be kept of all quality control assessments to include:                   <ul style="list-style-type: none"> <li>▪ The date of the check</li> <li>▪ The quantity of drives checked</li> <li>▪ The outcome (fail/pass)</li> <li>▪ A description of corrective actions taken as the result of any failed quality control checks.</li> <li>▪ Serial numbers of all drives that fail the sanitization process must be recorded in the Quality Control log, regardless of any serial number recordation opt-out agreement that may be in place</li> </ul> </li> </ul> </li> <li>• The recordkeeping audit trail for the CPU throughout entire sanitization process</li> <li>• Confirmation receipt or Certificate of Destruction reflecting serial numbers is provided to client indicating Electronic Media have been physically sanitized and/or destroyed.</li> <li>• Documentation left with Client to indicate any drives that failed the wiping process. This document must include the serial numbers of those drives, regardless of any serial number recordation opt-out agreement that may be in place. If any non-sanitized drives are left with the Client, this document must also state that custody of the Electronic Media is being transferred back to the Client.</li> </ul>	<p>Auditor will review Questionnaire responses and the company’s written policies and procedures detailing their standard Electronic Media <b>sanitization process</b>.</p> <p>Applicant will demonstrate its ability to successfully sanitize Electronic Media by:</p> <ul style="list-style-type: none"> <li>• Completing sanitization on four (4) control devices provided to Applicant during a mock operation staged at a predetermined location – These devices will have been preformatted with a known amount of control data which must be sanitized and returned to the Auditor prior to his departure. These will be sent to a data recovery service to verify that the data is not conventionally retrievable.</li> </ul> <p>All four (4) devices will be sent to a data recovery service to verify that data is not conventionally retrievable. If any devices are found to be containing data, Applicant will NOT be NAID Certified.</p> <p>Auditor will observe the entire sanitization process.</p>

	Initial	Criteria	Audit Methodology
3.3	<p>Applicant Claims</p> <hr/> <p><input type="checkbox"/> Not Applicable</p> <p>Auditor Verifies</p> <hr/>	<p><i>APPLIES TO PLANT-BASED CERTIFICATION ONLY</i></p> <p><b>SANITIZATION OF ELECTRONIC MEDIA (Plant-based)</b></p> <p>The essential components of the Sanitization Process are defined in the <b>Sanitization Process Questionnaire responses</b>.</p> <p>The Company has a written and verifiable process for the sanitization of Electronic Media, to include the following:</p> <ul style="list-style-type: none"> <li>• Staging</li> <li>• Acceptance, identification &amp; recording (of serial numbers), and tagging of Electronic Media. Procedures for recording serial numbers must include the following: <ul style="list-style-type: none"> <li>○ That serial numbers of all Electronic Media being sanitized for each client are recorded, unless the Client has signed an agreement opting out of this requirement. And that any opt out agreement must state that the Company is obligated, under NAID Certification standards, to have the client sign the agreement if they choose to not have their serial numbers recorded.</li> <li>○ That the log of recorded serial numbers of sanitized Electronic Media is returned to the Client upon the completion of the service, unless the Client has opted out of this requirement.</li> <li>○ That a log of recorded serial numbers, a log of Clients that have opted out of serial number recordation, and copies of opt-out agreements are retained for a specified length of time, as documented in the Company's written policies, or in accordance with Client Agreements or contractual stipulations.</li> </ul> </li> <li>• Wiping Software Product used</li> <li>• Recovery or verification Software used</li> <li>• Quality control procedures, to include the following: <ul style="list-style-type: none"> <li>○ The quality control software manufacturer is different than the sanitization software manufacturer, and that the Company employee who performs quality control is never the same person that performed sanitization on the same drive(s).</li> <li>○ A specific number or percentage of sanitized drives, as determined by the Company, is selected for quality control assessment on a routine basis.</li> <li>○ Instructions that in the event of a quality control assessment revealing recoverable data from a sanitized drive, all drives processed since the last successful quality control assessment will be reprocessed.</li> <li>○ Instructions that a log must be kept of all quality control assessments to include: <ul style="list-style-type: none"> <li>▪ The date of the check</li> <li>▪ The quantity of drives checked</li> <li>▪ The outcome (fail/pass)</li> <li>▪ A description of corrective actions taken as the result of any failed quality control checks.</li> </ul> </li> </ul> </li> <li>• Tagging/identification and separation/isolation of sanitized Electronic Media after processing</li> <li>• The recordkeeping audit trail for the Electronic Media throughout entire sanitization process</li> <li>• Confirmation receipt or Certificate of Destruction reflecting serial numbers is provided to client indicating Electronic Media have been physically sanitized and/or destroyed.</li> </ul>	<p>Auditor will review Questionnaire responses and the Company's written policies and procedures detailing their standard Electronic Media <b>sanitization process</b>.</p> <p>Applicant will demonstrate its ability to successfully sanitize Electronic Media by:</p> <ul style="list-style-type: none"> <li>• Completing sanitization on two (2) control devices provided to Applicant at audit appointment – These devices will have been preformatted with a known amount of control data which must be sanitized and returned to the Auditor prior to his departure. These will be sent to a data recovery service to verify that the data is not conventionally retrievable.</li> <li>• Random selection of two (2) devices from the Applicant's processed inventory, each between 80 &amp; 120 GB in size – Auditor will randomly select the two devices which will be sent to the data recovery service to verify that the data is not conventionally retrievable. These will be returned to Applicant after testing/analysis is completed.</li> </ul> <p>All four (4) devices will be sent to a data recovery service to verify that data is not conventionally retrievable. If any devices are found to be containing data, Applicant will NOT be NAID Certified.</p> <p>Auditor will observe the sanitization process for at least one device.</p> <p><b>(For Solid State Electronic Media Beta Phase Only: NAID Certification staff will review the Sanitization Process Questionnaire and conduct a pre-audit site visit or interview to determine and agree upon the type and quantity of control Electronic Media and audited Electronic Media to be sent for post audit verification.)</b></p>

