

# National Association for Information Destruction, Inc.



**NAID<sup>®</sup> Certification**  
*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 PROGRAM**

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 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 security, employee hiring and screening, operational destruction process, and insurance.

NAID Members who are seeking Certification for the first time are required to submit the most current Certification Application and associated fees to NAID Headquarters. Once the application is received complete by NAID Headquarters, an audit is assigned to the location to perform the initial 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. This Certification will be effective for one calendar year.

Certified NAID Members are required to apply for recertification on a yearly basis to keep their Certification active. The most current Certification Application and associated fees must be submitted to NAID Headquarters prior to the first day of the month in which the current Certification expires. After the initial audit for the first year, recertification audits will then be required every other year. During the years in which an audit is required, the process for initial audits will be repeated (see above). For non-audit years, Certification will be awarded once a completed application and associated fees are received, prior to the expiration date.

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 submit an application and pass an audit to be certified. NAID members who receive certification must specify which location is 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 to 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.aidonline.org](http://www.aidonline.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@aidonline.org](mailto:certification@aidonline.org).

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

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

### **Initial/New Certification & Recertification Years Requiring Audits (1<sup>st</sup> year, 3<sup>rd</sup> year, 5<sup>th</sup> year, etc.):**

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 forwards a copy of the application to the regional auditor.
3. The auditor contacts the applicant to schedule the initial 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. 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).

### **Recertification Process for Non-Audit Years (2<sup>nd</sup> year, 4<sup>th</sup> year, 6<sup>th</sup> year, etc.):**

1. A Certified NAID Member submits a completed Certification Application to NAID Headquarters prior to the first day of the month in which the current Certification expires. This includes the Additional Required Materials requested on page 2, as well as the application fee.
2. Once the application is determined to be complete, 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, 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 50% 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.

### **MULTIPLE LOCATIONS/ CORPORATE PROGRAM**

Companies with three or more locations may utilize this program. Depending upon the number of Company Branches, the audit schedule and fees vary:

- Companies with 3 to 24 Branches – Under this program, each company branch/location providing information destruction services must pass an initial audit per the NAID Certification specifications. Each year thereafter, one-third of the company locations must be audited and approved in order to maintain their Certification. The Branch Application fees are paid at the time of application and are at the standard Certification rates.
- Companies with 25 or more Branches - Under this program, one third of the company branches/locations providing information destruction services must pass an initial audit per the NAID Certification specifications. During each the of two following years, one-third of the company locations must be audited and approved in order to maintain their Certification. The Headquarters & Branch Application fees are paid each year at the time of application and are at a higher Multi-location Program rate.

For more information, contact the NAID International Headquarters Office at (+1) 602.788.6243 ext. 206 or [certification@naidonline.org](mailto:certification@naidonline.org).

# The NAID<sup>®</sup> Certification Program

## DEFINITIONS

The following are definitions of words or terms used in regard 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.

**BIN TIP** –The process of servicing a collection bin or exchanging bins containing Confidential Customer Media to be destroyed.

**COLLECTION FACILITY** – A facility separate from a secure destruction facility where Confidential Customer Media is stored exactly as accepted from a customer, with no further modification of packaging and no access or processing by staff after collection. Confidential Customer Media for destruction may not be stored for a period longer than 3 business days before being transferred to a secure destruction facility.

If Confidential Customer Media is stored in a facility longer than three business days, the facility is classified as a Transfer Processing Station (*see definition and application criteria for details*).

In the event that the Company location maintains its own commercial records storage center, and stores/stages Confidential Customer Media generated for destruction from that facility exclusively, the facility is NOT considered a Collection Facility. However, if a records storage center is also used to store Confidential Customer Media on an intermediary basis while in transit from customer location to a separate destruction facility, it is then classified as a Collection Facility.

A Collection Facility must meet all program Operational Security requirements (*see section 2 in the criteria*) as a destruction facility with the exception of a CCTV monitoring and recording system.

