National Association for Information Destruction, Inc.

NAID® Electronic Media Certification

2019

World Headquarters
3030 N. 3rd St., Suite 940, Phoenix, AZ 85012
Phone: (602) 788-6243 & Fax: (480) 658-2088
E-mail: certification@naidonline.org

ABOUT THE CERTIFICATION PROGRAM

The NAID Certification Program is offered on a voluntary basis to all NAID active member companies providing information destruction services. NAID members may seek certification for Onsite and/or Plant-based Operations in Hard Drive Sanitization, SSD Overwrite, Degaussing Physical Hard Drive and Non-Paper Media destruction. The NAID Certification Program establishes standards for secure destruction process including areas in security, employee screening, operational destruction process and insurance.

NAID Members seeking initial Certification are required to submit the most current Certification Application and applicable fees to NAID Headquarters. Once the completed application is received an auditor is assigned to perform the initial audit. All audits are performed by security professionals with the Certified Protection Professional (CPP) accreditation issued by the American Society for Industrial Security.

Upon completion of a successful audit, the member is issued a certificate including their company name, type(s) of operations and endorsements for that location. The NAID Member is also listed on the NAID website as a certified location. This Certification is in effective for one calendar year.

Certified NAID Members are required to apply for recertification on an annual basis in order to retain their Certification. The most current Certification Application and applicable fees must be submitted to NAID prior to the first day of the month in which the current Certification expires. After the initial audit, recertification audits will then be required annually.

Under the above program, the certification application and applicable 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. Additional forms can also be found at www.naidonline.org. NAID is committed to maintaining the integrity of the Certification Program and is here to assist your company in achieving Certification. Any questions can be directed to certification@isigmaonline.org.

NAID® Electronic Media Overwriting Certification Application

2019

(Note there is no additional fee to also certify hard copy media, including paper. To add this media, submit the completed Section 3.1 of the Physical Destruction Operations application when submitting this application.)

Company Name: _____ **Audit Contact:** _____

Physical Address: _____ Unit/Ste.: _____

City: _____ State: _____ Postal Code: _____

Phone: _____ Fax: _____ Email: _____

PROFILE INFORMATION

Normal Hours of Operation: _____ Number of Collection Vehicles/Trucks in Fleet: _____

Are any of your Collection Vehicles stored at a location other than address above?

☐ ***No*** ☐ ***Yes*** *(list address)*: _____

First Truck Dispatch Time: _____

TYPE OF AUDIT:

☐ ***Initial*** If an initial audit, are you using a NAID approved consultant? ☐ ***No*** ☐ ***Yes***

Name of Consulting Firm: _____ *(Consulting firm must be pre-approved by NAID)*

☐ ***Recertification***

Operation(s) & Endorsement(s):

☐ ***PLANT-BASED***

- ☐ ***Computer Hard Drive Sanitization***
- ☐ ***Solid-State Overwrite (including mobile phones and hand-held devices)***
- ☐ ***Degaussing***
- ☐ ***Physical Destruction of Hard Drives***
- ☐ ***Physical Destruction of Non-Paper Media***

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

☐ ***Electronics Recycling*** ☐ ***Resale or Storage of Sanitized Media*** ☐ ***Other:*** _____

☐ ***ONSITE***

- ☐ ***Computer Hard Drive Sanitization***
- ☐ ***Solid State Overwrite (including mobile phones and hand-held devices)***
- ☐ ***Degaussing***
- ☐ ***Physical Destruction of Hard Drives***
- ☐ ***Physical Destruction of Non-Paper Media***

Custodial Service:

If you accept intermediary or temporary custody of confidential material prior to destruction then the entire process is eligible for certification. (If you would like to add this to your certification please check all that apply and fill out the NAID Custodial Membership/Certification Addendum.)

- ☐ Records Storage
- ☐ Document Scanning/Imaging
- ☐ Aggregator/Transportation
- ☐ Data Recovery/Forensic Breach Investigation
- ☐ Online Backup
- ☐ Backup Tape Rotation

NAID Use Only			
New or Recert.:		Auditor:	
Audit # :	Received:	Completed:	Expires:

National Association for Information Destruction, Inc.
3030 N. Third Street, Suite 940, Phoenix, AZ 85012
Phone: (602) 788-6243 Facsimile: (480) 658-2088
Email: accounting@naidonline.org

2019 NAID Electronic Media Certification Application Payment Authorization

Application Fee per Site: **(includes all scheduled and unannounced auditing fees)**

□ **US $2830:**
Sanitization Operation Only
Degaussing Operation Only
SSD Overwrite Only

□ **US $3705:**
Sanitization Operation AND Degaussing Operation
Sanitization Operation AND SSD Overwrite
Degaussing Operation AND SSD Overwrite

□ **US $4505:**
Sanitization Operations AND Degaussing Operations AND SSD Overwrite

COMPANY NAME _____ **CITY, STATE/PROV** _____

Method of Payment (select one):

☐ **ONE TIME PAYMENT BY CHECK** (must be issued from a U.S. bank account or converted to U.S. funds)

☐ **ONE TIME PAYMENT BY CREDIT CARD –** AmEx / MC / Visa / Discover (complete form below, print out and send via mail or fax.)