	Initial	Criteria	Audit Methodology
3.4	Applicant Claims _____  <input type="checkbox"/> <b>Not Applicable</b>  Auditor Verifies _____	<p><b>APPLIES TO PLANT-BASED CERTIFICATION ONLY</b></p> <p>Standard operating procedures states that the destruction or Electronic Media sanitization is completed within 30 days, or the policies and procedures, the terms and conditions, and contracts used by the applicant must specify and reflect the actual time frame in which destruction is performed.</p> <p>Standard operating procedures state that sanitization and physical destruction of Electronic Media occurs within (indicate timeframe) _____.</p>	Auditor will check procedures manual to assure that there is a procedure stating that all media are destroyed or sanitized within requisite timeframe and verify the timeframe indicated by the applicant. Exceptions include acts of God, breakdowns or client instruction (or permission) to retain media for a longer period
3.5	Applicant Claims _____  Auditor Verifies _____	<p>The Sanitization process has a method of quality control in place to ensure all information has been removed from the sanitized Electronic Media.</p> <p>The quality control procedures are described in the Company's procedures manual and the <b>Sanitization Process Questionnaire responses</b>, Minimally this quality control procedure must include:</p> <ul style="list-style-type: none"> <li>• The quality control software manufacturer is different than the sanitization software manufacturer, and that the Company employee who performs quality control is never the same person that performed sanitization on the same drive(s). For Onsite Sanitization, if the same Company employee performs both sanitization and quality control, the Auditor will determine whether the quality control procedures that are in place effectively ensure that all information has been removed from the sanitized drive(s).</li> <li>• A specific number or percentage of sanitized drives, as determined by the Company, is selected for quality control assessment on a routine basis.</li> <li>• For Onsite Sanitization, the Quality Control assessment is performed at each Client's site, and deemed successful, prior to leaving the site.</li> <li>• Instructions that in the event of a quality control assessment revealing recoverable data from a sanitized drive, all drives processed since the last successful quality control assessment will be reprocessed.</li> <li>• Instructions that a log must be kept of all quality control assessments to include:                         <ul style="list-style-type: none"> <li>○ The date of the check</li> <li>○ The quantity of drives checked</li> <li>○ The outcome (fail/pass)</li> <li>○ A description of corrective actions taken as the result of any failed quality control checks.</li> <li>○ Serial numbers of all drives that fail the sanitization process must be recorded in the Quality Control log, regardless of any serial number recordation opt-out agreement that may be in place.</li> </ul> </li> </ul>	<p>Auditor will review <b>Sanitization Process Questionnaire response</b> and check procedures manual to assure that quality control procedures which ensure all information has been removed from the sanitized Electronic Media are described; minimally this requires a specific number or percentage of sanitized drives to be selected on a routine basis for data recovery attempts, and any quality control assessment revealing recoverable data from a sanitized drive requires the Company to reprocess any and all drives processed since the last successful quality control check.</p> <p>The Auditor will also verify that the quality control software manufacturer is different than the sanitization software manufacturer, and that the Company employee who performs quality control is never the same person that performed sanitization on the same drive(s). In the event that the same Company employee performs both sanitization and quality control, the Auditor will determine whether the quality control procedures that are in place effectively ensure that all information has been removed from the sanitized drive(s).</p> <p>For Onsite Sanitization Operations, the Auditor will also check the written quality control procedures to ensure that quality control is performed at each Client's site, and deemed successful, prior to leaving the site.</p> <p>Auditor will review quality control assessment logs, including review of any corrective actions.</p>
3.6	Applicant Claims _____  <input type="checkbox"/> <b>Not Applicable</b>  Auditor Verifies _____	<p>Physically destroyed media must be disposed (sold, gifted, or discarded) in a responsible manner.</p> <p>Applicant must attach a list of all current recipients (within past year) of destroyed media, indicating type of media and final disposition of the media by these recipients.</p>	Auditor will review list of recipients and manner in which the media are disposed subsequent to destruction and verify that Company has written agreements or documentation in place to support stated responsible disposal (materials recycling, metals recovery/smelting, landfill, etc.).