**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.

**MICRO MEDIA** - Microfiche and Microfilm only; this does NOT include CD's, DVD's, x-rays, cassette tapes, nor any data recording and storage device.

**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.

**PAPER OR PRINTED MEDIA** – Information printed on paper or other material that can be read by the naked eye without the assistance of a special device, such as documents, ID badges, credit/debit cards and photos.

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

**PURGE** – An information destruction project that is defined by the service provider and client as an inordinately large amount of Confidential Customer Media to be destroyed.

**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.*

**TRANSFER PROCESSING STATION** – A facility without destruction capability, and where Confidential Customer Media destined for a destruction facility are batched, sorted, cleaned or repackaged within the facility; or a facility where Confidential Customer Media is stored for more than three business days while in route to a destruction facility.

A Transfer Processing Station must meet all the same program Operational Security requirements as a destruction facility (*see Application criteria requirements*).

**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

January 2010

## U.S. & Canada Applicants only

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

### Profile Information

Year Destruction Business Established: \_\_\_\_\_ Total Number of Access & Non-Access Individuals for this Location: \_\_\_\_\_

General Liability (Aggregate or Umbrella) Indemnification Level: \$\_\_\_\_\_million

Normal Hours of Operation: \_\_\_\_\_

No. Of Vehicles/Trucks in Fleet: Mobile Destruction/Shredding: \_\_\_\_\_ Collection: \_\_\_\_\_

Are any of your Destruction or 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): \_\_\_\_\_

### Operation(s) Application is for:

**MOBILE**

*Do your destruction trucks & drivers service any of your other company locations?*

No  Yes - To Certify, please include all drivers on employee list and indicate location(s)

City & State: \_\_\_\_\_

**PLANT-BASED**

*Other than information destruction, what other operations take place within the building (check all that apply)?*

None

Recycling (of unshredded paper)  Records Storage  Other (please indicate): \_\_\_\_\_

*Do you utilize Collection Facilities or Transfer Processing Stations (check all that apply)?*

NO ( no Collection Facilities & no Transfer Processing Stations)

Collection Facilities utilized (# Facilities): \_\_\_\_\_

Transfer Processing Stations\* utilized (# Stations): \_\_\_\_\_

\*Transfer Processing Station Audit (see Definition) – must be audited and meet the physical facility security requirements.

Application must indicate all Transfer Processing Stations (and their addresses) used by a Plant-based Destruction Branch.

Media Endorsement(s) for: (Must check (apply for) at least one – See Definitions Page for descriptions of the media below)

**PAPER OR PRINTED MEDIA**

**MICRO MEDIA (Microfiche or Microfilm only)**

**Physical Destruction of Conventional COMPUTER HARD DRIVES**

Do you offer any of the services above, for which you are NOT seeking Certification?  No  Yes (specify): \_\_\_\_\_

Application Fee (per site): \$825 for Mobile or Plant-based Operation \$660 per Transfer Processing Station\*  
 \$935 for BOTH Mobile & Plant-based Operations \$935 for Mobile Op w/Transfer Processing Station

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: ____/____/____	Complete: ____/____/____	DBS Updates: ____/____/____	Packet Sent: ____/____/____
Audit Appt: ____/____/____	Auditor Rec: ____/____/____	CRB Approval: ____/____/____	Expires: ____/____/____
Funds given to controller: ____/____/____ Invoice: YES NO		Audit required: YES NO	

**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.

In addition, 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 Destruction and Collection Vehicles** – A List of all mobile information destruction and collection vehicles, including Vehicle make & model, VIN, License Plate Number and the State the vehicle is licensed in.
- 3) **List of Recipients of Destroyed Media** – List should include all companies receiving destroyed media from Applicant within the last year and ultimate responsible disposition of materials (pulping, incineration, smelting, 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)
- 5) **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 shredding 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 met the criteria for the type(s) indicated on this application may be considered a failure of the audit.
4.  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.
5.  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 and/or destruction of Confidential Customer Materials.
6.  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.
7.  The Company will hold NAID harmless from any claim of damage or loss as a result of the Company's failure to achieve Certification.

