

# National Association for Information Destruction, Inc.



## **NAID<sup>®</sup> Certification** **Computer Hard Drive Sanitization** *January 2010*

**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

## Computer Hard Drive Sanitization

### January 2010

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: \_\_\_\_\_  
 General Liability (Aggregate or Umbrella) Indemnification Level: \$\_\_\_\_million  
 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.*
- MOBILE** – Physical destruction (not overwriting or wiping) of computer hard drives performed at the customer’s premises.

*Other than sanitization of hard drives, what other operations take place within the building (check all that apply)?*

- None
- Physical Destruction of Electronic Media*
- Resale or Storage of Sanitized Media*
- Deguassing*
- Other (please indicate):* \_\_\_\_\_

**Application Fee: \$2420\***

\*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  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 certification or does business. NAID is not responsible for the compliance of its individual 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 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 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 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 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.  Certification is optional and is not required for NAID membership.
2.  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.
3.  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 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.
4.  The Company understands the 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 hard drives or sample sanitized hard drives from the Company "stock," this will be considered a failed audit and the Company will not be NAID Certified. Also, all sample "stock" hard drives will be returned, but the Company acknowledges that NAID and/or its agents are not responsible for damage that may occur to the hard drives during this recovery testing.
5.  The stated application fees are only applicable for control hard drives and sample hard drives 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 hard drives 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.

6.  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.
7.  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 Computer Hard Drives.
8.  The Company must reapply for certification on an annual basis, prior to the expiration of the current certification. If the Company chooses not to reapply and/or not to submit to the required audit, it will result in loss of Certification. Loss of certification will not affect NAID membership.
9.  The Company will hold NAID harmless from any claim of damage or loss as a result of the Company’s failure to achieve certification.
10.  The location applying for the Sanitization endorsement for NAID Certification must provide physical media destruction as a component of this process.
11.  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.
12.  The Company understands that the specifications and fees for certification are subject to change at the discretion of the NAID Board of Directors.
13.  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).
14.  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.
15.  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.
16.  The Company understands that random Unannounced Audits are part of the 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.
17.  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.
18.  At any time during the application and/or audit process or after Certification, the Company acknowledges that NAID, its agents and/or the Certification Auditor may investigate or require additional information or documentation from the Company in order to verify information on this Application or the Certification criteria.
19.  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.
20.  If at any time during the process of an audit of the Company or its locations, or during its Certification, *any* of the information submitted as part of the Application changes, such as, but not limited to, a change in ownership, change in operations, change in address, or closure of a location, the Company must notify NAID in writing within 15 days of this status change. **Failure to do so may result in fines, sanctions and/or revocation of Certification.**
21.  The Company agrees that if any location for which it is seeking NAID Certification becomes certified, then if at any time during the audit process or Certification the Company elects to discontinue any or all 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 Certification status) of the change.
22.  The Company understands that ALL NAID certifiable services/operations being offered to the Company’s customers must be Certified by January 1, 2011, in order to maintain NAID Certified status. If the Company is not, at the time of this application, seeking Certification for all certifiable services being offered, it must submit an additional application and fees prior to December 31, 2010 to apply for Certification for the additional services. **Failure to apply for and/or successfully pass an audit of all certifiable operations prior to January 1, 2011 will result in the removal of all NAID Certifications.**