	Initial	Criteria	Audit Methodology
3.7	Applicant Claims _____  <input type="checkbox"/> <b>Not Applicable</b>  Auditor Verifies _____	<p><b>TRANSFER OF CUSTODY (IF APPLICABLE)</b></p> <p>A third party destruction, transport or logistics service is used for each of the following services as indicated below, whether subcontracted or arranged by Applicant for their Client.</p> <p>Applicant (Check all that apply)</p> <p><input type="checkbox"/> Temporary Staffing (Not allowed for Onsite Sanitization)</p> <p><input type="checkbox"/> Transportation (of media prior to destruction)</p> <p><input type="checkbox"/> Physical Destruction of Electronic Media</p> <p><input type="checkbox"/> Other (describe): _____</p> <p>Note: If the Applicant arranges for the use of an agent on behalf of the client (i.e. transportation for client's media prior to sanitization process or physical destruction of Electronic Media), full disclosure must be made to the client regarding the circumstances of the custody chain and whether that meets the applicable NAID Certification specifications.</p>	<p>Auditor will review Subcontractor list provided and discuss with Company all transfer of custody scenarios claimed.</p> <p>In the event that there is a Transfer of Custody, or a transfer or extension of Fiduciary Responsibility (i.e., Subcontracting), the following policies are necessary for the Applicant's operation to be NAID Certified:</p> <ul style="list-style-type: none"> <li>All affected clients have explicitly been notified in writing (including email or other electronic method) that they are fully aware of the process; including                             <ul style="list-style-type: none"> <li>any imminent or potential transfer of custody and/or fiduciary responsibilities, including identifying the parties destined to accept custody</li> <li>the exact location of destruction</li> <li>the method of the destruction</li> </ul> </li> <li>All Access Individuals of all companies or agents in the chain of custody, including third party transporters, acknowledge in writing that they understand that all media with which they come in contact may be confidential, and accept the fiduciary responsibility; or alternatively, such companies agree in writing or certify to the Company that their employees have acknowledged in writing such understanding and agreement. Copies of such agreements shall be on file at the NAID Member's office. If Company does not obtain such commitments, then it must notify its Clients in writing that such service is not NAID Certified.</li> <li>All Access Employees and Individuals in the subsequent chain of custody submits to the same background screening required for NAID Certification.</li> <li>All agents subsequently accepting custody of media must meet the current NAID Certification specifications for all applicable criteria.</li> </ul> <p>Documentation to verify above policies must be available at the Applicant's location. When a site visit is required for verification, Applicant assumes responsibility for any additional time/costs of the Auditor and for making the necessary arrangements with the agent for such site visit.</p>
<b>COMPANY ASSURANCES</b>			
4.1	Applicant Claims _____  Auditor Verifies _____	Company is a legally registered business in the state of residence.	Auditor to examine business license.
4.2	Applicant Claims _____  Auditor Verifies _____	General liability insurance (aggregate or umbrella) of \$2,000,000 or more.  <b>General Liability (Aggregate/Umbrella Indemnification Level): \$ _____ million</b>	Auditor to examine valid insurance documents, which could be a certificate of insurance or a letter from broker verifying coverage limits. Letter must be dated no earlier than one month prior to audit.
4.3	Applicant Claims _____  Auditor Verifies _____	Company is current with all local, state, and federal permits/licenses required for the recycling of computer equipment.	Auditor to examine permits/license required for the recycling of computer or electronic equipment, if applicable.

Upon completion of the application, including providing responses to the *Sanitization Process Questionnaire*, please submit the entire application and additional required materials to:

Fax: (620) 788-4144 (if paying by credit card)

OR

Mail: NAID, Certification Program, 1951 W. Camelback Rd. Suite #350, Phoenix, AZ 85015

## **SANITIZATION PROCESS QUESTIONNAIRE**

---

*Please fully respond to each of the questions below, as well as indicating where (page or section) it is addressed within your company's policies and procedures. Please attach a separate sheet with your responses. If applying for both Onsite and Plant-based Sanitization Operations, please fill out a separate questionnaire for each type of operation.*