8.  The Company agrees that any location seeking NAID Certification will be certified for Micro Media (Microfiche and Microfilm) destruction only if the Company: 1) indicates in the application for such location that the location possesses equipment that meets the required specification; 2) the equipment was inspected by the auditor at the time of the NAID Certification audit; and 3) the destruction is being performed at the location (generally only at plant-based operations) for which the Company is seeking Certification.
9.  The Company agrees that any location seeking NAID Certification will be certified for Computer Hard Drive destruction only if: 1) the Company has an established and published standard destruction method for physically destroying computer hard drives; 2) all customers receiving Computer Hard Drive Destruction services have agreed to or have been notified in writing to these standard procedures or other specific procedures; 3) these standard procedures have been demonstrated to the NAID Auditor during the NAID Certification audit of this location; and 4) the destruction is being performed at the location (generally only at plant-based operations) for which the Company is seeking Certification.
10.  The Company understands and agrees that if a location becomes Certified for Mobile Operations only, then the Company must always destroy while on or near the customer's premises unless the customer has agreed in writing (including notification to the customer by e-mail or as part of the customer's agreement with the Company) to permit destruction at a site remote from the customer's location. If the Company's mobile unit performs the shredding away from the customer site without such written consent or notice, the Company will be considered to be no longer following the Mobile Certification standards and may be subject to review and investigation by the Certification Review Board.
11.  The Company understands and agrees that if the Company is applying for Plant-based Operations, the Company must maintain at least 90 days of CCTV recordings for each plant or Transfer Processing Station and 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 all destruction locations will utilize Company service paperwork or contract that includes customer acknowledgement, receipt or agreement regarding the specific service it is receiving. If destruction services rendered by the Company after it is NAID Certified are not among those for which the Company is NAID Certified, but such services could be NAID Certified (plant-based, mobile operations or sanitization operations, and/or destruction endorsements for paper/printed media, micro media or computer hard drives) and/or are recycling services of unshredded/intact paper, then the Customer 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 customer agreement/contract or another written notice (including e-mail or another electronic method that may be printed) delivered by the Company to the customer/recipient of services.

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

22.  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.
23.  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.**
24.  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.
25.  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.
26.  This Application is truthful and accurately represents the daily operating procedures of the Company's secure shredding operations. The Company understands that if any of its representatives willfully deceive NAID or a Certification Auditor, the Company could be immediately removed from NAID, or the Certification may be revoked.
27.  Indications of the signatory's initials above and the signature below acknowledge that I am an owner, corporate officer or official representative of the Company submitting this Application. The undersigned has full authority to request that the Company apply for NAID Certification and submit to any requisite audits, with full knowledge of the Company's operation to accurately complete the Application, and the authority to execute this agreement.