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

23.  The Company understands that the NAID Auditor does NOT approve or deny 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 Certification, or denial of application.
24.  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 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 Certification and why the finding is incorrect. The Company understands that the Certification Review Board will rule on the dispute within one month from receiving it. The Company will accept the ruling of the Certification Review Board as final and seek no further remedy, legal or otherwise, except to reapply for Certification at the Company's discretion.
25.  This Application is truthful and accurately represents the daily operating procedures of the Company's Sanitization and Physical Hard Drive Destruction operations. If any of the Company's representatives willfully deceive NAID or a Certification Auditor, the Company could be immediately removed from NAID, or the Certification may be revoked.
26.  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	<p>Applicant Claims</p> <hr/> <p>Auditor Verifies</p> <hr/> <p><i>All Access Individuals and Non-Access Employees must sign a Confidentiality Agreement and employees must be legally Registered to work at company.</i></p> <p><i>(See Employment Information Disclaimer.)</i></p>	<p>Files for all <b>Access Individuals* and Non-Access Employees' must contain the following documentation:</b></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</li> </ul> <p>In addition to the documents listed above, screening for <b>Access Individuals*</b> must include verification of:</p>
1.2	<p>Applicant Claims</p> <hr/> <p>Auditor Verifies</p> <hr/> <p><i>Access Individuals are subject to the employment screening restriction requirements of NAID Certification, including employment verification, criminal background check and initial employment drug-screening.</i></p> <p><i>(See Employment Information Disclaimer.)</i></p> <p>* Access Individuals who are 1) Subcontractors, independent contractors, or employees thereof , 2) officers, directors, owners and/or partners of the Company but who are not engaged in the day-to-day operation of the Company, or 3) other individuals who have access to or can grant or authorize access to the Confidential Customer Media to be destroyed at the Company's location are exempt from the employment verification, drug screening requirements, and I-9 requirements. This means that any Access Individuals representing the Headquarters of the Company's information destruction division, minimally the President/Vice President of area &amp;/or Audit Coordinator, must have criminal background searches conducted.</p> <p>Also, for Non-Employees or Subcontractors, the Company may have a written agreement in place stating that the current NAID Certification employee screening requirements are being met, in lieu of the actual records.</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>	<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</li> <li>○ Statewide database search for all states on SS Header Search</li> <li>○ County database search for all counties on SS Header Search</li> </ul> </li> <li>• <b>7 Year Employment History Verification</b></li> <li>• <b>Pre-hire or Initial Drug Screening</b></li> </ul> <p>*Access Individuals who are exempt from the employment verification, drug screening requirements, and I-9 requirements are 1) officers, directors, owners and/or partners of the applicant company not engaged in the day-to-day operation of the applicant company, 2) others who have access to, can grant or authorize access to the Confidential Customer Media to be destroyed at the applicant's location but are not engaged in the day-to-day destruction operations, and/or 3) independent contractors, Subcontractors or employees thereof.</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>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 style="padding-left: 40px;">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 style="padding-left: 40px;">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> <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, 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>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>, both statewide and county-by-county searches must be conducted for any record searches conducted after July 1, 2005. Prior to that date, either statewide or county-by-county searches were acceptable. If both statewide and county searches are not available in a particular state, the applicant may do the one available and provide documentation to support the unavailability of the other. Searches done at the federal/national level are not required and may not be used in lieu of state or county level searches.</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><b>(NOTE: Continued on the next page)</b></p>

	Initial	Criteria	Audit Methodology
			<p><i>(NOTE: Continued from the previous page)</i></p> <p>A <b>social security header search</b> 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. Prior to January 1, 2006, the Social Security Header search was not required for Certification.</p> <p>The criminal record search <b>must be current</b>, 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 information. 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 Customer Media.</p>
1.3	<p>Applicant Claims _____</p> <p>Auditor Verifies _____</p>	<p><b>Access Individuals</b>, other than those exempted from the drug screening requirements as discussed above, 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>
1.4	<p>Applicant Claims _____</p> <p>Auditor Verifies _____</p>	<p>All <b>Access Employees</b> have criminal record searches conducted every three years by the following method (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>
1.5	<p>Applicant Claims _____</p> <p>Auditor Verifies _____</p>	<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>			
2.1	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
2.2	Applicant Claims _____ Auditor Verifies _____	<b>Access Individuals</b> display company-issued photo I.D. badges at all times 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 _____ Auditor Verifies _____	While at customer's location, drivers and other employees of contractor must wear a specific uniform (minimum of company shirt) to improve recognition by customers.	Auditor to inspect uniform of at least one driver and confirm that wearing a uniform is specified in policies and procedure manual(s).
2.4	Applicant Claims _____ Auditor Verifies _____	At time of media pick-up, customer must be provided with a receipt indicating type and quantity of media and an acknowledgement of the services rendered.	Auditor will inspect the company policies and procedures manual to insure that customer documentation process contains the requisite information and will inspect a copy or sample of the customer documentation.  If a subcontractor is used for transport prior to destruction, the subcontractor must provide the customer and the applicant company with the customer receipt documentation. Auditor to verify documentation has been provided by the subcontractor and is being utilized by inspecting a copy of a past customer receipt.
2.5	Applicant Claims _____ Auditor Verifies _____	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.	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.  Auditor will inspect the company policies and procedures manual to assure that secure custody of the media prior to sanitization or destruction is addressed.  At the plant, Auditor will determine that there is a secured area designated for holding media when unattended until that media can be sanitized or destroyed.
2.6	Applicant Claims _____ Auditor Verifies _____	All media are securely contained during transfer from customers' custody to transportation vehicle to prevent loss from wind, tipping/spillage or other atmospheric conditions.	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.
2.7	Applicant Claims _____ Auditor Verifies _____	All vehicles used for transfer of client media will have the applicable government inspection for roadworthiness on file.	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, which does not require an inspection of commercial vehicles, auditor will require copy of government statement saying so. Three vehicle records will be checked.