1. Do you provide your Clients with any written information diagramming or describing the stages of your sanitization process? If yes, please attach.
2. Briefly describe the receipt/acceptance of media, identification and recording of serial numbers for Electronic Media, and labeling of media for either sanitization or physical destruction:
3. How are Electronic Media for sanitization, Electronic Media for physical destruction and Electronic Media that require no destruction services identified and segregated?
4. Do you stage/hold Electronic Media identified for sanitization in an area other than where they will be sanitized? If so, describe when and how these are moved to the sanitization area.
5. Do you stage/hold Electronic Media identified for physical destruction in an area other than where they will be destroyed? If so, describe security and when and how these are moved to the physical destruction area.
6. How is Electronic Media to be sanitized and those to be physically destroyed secured from unauthorized access and isolated from commingling with other equipment or media for disposal, resale or some other purpose?
7. Identify the sanitization/wiping software product or equipment used and describe the method utilized, i.e. 1's and 0's, random characters, Secure Erase, etc.
  - Manufacturer:
  - Model/Version Number:
  - Serial Number:
  - Method:
8. How do you determine when wiping/sanitization is no longer acceptable, i.e. damaged sectors, and that physical destruction is now required?
9. Briefly describe your physical destruction process for Electronic Media.
10. Identify the Recovery/Verification Software or Equipment used during the Quality Control check to confirm that no information is recoverable from the sanitized Electronic Media (or define in detail method used); the QC software manufacturer must be different than the Sanitization software manufacturer.
  - Manufacturer:
  - Version/Model Number:
  - Serial Number:

11. Briefly describe your firm's Quality Control Process that confirms again that no recoverable information is on the sanitized Electronic Media. The process must minimally include the following:

- Percentage or number of random devices selected
- The QC process on a particular device is performed by a different individual than the one who sanitized the unit
- Procedure to follow if check reveals that the device has not been completely or properly sanitized (recoverable information on it)

12. After sanitization and quality control, how is Electronic Media tagged/identified and separated/isolated from those still to be sanitized or destroyed?

13. Describe or provide a sample of the recordkeeping audit trail for Electronic Media throughout the entire sanitization process.

14. Provide a sample copy of the certificate or confirmation of Electronic Media sanitization and/or physical destruction provided to the Client. This should, at minimum, include:

- Original receipt date of Electronic Media
- Serial numbers of Electronic Media
- Completion date for sanitization and/or physical destruction

15. Do you use a common carrier, subcontractor or another non-employee or entity to transport Electronic Media for sanitization or destruction? If yes, please describe the process and include a list of all entities used within the last year.

# Certification Documents & Forms

NAID<sup>®</sup> has designed specific documents and forms to be used for the Certification Program that are on the following pages for your convenience. These forms can be used as designed or you can create your own personalized form in its place. If you do decide to develop your own form please be certain to reflect, at the minimum, the same information shown on NAID's form. These forms can also be found at [www.naidonline.org](http://www.naidonline.org) under Forms.

<b>Form</b>
<b>Audit Preparation Checklist</b>
<b>Additional Required Materials for Certification Application</b>
<b>Agreement for Responsible Disposal</b>
<b>Employee Notice of Unannounced Audits</b>
<b>Serial Number "Opt Out" Agreement</b>
<b>Operational Security Maintenance Check</b>
<b>Substance Abuse Recognition Training Program Approval Submission Form</b> <i>(for pre-approving Substance Abuse Programs if Option #2 for Item 1.3 on the Certification Application is chosen instead of randomly drug screening.)</i>
<b>Visitor Log</b>

## NAID® CERTIFICATION PROGRAM SANITIZATION AUDIT PREPARATION CHECKLIST

The following checklist has been prepared to help you expedite a successful Certification audit. You should review this checklist at least one week prior to your scheduled audit to ensure all items are in place.

### Items 1.1 through 1.6 – EMPLOYEE REQUIREMENTS

- All** employee files must contain completed **Confidentiality Agreements** and an **I-9 form** (or proper work permit/registration paperwork).
- All **ACCESS** employee files must contain an **Employment History Verification**, a **Criminal Record Search** (at least 7 years of history) and **Drug Screening Results**.\*
- All employee files for **DRIVERS** must contain a copy of a **valid driver license** and/or commercial driver license and any additional items required by governmental jurisdiction for drivers.
- All drivers and destruction processing employee files must contain an acknowledgment of the company's written policies and procedures. A new acknowledgment must be signed on an annual basis.
- File containing documentation supporting **annual random Access employee criminal searches**.
- For the **annual Access employee drug/substance** monitoring:
  - Option 1 - Drug/Substance Screening on annual random basis, then a file containing documentation supporting the 50% annual random **ACCESS** employee drug testing should be available.

OR

- Option 2 – Drug/Substance Management Training, then a file containing proof of completed yearly management training should be in available.