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

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

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

	Initial	Criteria	Audit Methodology
<b>EMPLOYEE REQUIREMENTS</b>			
1.1	Applicant Claims <hr/> Auditor Verifies <hr/>	<p><i>All Access Individuals and Non-Access Employees</i> must sign a Confidentiality Agreement and employees must be legally Registered to work at company.</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:</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 employment verification, criminal background check and initial employment drug-screening.</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. <b>Searches done at the federal/national level are not required and may not be used in lieu of state or county level searches.</b> <i>For all places in Canada</i>, searches must on a province/territory 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>(NOTE: Continued on the next page)</i></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>_____</p> <p>Auditor Verifies</p> <p>_____</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>_____</p> <p>Auditor Verifies</p> <p>_____</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="padding-left: 40px;">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>_____</p> <p>Auditor Verifies</p> <p>_____</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 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 customer with the printed information.  If destruction services rendered by the Company after NAID certification are not NAID Certified, but such services could be NAID Certified (plant-based or offsite services, mobile operations or sanitization operations, and/or destruction endorsements for paper/printed media, micro media or computer hard drives) 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 customer agreement/contract or another written notice (including e-mail or another electronic method that may be printed) delivered by the Company to the customer/recipient of services.	Auditor will inspect the company policies and procedures manual to ensure that customer documentation process contains the requisite information and will inspect a copy or sample of the customer documentation. If applicable, Auditor must inspect a copy or sample of the customer documentation when destruction or recycling services are NOT NAID Certified to verify such notification is stated.  <i>For Plant-based operation only.</i> 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 for destruction are always attended by a Company employee or physically secured from unauthorized access while in the custody of the destruction contractor before they are destroyed.	The auditor will verify that containers used in the field to transport media for destruction. from the client's facility to the destruction provider's vehicle have operable locks and are locked when unattended. Auditor will inspect the company policies and procedures manual to assure that custody of the media for destruction is addressed.  For Plant-based operations, Auditor will determine that there is a secured area designated for holding media when unattended until that media can be 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 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.  If in the field, Auditor to check area around collection or destruction vehicle to verify it is free from loose information-bearing media.

	Initial	Criteria	Audit Methodology
2.7	Applicant Claims _____ Auditor Verifies _____	All vehicles used for transfer of media will have the applicable government inspection for roadworthiness on file.	Auditor will review paperwork from the most recent inspection of all the 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.
2.8	Applicant Claims _____ Auditor Verifies _____	All vehicles used for transfer and/or destruction of media (whether intact or destroyed) will have lockable cabs and lockable fully enclosed boxes. These vehicle cabs and boxes must be locked during transport and when unattended by Access Individual.	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 in either separate category (Mobile Shredding and Collection Only), all trucks in each category must be made available for inspection. If there are 4 or more trucks in each category, 75% of the fleet in each category 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 or destruction 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 Claimed</b> _____ Auditor Verifies _____	<b>APPLIES TO MOBILE CERTIFICATION ONLY</b>  The company must perform mobile destruction services at the customer's site.	Auditor will verify that the Company policies and procedures manual indicates that mobile destruction services must be performed at the customer's site, unless there is a written customer agreement stating otherwise.  A Records Center is considered the customer's site when all media for destruction comes from within it.
2.11	Applicant Claims _____ <input type="checkbox"/> <b>Not Claimed</b> _____ Auditor Verifies _____	<b>APPLIES TO PLANT-BASED CERTIFICATION ONLY</b>  Unauthorized access to the designated secure destruction area and client records 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.
2.12	Applicant Claims _____ <input type="checkbox"/> <b>Not Claimed</b> _____ Auditor Verifies _____	<b>APPLIES TO PLANT-BASED CERTIFICATION ONLY</b>  All visitors entering the 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.

	Initial	Criteria	Audit Methodology
2.13	Applicant Claims _____ <input type="checkbox"/> Not Claimed _____ Auditor Verifies _____	<p><b><i>APPLIES TO PLANT-BASED CERTIFICATION ONLY</i></b></p> <p>There is a secure area within the building devoted only to destroying media. No baling of unshredded paper may take place in this area except cardboard.</p>	<p>Auditor to inspect building to determine that secured area for information destruction exists and that no baling of unshredded paper is processed there.</p> <p>If a secured area within the building is required, it must meet the following specifications:</p> <ul style="list-style-type: none"> <li>• There must be enough space within this area to stage all media to be destroyed.</li> <li>• The wall or fence securing this area must be a minimum of six feet tall and have a lockable gate or door.</li> <li>• 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> </ul>
2.14	Applicant Claims _____ <input type="checkbox"/> Not Claimed _____ Auditor Verifies _____	<p><b><i>FOR EACH BRANCH THAT APPLIES FOR PLANT-BASED CERTIFICATION:</i></b></p> <p>There is a <u>monitored</u> 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>
2.15	Applicant Claims _____ <input type="checkbox"/> Not Claimed _____ Auditor Verifies _____	<p><b><i>APPLIES TO PLANT-BASED CERTIFICATION ONLY</i></b></p> <p>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.</p> <p><b>Recordings must be retained for 90 days in an organized, retrievable manner.</b></p>	<p>Auditor to inspect the closed circuit monitoring system to ensure that it meets 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>90 days of 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>