	Initial	Criteria	Audit Methodology
2.8	Applicant Claims _____ 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 _____ 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 _____ Auditor Verifies _____	Unauthorized access to the designated sanitization or secure destruction area and client media is effectively prevented.	Auditor to inspect all entrances to see that unauthorized access to secured area 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 _____ Auditor Verifies _____	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 plant. This log info/record must be maintained for one year.	Auditor will examine visitor/contractor logs and verify records maintained for one year.
2.12	Applicant Claims _____ Auditor Verifies _____	There is a secure area within the building devoted specifically for hard drive 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.	Auditor to inspect building to determine that separate secured areas exist for hard drive sanitization and physical media destruction; Staging for each process must have separate secure areas if not contained within the sanitization or destruction area.  The secured areas within the building must meet the following specifications: <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 _____ Auditor Verifies _____	There is a <u>monitored</u> alarm system in place and utilized when the secure destruction building is unoccupied. Monitoring Company:	Auditor is to inspect alarm system to make sure it is operational and examine alarm test reports &/or invoices from alarm monitoring service.

	Initial	Criteria	Audit Methodology
2.14	Applicant Claims _____ Auditor Verifies _____	There is a closed circuit camera system monitoring all access points into the secure destruction building/area and all processing activity with sufficient clarity to identify people and their activities.  <b>Recordings must be retained for 90 days in an organized, retrievable manner.</b>	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.  <b>CCTV playback must be available at the time of the scheduled audit.</b>  Auditor to inspect recording library system and to review four 4-minute samples: <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> Recording of operations may be suspended for playback recordings.
2.15	Applicant Claims _____ Auditor Verifies _____	The following Operational Security systems are checked and maintained on a monthly basis: <ul style="list-style-type: none"> <li>• Alarm system</li> <li>• Lighting</li> <li>• Door Locks</li> <li>• Visitor Logs</li> </ul> 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.  Monthly and Weekly Logs must be kept for one year using the NAID-issued Forms (or the information/content contained on it).	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.
<b>SANITIZATION &amp; PHYSICAL DESTRUCTION PROCESS</b>			
3.1	Applicant Claims _____ Auditor Verifies _____	<b>PHYSICAL DESTRUCTION OF CONVENTIONAL COMPUTER HARD DRIVES</b>  The company has a written and verifiable process for the physical destruction (not wiping or overwriting) of conventional computer hard drives.  Method of Physical Destruction: _____  <input type="checkbox"/> Plant-based only  <input type="checkbox"/> Plant-based & Mobile	Auditor will review the company's written policies and procedures for their standard <b>physical destruction</b> (not wiping or overwriting) of computer hard drives. As part of their methodology, company must record the serial numbers of all hard drives or CPUs being destroyed for each client. Company must have printed procedures for the physical destruction of computer hard drives.  Auditor to review Questionnaire responses and the company's policies and procedures to assure physical destruction of electronic media is addressed.

	Initial	Criteria	Audit Methodology
3.2	<p>Applicant Claims</p> <p>_____</p> <p>Auditor Verifies</p> <p>_____</p>	<p><b>SANITIZATION OF CONVENTIONAL COMPUTER HARD DRIVES</b></p> <p>The company has a written and verifiable process for the sanitization of conventional computer hard drives.</p> <p>The essential components of the Sanitization Process are defined in the <b>Sanitization Process Questionnaire responses</b>.</p>	<p>Auditor will review Questionnaire responses and the company's written policies and procedures detailing their standard computer hard drive <b>sanitization process</b>. Some of the key components included in this process are:</p> <ul style="list-style-type: none"> <li>• Staging</li> <li>• Acceptance, identification &amp; recording (of serial numbers), and tagging of computer hard drives</li> <li>• Wiping Software Product used</li> <li>• Recovery or verification Software used</li> <li>• Quality control through random checks</li> <li>• Tagging/identification and separation/isolation of sanitized hard drives after processing</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 computer hard drives have been physically sanitized and/or destroyed.</li> </ul> <p>Applicant will demonstrate its ability to successfully sanitize computer hard drives by:</p> <ul style="list-style-type: none"> <li>• Completing sanitization on two (2) control hard drives provided to Applicant at audit appointment – These hard drives 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) hard drives from the Applicant's processed inventory, each between 80 &amp; 120 GB in size – Auditor will randomly select the two hard drives 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) hard drives will be sent to a data recovery service to verify that data is not conventionally retrievable. If any hard drives are found to be containing data, Applicant will NOT be certified.</p> <p>Auditor will observe the sanitization process for at least one hard drive.</p>
3.3	<p>Applicant Claims</p> <p>_____</p> <p>Auditor Verifies</p> <p>_____</p>	<p>Standard operating procedures states that the destruction or computer hard drive 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 computer hard drives occurs within (indicate timeframe) _____.</p>	<p>Auditor will check procedures manual to assure that there is a procedure stated 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</p>