*\*Individuals who are officers, directors, owners and/or partners of the applicant company or other individuals who have access to, can grant or authorized access to the confidential materials to be destroyed at the applicant's location but who are not engaged in the day-to-day operation of the applicant company are exempt from the employment verification and drug screening requirements.*

### Items 2.1 through 2.15 – OPERATIONAL SECURITY

- Policies and Procedures manual** for employees and drivers updated and accessible. Employee manual must include:
  - Stated media destruction timeframe(s)
  - Quality control procedures
  - Customer documentation process that includes customer acknowledgement, receipt or agreement of the specific services they have received (Sample of documentation must be available for the auditor)
  - Access controls and unauthorized access prohibiting measures (Plant-based operations)
  - The standard physical destruction method of computer hard drives (not wiping or overwriting)
  - Unannounced audit procedure and process – at least one person should be named as a contact in the event of an unannounced audit
  - Policy for notifying management of a potential release of, or unauthorized access to confidential Customer Material
- All **ACCESS** employees in possession of and utilizing **photo I.D. badges** while on duty.
- Company uniform** worn by required employees.
- Customers are provided with a receipt at the time of Media pickup, which includes the following:
  - Type of Media
  - Quantity of Media
  - Acknowledgement of the services rendered (Sanitization/overwriting or physical destruction)
- Collection vehicles protect material from loss due to wind, tipping/spillage or other atmospheric conditions.
- File containing most recent inspections of all commercial vehicles. Inspections must be within the timeframe stated in the applicable state laws.\*\*
- The **required number of vehicles** to be inspected will be available on the day of audit. (Requirements are: Three or less, all vehicles must be available. Four or more vehicles, 75% of vehicles must be available.) \*\*\*
- All vehicles used for transfer of media have lockable cabs and lockable fully enclosed boxes. Locks must always be used during transport and when left unattended.
- Readily accessible, **operable two-way communication devices** for all drivers of collection vehicles.

## AUDIT PREPARATION CHECKLIST

### -continued-

- Visitor badges** are available. (All visitors must sign visitor log and must be escorted or under the supervision of an ACCESS individual at all times while in the plant.)
- Visitor logs** available for one year.
- A secured area designated is available for holding media when unattended until destroyed.
- A secured area devoted to hard drive sanitization is available.
- A separate area for physical destruction of hard drives is available.
- If the building is not devoted to only destroying media, then a **secured area** within building must meet these certification requirements:
  - Enough space within the area to stage all materials to be destroyed.
  - Wall or fence securing the area must be a minimum of 6ft tall. (If the wall or fence does NOT go all the way to the ceiling then the area MUST have a ceiling mounted sensor alarm inside and over the perimeter of the secured destruction area to detect breach of secured fence/wall.)
  - Wall or fence securing the area must have lockable gate or door.
- Monitored alarm system** in place and utilized when secure destruction building/area is unoccupied.
- Closed circuit camera system monitoring all access points into secure destruction building/area.
- Closed circuit camera system provides sufficient clarity to identify individuals and their activities.
- CCTV playback** available to auditor for **90 days** from date of audit.
- Operational Security Maintenance Check logs** available for one year.
  - Alarm, Lighting, Door Locks and Visitor Logs are checked on a monthly basis.
  - CCTV system is checked on a weekly basis, which includes a minimum five minutes of playback to ensure that the cameras and recording system are operating correctly.
- An ACCESS individual is available on the day of the audit to operate the CCTV equipment for the auditor.

*\*\*If there is a jurisdiction which does not require inspections, the file must contain proof of the government statement supporting this.*

*\*\*\*If all vehicles are not made available to auditor, the company must provide written testimony on company letterhead that those vehicles are of equal or superior condition or roadworthiness and security. The testimony must be signed by an officer or the company. The required number of vehicles though, must be available for the auditor*

### Items 3.1 through 3.7 – THE SANITIZATION & TRANSFER OF CUSTODY PROCESS

- Written Policies and Procedures, as referenced in the Sanitization Process Questionnaire, are available.
- File containing documentation/agreements for the recipients of destroyed materials submitted on your Certification Application. The signed **Agreement for Responsible Disposal of Materials** (or customized document with similar wording) would be between you and your recipient indicating the type of media being destroyed and the final disposition of said media.
- IF APPLICABLE**, file containing supporting documentation for any **transfer of custody** scenarios. This would include subcontractor list, subcontractor agreements, client agreements and proof of meeting certification requirements.

### Items 4.1 through 4.3 – COMPANY ASSURANCES

- File containing business license(s) and any other supporting documentation on business.
- File containing **valid proof of general liability insurance** (aggregate or umbrella) of **\$2,000,000.00** or more.
- File containing **permits/license** required for the recycling of computer or electronic equipment, if applicable.

**Note:** The  indicates sample forms that are available online at [www.naidonline.org](http://www.naidonline.org) either under Forms or in the Members Only section on the Certification Program page.