	Initial	Criteria	Audit Methodology
2.16	Applicant Claims _____ <input type="checkbox"/> Not Claimed _____ Auditor Verifies _____	<p><b>APPLIES TO PLANT-BASED CERTIFICATION WITH A WITH COLLECTION FACILITY</b></p> <p><b>Collection Facilities*</b> are used to store media as accepted by customer and will be transferred to a destruction facility within 3 business days. Facility has restricted access with a monitored alarm system. The list of all Collection Facility locations associated with this plant-based is included with this Application.</p> <p>Number of Collection Facilities: _____</p> <p><b>ADDRESS:</b> _____</p> <p>_____</p> <p><i>*USE ADDITIONAL SHEET OF PAPER, IF NECESSARY, TO LIST THE ADDRESSES OF ALL COLLECTION FACILITIES USED WITH THIS LOCATION.</i></p>	<p>For each <b>Collection Facility</b>, Auditor will check records and procedures manuals to assure that media for destruction are not processed and not stored for more than 3 business days and that the following are maintained*:</p> <ul style="list-style-type: none"> <li>• Access is restricted to Access Individuals</li> <li>• Visitor/Contractor Log</li> <li>• I.D. badges are worn by employees and visitors.</li> <li>• Monitored Alarm System</li> <li>• In the event that the facility also stores records (or is a records center), recycles or bales intact/unshredded paper, or conducts other activities, the collection of media for destruction must be in a Designated (or Delineated) Area or Secured Area depending upon the following:</li> </ul> <p><b>When all employees are Access</b>, a Designated (or delineated) Area is required: Auditor to check that collection area is visually marked/designated or media for destruction is labeled as such.</p> <p><b>When employees are both Access &amp; Non-Access</b>, a Secure Area within Facility is required. Auditor to check that a secured area within the meets the following specifications:</p> <ul style="list-style-type: none"> <li>○ There must be enough space within this area to stage all media to be destroyed.</li> <li>○ The wall or fence securing this area must be a minimum of six feet tall and have a lockable gate or door.</li> <li>○ 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> </ul> <p>*Important Note: Auditor may or may not check the actual facility for requirements at the time of an audit.</p>
2.17	Branch Claims _____ <input type="checkbox"/> Not Claimed _____ Auditor Verified _____	<p><b>APPLIES TO PLANT-BASED CERTIFICATION WITH A TRANSFER PROCESSING STATION</b></p> <p><b>Transfer Processing Stations (TPS)*</b> are used to store materials for destruction no longer than 15 business days and meet the same operational requirements as a secure, plant-based destruction facility. The list of all TPS locations associated with this Branch is included with this Application. Each TPS will be charged an additional audit fee.</p> <p>Number of Transfer Processing Stations: _____</p> <p><b>ADDRESS:</b> _____</p> <p>_____</p> <p><i>*USE ADDITIONAL SHEET OF PAPER, IF NECESSARY, TO LIST THE ADDRESSES OF ALL TRANSFER PROCESSING STATIONS USED WITH THIS LOCATION.</i></p>	<p>For each <b>Transfer Processing Station</b>, Auditor will check records and procedure manuals to assure that materials are not stored for more than 15 business days and that the following are maintained*:</p> <ul style="list-style-type: none"> <li>• Access is restricted to Access Individuals</li> <li>• Visitor/Contractor Log</li> <li>• I.D. badges are worn by employees and visitors.</li> <li>• Monitored Alarm System (records checked)</li> <li>• In the event that the facility also stores records (or is a records center), recycles or bales intact/unshredded paper, or conducts other activities, the collection and processing of media for destruction must be in a Designated (or Delineated) Area or Secured Area depending upon the following:</li> </ul> <p><b>When all employees are Access</b>, a Designated (or delineated) Area is required: Auditor to check that collection area is visually marked/designated or media for destruction is labeled as such.</p> <p><b>When employees are both Access &amp; Non-Access</b>, a Secure Area within Facility is required. Auditor to check that a secured area within the facility meets the following specifications:</p> <ul style="list-style-type: none"> <li>○ There must be enough space within this area to stage all media to be destroyed.</li> <li>○ The wall or fence securing this area must be a minimum of six feet tall and have a lockable gate or door.</li> <li>○ 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> </ul> <ul style="list-style-type: none"> <li>• Maintains a closed circuit camera system, with 90 days of recording, monitoring all ingress/egress points into the secure building/area and processing activity with sufficient clarity to identify people and their activities.</li> </ul>