	Initial	Criteria	Audit Methodology
3.4	Applicant Claims _____ Auditor Verifies _____	The Sanitization process has a method of quality control in place to ensure all information has been removed from the sanitized hard drives.  The quality control procedures are described in the company's procedures manual and the <b>Sanitization Process Questionnaire responses</b> .	Auditor will review <b>Sanitization Process Questionnaire response</b> and check procedures manual to assure that quality control procedures are in place, which ensure all information has been removed from the sanitized hard drives; minimally this requires a random sampling of sanitized units for data recovery attempts.
3.5	Applicant Claims _____ Auditor Verifies _____	Physically destroyed media must be disposed (sold, gifted, or discarded) in a responsible manner.  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.	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.).
3.6	Applicant Claims _____ <input type="checkbox"/> <b>Not Claimed</b> _____ Auditor Verifies _____	<p><b>TRANSFER OF CUSTODY (IF APPLICABLE)</b></p> <p>Transfer of custody is used for each as indicated, whether subcontracted or arranged by Applicant for their client.</p> <p>Applicant (Check all that apply)</p> <p><input type="checkbox"/> Temporary Staffing</p> <p><input type="checkbox"/> Transportation (of media prior to destruction)</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), full disclosure must be made to the client regarding the circumstances of the custody chain and whether that meets the applicable 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 <b>Transfer of Custody</b>, or a transfer or extension of <b>Fiduciary Responsibility</b> (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 <b>clients</b> have explicitly been notified in writing (including email or other electronic method) that they <b>are fully aware of the process</b>; 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 <b>Access Individuals</b> 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 <b>fiduciary responsibility</b>; 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 customers in writing that such service is not NAID Certified.</li> <li>• <b>All Access Employees and Individuals</b> 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>

	Initial	Criteria	Audit Methodology
<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.	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.*

1. Do you provide your customers 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 hard drives, and tagging of computers for sanitization and physical destruction:
3. How are hard drives for sanitization, hard drives for physical destruction and drives that require no destruction services identified and segregated?
4. Do you stage/hold hard drives 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 hard drives 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 are the CPUs/hard drives 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 used and describe the method utilized, i.e. 1's and 0's, random characters, Secure Erase, etc.
  - Manufacturer:
  - 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 computer hard drives.
10. Identify the Recovery/Verification Software used during the Quality Control check to confirm that no information is recoverable from the sanitized hard drives (or define in detail method used); the QC software manufacturer must be different than the Sanitization software manufacturer.
  - Manufacturer:
  - Version Number:
  - Serial Number:
11. Briefly describe your Quality Control Process that confirms again that no recoverable information is on the sanitized hard drives. The process must minimally include the following:
  - Percentage or number of random hard drives selected
  - The QC process on a particular hard drive is performed by a different individual than the one who sanitized the unit
  - Procedure to follow if check reveals that the hard drive has not been completely or properly sanitized (recoverable information on it)

12. How are the sanitized and quality checked hard drives 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 hard drives/CPU's throughout the entire sanitization process.

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

- Original receipt date of hard drives
- serial numbers of hard drives
- completion date for sanitization and/or physical destruction

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

# Certification Forms

NAID<sup>®</sup> has designed specific 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>Additional Required Materials for Certification Application</b>
<b>Agreement for Responsible Disposal</b>
<b>Employee Notice of Unannounced Audits</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 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 above 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 does accept the fiduciary responsibility to process and dispose of the Destroyed Materials as agreed herein
- The materials will only be transferred to an entity or agent that is not a party to this agreement under the condition of acceptance of fiduciary responsibility by the third party entity in accordance with this agreement. The transfer of the materials to a third party will not relieve the Disposal Agent of its obligations under this agreement.
- 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)**

## 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		
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: \_\_\_\_\_