## NAID<sup>®</sup> CERTIFICATION PROGRAM ADDITIONAL REQUIRED MATERIALS FOR APPLICATION

Company Name: \_\_\_\_\_ City/Town: \_\_\_\_\_ Audit #: \_\_\_\_\_

### Access Individuals and Non Access Individuals List

Owners/Partners/Officers of the Company	Title	Involved in Daily Operations Y/N	NAID Auditor use only					
			Conf Agr	Criminal	Drug	Driver Req	File Checked	

*\*All individuals listed here must have a signed Confidentiality Agreement and Criminal Record Search on file. If the individual is not involved in the daily operations of the business, then they can be exempt from the employment verification and drug screening requirements.*

Employee Name	Date of Hire	Access Y/N	Driver Y/N	Citizen Y/N	NAID Auditor use only						
					All Employees		Access Employees only			File Checked	
					Conf Agr	I-9	Emp Ver	Criminal	Drug		Driver Req
1.											
2.											
3.											
4.											
5.											
6.											
7.											
8.											
9.											
10.											
11.											
12.											
13.											
14.											
15.											

## ADDITIONAL REQUIRED MATERIALS FOR APPLICATION

-continued-

Company Name: \_\_\_\_\_

City/Town: \_\_\_\_\_

### List of Destruction and Collection Vehicles

Destruction or Collection	Vehicle Make	Vehicle Model	Vehicle Vin Number	License Plate Number	State/Country of License
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

### List of Additional Paper/Printed Media Destruction Equipment (cont. from Item 3.1)

Equipment Type (Continuous Shred, Cross Cut, Pierce & Tear, Pulverizer, Disintegrator, Hammermill, Unspecified Equipment* or Pulping/Incineration [plant-based only])	Mobile or Plant-based	Manufacturer	Model	Serial #	Capacity (lbs/hr)	HP
2.						
3.						
4.						
5.						

\*For Unspecified Equipment please attach detailed description with OEM specs, including dimensions/specification of cutting mechanism (screen hole size, blade width, etc.). Attach additional sheets if necessary.

### List of Recipients of Destroyed Materials

Name of Recipient	Final Disposition of Materials (pulping, incineration, smelting, etc.)
1.	
2.	
3.	

AGREEMENT FOR RESPONSIBLE DISPOSAL OF DESTROYED MATERIALS

(between a Secure Destruction Service and Disposal Agent)

The following Secure Destruction Service is NAID® Certified or seeking NAID® Certification and is in possession of destroyed materials as identified below that it must responsibly dispose:

SECURE DESTRUCTION SERVICE firm: \_\_\_\_\_

Address: \_\_\_\_\_

Destroyed Materials consisting of: \_\_\_\_\_

The following Disposal Agent accepts the Destroyed Materials and will responsibly dispose of these materials in the method identified below:

DISPOSAL AGENT firm: \_\_\_\_\_

Address: \_\_\_\_\_

Final Disposition Method of Materials Received: \_\_\_\_\_

\_\_\_\_\_

By signature below, the Disposal Agent agrees to the following in accepting the Destroyed Materials from the Secure Destruction Service:

- Disposal Agent agrees to process and route the Destroyed Material by a mutually acceptable method and to a mutually agreed destination that fulfills the obligation to keep them from entering the public realm in a manner in which they could be reconstituted (such as in packing materials or animal bedding) or that is violation of any environmental regulations.
- The Disposal Agent agrees that the final disposition method identified above will be adhered to unless notice and permission have been obtained from the Secure Destruction Service firm in writing in advance.
- The Disposal Agent understands that the decision to use their firm to accept the Destroyed Material and process it under the agreed manner is required by the NAID Certification standards.
- The Disposal Agent understands that the decision by the Secure Destruction Service to transfer the Destroyed Materials to the Disposal Agent is made only in consideration of their ability and willingness to comply with this agreement.
- The Disposal Agent agrees to process and dispose of the Destroyed Materials as agreed herein
- The Secure Destruction Service also agrees that this is not an agreement that transfers any obligation or intention on the part of the Disposal Agent to provide secure destruction services.

Disposal Agent

Representative's Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Representative's Printed Name: \_\_\_\_\_



# NOTICE TO EMPLOYEES UNANNOUNCED AUDITS for NAID CERTIFICATION



All employees are hereby notified that **your company**, as a NAID Certified Operation, **is subject to Unannounced Audits** based on the Certification criteria of your most recently completed and approved Certification Application with NAID. A downloadable copy of the application and criteria can be found at [www.naidonline.org](http://www.naidonline.org)

## **ABOUT THE AUDITOR**

- All Certification Audits are conducted by NAID-subcontracted, independent auditors who have achieved their CPP (Certified Protection Professional) designation – the highest level of professional security management accreditation from ASIS International.
- The Auditor is charged with the responsibility and discretion to confirm that your company is complying with NAID Certification standards/criteria.