	Initial	Criteria	Audit Methodology
2.18	Branch Claims _____ <input type="checkbox"/> Not Claimed _____ Auditor Verified _____	<p><b>APPLIES TO PLANT-BASED CERTIFICATION (INCLUDING ANY TRANSFER PROCESSING STATION AND/OR COLLECTION FACILITY)</b></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>	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.

**ENDORSEMENTS & THE DESTRUCTION PROCESS**

3.1	Applicant Claims _____ <input type="checkbox"/> Not Claimed _____ Auditor Verifies _____	<p><b>MEDIA ENDORSEMENT</b></p> <p><b>PAPER or PRINTED MEDIA</b> is destroyed by commercial grade destruction equipment with the following OEM specifications or produces particle sizes no larger than those listed below (applicant to check and complete details for all equipment used):</p> <p><input type="checkbox"/> <b>Continuous Shred:</b> Width (max): 5/8 inch &amp; Length: Indefinite</p> <p><input type="checkbox"/> <b>Cross Cut or Pierce &amp; Tear:</b> Width (max): 3/4 inch &amp; Length (max): 2.5 inches</p> <p><input type="checkbox"/> <b>Pulverizer, Disintegrator or Hammermill*</b> Screen Size (max): 2-inch diameter holes</p> <p><input type="checkbox"/> <b>Unspecified Equipment</b> Please describe the type of equipment and cutting mechanism specifications (screen hole size*, blade width, etc.): _____                      _____                      _____</p> <p>Mobile or Plant Equipment: _____                      Manufacturer: _____                      Model: _____                      Serial #: _____                      Capacity/Throughput (lbs/hr): _____                      Horsepower: _____</p> <p><input type="checkbox"/> <i>See attached form listing additional/all equipment information</i></p> <p><input type="checkbox"/> <b>Pulping or Incineration (Plant-based only)</b>                      Manufacturer: _____                      Model: _____                      Serial #: _____</p>	<p>Certified operations must always utilize commercial grade destruction equipment that meet the Certification specifications.</p> <p><b>CONTINUOUS SHRED, CROSS-CUT, PIERCE &amp; TEAR, PULVERIZER, DISINTEGRATOR &amp;/OR HAMMERMILL:</b>                      Auditor to verify the equipment in use to destroy paper media meets the specifications by:</p> <p style="padding-left: 40px;">Using the OEM specs listed on an invoice or spec sheet that matches the serial number on the equipment.</p> <p style="text-align: center;"><b>OR</b></p> <p style="padding-left: 40px;">Measuring the width of the cutters and/or screens</p> <p>Acceptable deviant tolerance: 1/16 inch</p> <p><b>UNSPECIFIED EQUIPMENT:</b></p> <ul style="list-style-type: none"> <li>• The auditor verifies the particles produced by the equipment are reasonably consistent with the OEM specifications for the equipment.</li> <li>• The auditor verifies that the equipment is conventionally regarded as commercial grade and is consistent with the description provided in this Application.</li> <li>• The auditor verifies that the shredded particles are similar in size to those produced by any of the NAID specified destruction equipment (cross cut, pierce &amp; tear, pulverizer, etc.).</li> </ul> <p>*For destruction equipment with adjustable screens, the Certified location must have a NAID-issued Screen Changing Log (or the information/content contained on it) noting the starting point of the log and the pertinent information regarding any screen changes. A log must be kept on or near each machine, which includes mobile destruction logs being carried in the truck. Records must be maintained for one year. Auditor will review the log(s) during the audit.</p> <p><b>PULPING OR INCINERATION (PLANT-BASED ONLY)</b>                      In-House Pulping or Incineration must not require any Transfer of Custody:</p> <p>If the NAID Member seeking NAID Certification owns or leases the pulping or incineration equipment and building, and also does not transfer custody of media to a third party for transport or processing before media are pulped or incinerated, then the results of the pulping or incineration must effectively reduce the media to a size or condition that is unreadable and not reconstructible</p>
-----	---	---	---