When an Auditor arrives for an Unannounced Audit, please contact the following

***COMPANY REPRESENTATIVE(S)/AUDIT CONTACT***

## **YOUR RIGHTS**

- **ASK and VERIFY** the following from **AUDITOR**:
  - **Auditor Assignment & Confidentiality Agreement**
    - Must be signed and dated by NAID Program Official and Auditor
    - You may make a copy of this for your company records
  - **Auditor Photo ID Badge**
    - Must be signed by auditor
    - You may copy down the Auditor # if you wish to verify
  - If you have any reason to doubt the legitimacy of the audit, you may contact NAID as indicated below and/or see the auditor photos posted in the Certification Program section of the “Members Only” page of [www.naidonline.org](http://www.naidonline.org).
- Only **allow the Auditor access** to the operations and/or documentation **to what you**, as an individual employee, **have access**.
- The Audit **should not unreasonably disrupt** your current operations or ability to perform **services**. This Unannounced Audit is a check to see that your company practices are consistent with the Certification standards. Therefore, the auditor will **NOT** be reviewing all of the Certification documentation &/or criteria.

## **YOUR RESPONSIBILITIES**

- The **auditor should be allowed access to the operations and documentation** necessary to verify that your company meets the Certification standards/criteria as set forth in the Certification Application. If you have the authority to admit the auditor, please do so.
- If you cannot provide the auditor access to particular aspects that s/he wants to see, please **notify the appropriate person at your company** who can provide this access, i.e. owner or Audit Contact (indicated above).
- If asked, you should **sign the Auditor’s Report** acknowledging that the auditor did come to your operations to conduct an Unannounced Audit – your signature does **NOT** indicate agreement with the findings in the report.

**National Association for Information Destruction, Inc.**

**NAID Certification Program**

**1951 W Camelback Rd, Suite 350, Phoenix, AZ 85015**

**Phone: (602) 788-6243 ext. 202 or ext. 206**

**Web site: [www.naidonline.org](http://www.naidonline.org)**

**Email: [Certification@naidonline.org](mailto:Certification@naidonline.org)**

# Serial Number Recordation "Opt-Out" Agreement

As a condition of NAID AAA Certification, \_\_\_\_\_ is required  
NAID AAA Certified Company  
to record the serial numbers of all computer hard drives or Central Processing Units (CPUs) that are physically destroyed and/or sanitized, unless their clients release them from that requirement in writing and in advance by executing this form.

The recording of serial numbers of destroyed computer hard drives or CPUs could be considered a critical element in determining, investigating and defending against regulatory non-compliance, potential data breaches, and data breach notification requirements. Failure to obtain a written record of the serial numbers of destroyed computer hard drives or CPUs could possibly be considered irresponsible or negligent in the event that the proper destruction of those devices is questioned at some point in the future.

## AGREEMENT

I \_\_\_\_\_, as a duly appointed and authorized representative of  
\_\_\_\_\_, do hereby release \_\_\_\_\_ from their  
(Client Name) NAID AAA Certified Company

obligation under the NAID AAA Certification requirements to record the serial numbers of  
computer hard drives or CPUs that are sanitized and/or physically destroyed by them on our behalf in accordance with the existing terms of service. I understand that

\_\_\_\_\_ will still be provided with a Certificate of Destruction,  
(Client Name)  
to include the date and the quantity of the items that have been securely destroyed and/or sanitized.

I agree that NAID and \_\_\_\_\_ will be held harmless from all claims, loss, or  
NAID AAA Certified Company  
threatened loss, or any expense by reason of the liability or potential liability arising from the failure to record the serial numbers of destroyed computer hard drives or CPUs.

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Print Company Name

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

NAID® Certification Program

# Operational Security Maintenance Check

*For Plant-based NAID Certified Operations  
(must be kept on file for one year)*

MONTHLY checks to ensure systems are functional and in compliance with NAID Certification Standards			
Alarm System		Initial	Corrective Actions/Notes
Motion Detectors	Visually inspect and walk check each sensor . Observe light diodes - blinking indicates motion detected. Check that 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. It is recommended, but not required, that contacts be mounted with one-way screws and wiring from contact to inside the wall/door be in conduit.		
Key Pads	Visually inspect for functionality and test all circuits, i.e. opening/closing reports. Consider if access code needs to be replaced - once every three months is a good practice.		
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		
Visitor Access Logs			
Visitor In/Out Logs	Visually check that logs are being completed properly (both check in and out are recorded) and filed		# of visitors since last check:
Visitor Badges	Ensure sufficient visitor badges are available based on average demand in a day		# of visitor badges available:
Other Items			
Lighting	Visually check that all lighting is working properly (including lighting at night for CCTV system)		
Locks	Check that all doors and fence gate locks into and within Plant are working properly		

Conducted by (printed name): \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

## NAID® Certification Program

### WEEKLY checks to ensure CCTV system is functional and in compliance with NAID Certification Standards

CCTV System			
Cameras	Visually inspect for functionality. Check correct field of view so that all individuals and activity can be seen. Clean lenses.		
Camera Monitors	Visually check monitor for camera functionality and clarity of image		
Recorder	Visually check VHS/DV recorder for functionality - No recognizable delay should be seen between each frame/shot on each camera in system.		
Recording Library	Check most recent seven day recordings for replay standard. Verify library contains the last 90 days of recording and spot check several dates.		
DVR Storage (if applicable)	Check to see that storage capacity will not be exceeded before 90 day capacity reached.		