	Initial	Criteria	Audit Methodology
3.2	Applicant Claims _____ <input type="checkbox"/> Not Claimed _____ Auditor Verifies _____	<p><b>MEDIA ENDORSEMENT</b></p> <p><b>MICRO MEDIA DESTRUCTION</b></p> <p>The ability to destroy Micro Media (Microfiche or Microfilm only) is certified based on commercial grade destruction equipment or process which produces a particle size of 1/8 inch maximum dimension or less.</p> <p>Mobile or Plant Equipment: _____</p> <p>Manufacturer: _____</p> <p>Model : _____</p>	<p>Auditor will determine the applicant has equipment with an OEM cutter mechanism of 1/8 inch at its maximum cut dimension by:</p> <p>Using the OEM specs listed on an invoice or spec sheet that matches the serial number on the equipment.</p> <p style="text-align: center;"><b>OR</b></p> <p>Measuring the width of the cutters and/or screens</p> <p>Acceptable deviant tolerance: 1/16 inch.</p>
3.3	Applicant Claims _____ <input type="checkbox"/> Not Claimed _____ Auditor Verifies _____	<p><b>MEDIA ENDORSEMENT</b></p> <p><b>CONVENTIONAL COMPUTER HARD DRIVE DESTRUCTION</b></p> <p>The company has a written and verifiable process for the <b>physical</b> destruction (not wiping or overwriting) of conventional computer hard drives.</p> <p>Mobile or Plant-based Method: _____</p> <p>Method of Physical Destruction: _____</p>	<p>Auditor will review the company's written policies and procedures for their standard <b>physical</b> destruction (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 provided clients with printed materials on their standard destruction procedures or have specific, written agreements with clients' specifying another method of destruction for their computer hard drives. During audit, company must show these written standards and any client agreements for alternative methods used and demonstrate their ability to conduct their standard, described method of computer hard drive destruction.</p>
3.4	Applicant Claims _____ <input type="checkbox"/> Not Claimed _____ Auditor Verifies _____	<p><b>APPLIES TO PLANT-BASED CERTIFICATION ONLY</b></p> <p>Standard operating procedures for bin tips* state that the destruction of confidential media must take place within 3 business days of arriving at the destruction facility, or the policies and procedures, the terms and conditions, or contracts used by the applicant must specify and reflect the actual time frame in which destruction is performed.</p> <p>Standard operating procedures for bin tips* state that destruction occurs within (indicate timeframe) _____.</p> <p>For purges*, the destruction of confidential media must take place within 15 business days or the client must be notified.</p> <p>(*See <i>Certification Program Definitions</i>)</p>	<p>Auditor will check procedures manual to assure that there is a procedure stated that all media are destroyed 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>
3.5	Applicant Claims _____ Auditor Verifies _____	<p>Destruction process has a method of quality control in place to ensure destroyed information is within the stated standards for the specific media endorsements for which the company has applied.</p>	<p>Auditor will check procedures manual to assure that there is a regular quality control procedure in place for ensuring destroyed information are within stated standards.</p>
3.6	Applicant Claims _____ Auditor Verifies _____	<p>Destroyed media must be disposed (sold, gifted, or discarded) in a responsible manner, which does NOT include any type of REUSE (for purposes such as animal bedding or packing materials).</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 materials by these recipients.</p>	<p>Auditor will review list of recipients and manner in which media are disposed subsequent to destruction and verify that company has written agreements or documentation in place to support stated responsible disposal, i.e. pulping, incineration, smelting, etc.</p> <p>Auditor to check waste receptacles and area directly outside of the information destruction building/area to see that no unshredded, confidential information has been deposited in waste receptacles or that no loose information-bearing materials are scattered around or near the destruction building.</p>