Conducted by (printed name): \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

CCTV System			
Cameras	Visually inspect for functionality. Check correct field of view so that all individuals and activity can be seen. Clean lenses.		
Camera Monitors	Visually check monitor for camera functionality and clarity of image		
Recorder	Visually check VHS/DV recorder for functionality - No recognizable delay should be seen between each frame/shot on each camera in system.		
Recording Library	Check most recent seven day recordings for replay standard. Verify library contains the last 90 days of recording and spot check several dates.		
DVR Storage (if applicable)	Check to see that storage capacity will not be exceeded before 90 day capacity reached.		

Conducted by (printed name): \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

CCTV System			
Cameras	Visually inspect for functionality. Check correct field of view so that all individuals and activity can be seen. Clean lenses.		
Camera Monitors	Visually check monitor for camera functionality and clarity of image		
Recorder	Visually check VHS/DV recorder for functionality - No recognizable delay should be seen between each frame/shot on each camera in system.		
Recording Library	Check most recent seven day recordings for replay standard. Verify library contains the last 90 days of recording and spot check several dates.		
DVR Storage (if applicable)	Check to see that storage capacity will not be exceeded before 90 day capacity reached.		

Conducted by (printed name): \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

CCTV System			
Cameras	Visually inspect for functionality. Check correct field of view so that all individuals and activity can be seen. Clean lenses.		
Camera Monitors	Visually check monitor for camera functionality and clarity of image		
Recorder	Visually check VHS/DV recorder for functionality - No recognizable delay should be seen between each frame/shot on each camera in system.		
Recording Library	Check most recent seven day recordings for replay standard. Verify library contains the last 90 days of recording and spot check several dates.		
DVR Storage (if applicable)	Check to see that storage capacity will not be exceeded before 90 day capacity reached.		

Conducted by (printed name): \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

**NAID<sup>®</sup> CERTIFICATION PROGRAM  
SUBSTANCE ABUSE RECOGNITION TRAINING PROGRAM  
APPROVAL SUBMISSION FORM**

Please complete this form and submit to NAID to have your Certification Substance Abuse Recognition Program (SARP) approved. The form and the additional items required can be submitted via mail or faxed to (602) 788-4144. Once your program has been approved a confirmation will be sent to you via email or fax.

Please remember that all managers and supervisors must go through the program annually.

If you have any questions, please contact the NAID Certification Program Administrator at (602) 788-6243 ext 206 or at certification@naidonline.org.

**Company:** \_\_\_\_\_ **Individual Contact:** \_\_\_\_\_

Physical Address: \_\_\_\_\_

City: \_\_\_\_\_ State/Prov: \_\_\_\_\_ Country: \_\_\_\_\_ Postal Code: \_\_\_\_\_

Total # Supervisors Trained at above Operation: \_\_\_\_\_ Total # Destruction Employees at above Operation: \_\_\_\_\_

Is the application for multiple locations?  No  Yes

*If yes, please provide the Company name (if different than above), city and state of the other locations that will be utilizing this program.*

1. Company: \_\_\_\_\_ City: \_\_\_\_\_ State/Prov: \_\_\_\_\_ Country: \_\_\_\_\_

2. Company: \_\_\_\_\_ City: \_\_\_\_\_ State/Prov: \_\_\_\_\_ Country: \_\_\_\_\_

3. Company: \_\_\_\_\_ City: \_\_\_\_\_ State/Prov: \_\_\_\_\_ Country: \_\_\_\_\_

Agency administering the program: \_\_\_\_\_

Contact person at Agency: \_\_\_\_\_

Agency phone number: \_\_\_\_\_ Email address : \_\_\_\_\_

Title of Program: \_\_\_\_\_

Date the program was last conducted (or is to be conducted): \_\_\_\_\_

Duration of the program: \_\_\_\_\_ minutes

I am providing the following program information:

Type of or sample of dated documentation indicating the successful completion of the program:

- Certificate  Graded test  
 Signed attendance roster  Other, explain \_\_\_\_\_

**AND**

- Proof of DOT approved program **OR**  Outline of Program & Handouts/materials used during training

Signed: \_\_\_\_\_ Date: \_\_\_\_\_

Print Name: \_\_\_\_\_ Title: \_\_\_\_\_

**NAID Use Only**

**Substance Abuse Recognition Program Training Approval**

Signed: \_\_\_\_\_ Date: \_\_\_\_\_

Print Name: \_\_\_\_\_ Title: \_\_\_\_\_