	Initial	Criteria	Audit Methodology
3.7	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 (Check all that apply):</p> <input type="checkbox"/> Temporary Staffing <input type="checkbox"/> Transportation (of media prior to destruction) <input type="checkbox"/> Other (describe): _____	<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>
<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, Certificate of Incorporation or SEC filing.
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 an ACORD Certificate, a certificate of insurance or a letter from broker verifying coverage limits. Letter must be dated no earlier than one month prior to audit.

Upon completion of the application, please submit the entire application and additional required materials via  
**FAX (only accepted if paying by credit card)**  
 602-788-4144

OR

MAIL:

NAID, Certification Program, 1951 W. Camelback Road, Suite 350 Phoenix, AZ 85015

## NAID® CERTIFICATION PROGRAM 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 1.5 – 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.
- 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 2.16 – 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), if applicable
- 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 (Paper, Micro Media or Computer Hard Drives)
  - Quantity of Media
  - Acknowledgement of the services rendered
- Customers are notified in writing when they are provided a service that is NOT NAID Certified. This notification may be contained on a materials receipt, or another written agreement between the service provider and recipient of services.
- Containers used to transport confidential materials have operable locks. Locks must always be used when containers have confidential materials and are left unattended.
- Destruction and/or 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 in either category (mobile destruction or collection only), all vehicles must be available. Four or more vehicles in either category (mobile destruction or collection only), 75% of vehicles must be available.)\*\*\*
- All vehicles used for transfer and/or destruction of client records 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 or destruction vehicles.
- Waste receptacles are free from unshredded confidential materials and no loose information-bearing materials are scattered around destruction building/area.

## AUDIT PREPARATION CHECKLIST

-continued-

### **IF APPLYING FOR PLANT-BASED OPERATION ENSURE THAT THESE ITEMS ARE IN PLACE:**

- 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 confidential materials when unattended until destroyed.
- A secured area devoted only to destroying media is available. (No baling of unshredded paper may take place in this area, except cardboard.)
- 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 is 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 – ENDORSEMENTS & THE DESTRUCTION PROCESS**

- APPLICABLE FOR PAPER OR PRINTED MEDIA ENDORSEMENT:**  
Paper or Printed media destruction equipment produces particle sizes as follows:
  - Continuous Shred: Width (max): 5/8 inch & Length: Indefinite
  - Cross Cut or Pierce & Tear: Width (max): 3/4 inch & Length (max): 2.5 inches
  - Pulverized (Equipment with Screens)\*\*\*\*: Screen Size (max): 2 inch diameter holes
- APPLICABLE FOR MICRO MEDIA ENDORSEMENT:**  
Micro Media destruction equipment produces a particle size of 1/8 inch maximum or less.
- APPLICABLE FOR COMPUTER HARD DRIVE ENDORSEMENT:**  
File containing recorded serial numbers of all hard drives or CPUs destroyed for each client and copies of the written standards/agreements for computer hard drive destruction for these clients.
- 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.

\*\*\*\*NAID® issued **SCREEN CHANGING LOGS** (or the information/content contained on it) must be kept for one year, for each piece of equipment, noting the screen changes.

### **Items 4.1 through 4.2 – 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.

**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.

# Certification Forms

NAID® 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.

Form
<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<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 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: \_\_\_\_\_