NAME ON CARD: _____

BILLING ADDRESS: _____

CREDIT CARD # _____ EXP _____ CVV _____

SIGNATURE _____ DATE _____

Indications of the signature below acknowledge that I am an owner, corporate officer or official representative of the Company submitting this Payment Authorization and that I have full authority to execute this agreement.

NAME (PRINT): _____ TITLE: _____

SIGNATURE: _____ DATE: _____

NAID USE ONLY				
Audit#:	New/Recert:	App Rcvd:	Acct Rcvd:	Processed:

Employment Information Disclaimer

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

Also, a particular requirement of this application, although permissible under applicable laws and regulations, may violate applicable laws and regulations if applied in an impermissible manner, particularly in regard to hiring and retention practices. You should consult your own legal counsel to determine whether 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 date of hire. Also, the Applicant must indicate any employees who are not citizens of the employer's country. (***See the Definitions document for detailed descriptions of Access Individuals and Non-Access Individuals).***

2) List of Collection Vehicles – A List of all collection vehicles, including Vehicle make & model, VIN, License Plate Number and State vehicle is licensed in.

3) List of Recipients of Physically Destroyed Media/Materials – List should include all companies receiving destroyed media/materials from Applicant within the last year and ultimate responsible disposition of materials (materials recycling, metals recovery/smelting, landfill, etc.)

4) Subcontractor list (if applicable) – A list of all companies or agents used within the last year to subcontract any part of the information destruction process indicating what aspects of the process for which they are responsible and accept custody (See Definitions page); this must include any third party or common carriers used within the last year.

5) Sanitization Process Questionnaire *(see attached form – if applicable)* – Applicant must submit responses to all questions, including reference to how and where in their Policies and Procedures these items are addressed.

6) Degaussing Process Questionnaire *(see attached form – if applicable)* – Applicant must submit responses to all questions, including reference to how and where in their Policies and Procedures these items are addressed.

7) Special Consideration Letter *(only applicable for hardship or extreme circumstances)* – Letter requesting a temporary or conditional qualification for a specific NAID Certification criteria; Only considered under extreme or special circumstances, applicant must submit this written request (on Company letterhead and signed by an official Company representative) with their NAID Certification Application. The letter must identify the specific criteria, detail the hardship or special circumstance for consideration, and state how the applicant will achieve the intent of the criteria given their circumstances. The NAID Certification Review Board will review and respond to all requests.

We agree with and are bound to the following: (Please sign on bottom to indicate agreement with the following items.)

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

7. The stated application fees are only applicable for control devices and sample devices from the Company "stock" that have been sanitized using the method of overwriting with ones and/or zeros. The application fees will increase for the testing of devices that have been overwritten with random characters. These fees will be determined on a case-by-case basis and the Company will be contacted with a description of those fees.
8. All application fees are non-refundable, except in the instance where the Auditor fails to conduct the audit on the date, time and location indicated on the *Auditor Assignment & Confidentiality Agreement* (Appointment) form; and when, in such circumstance, the Company decides to withdraw their application.
9. At no time will the label "NAID Certification" or "NAID Certified" be applied, referenced or inferred to facilities or operations of the Company where 1) the location and operating details related to the facility or operation have not been specifically and formally provided to NAID for participation in the NAID Certification program, or 2) the facility or operation does not have any involvement related to the collection, transport, processing, wiping/sanitization, degaussing, and/or destruction of media.
10. The Company must reapply for NAID Certification on an annual basis, prior to the expiration of the current NAID Certification. If the Company chooses not to reapply and/or not to submit to the required audit, it will result in loss of NAID Certification. Loss of NAID Certification will not affect NAID membership.
11. The Company understands that NAID Certification status is public information. Information regarding renewals, lapses, certified operations and endorsements, Company contact information, and the Certification expiration date are displayed on the NAID website and made available to email subscribers.
12. The Company will hold NAID harmless from any claim of damage or loss as a result of the Company's failure to achieve NAID Certification.
13. The location applying for the Sanitization and/or Degaussing endorsement for NAID Certification must provide physical media destruction as a component of this process.
14. The Company understands and agrees that at least 90 days of CCTV recordings must be maintained and the Company must be able to produce them during the time of an audit. If the Company is unable to produce the 90 days of recordings at an audit, the Company may be subject to a reaudit, including associated costs for this reaudit.
15. The Company understands that the specifications and fees for NAID Certification are subject to change at the discretion of the NAID Board of Directors.
16. 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).
17. 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.
18. 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.
19. The Company understands that random Unannounced Audits are part of the NAID Certification Program. Only if asked and not a hardship, the Company will allow access to a NAID Certification Auditor for purposes of conducting such Unannounced Audits.
20. The Company understands that the NAID Certification Review Board tracks verified reports of certification non-compliance per company/location and may issue fines and/or sanctions or recommend removal of certification for certification violations, in accordance with the Certification Review Board Guidelines. Such fines and/or sanctions are in addition to any remedial actions ordered by the Certification Review Board (CRB) to bring the operation back into compliance. All fines must be paid within 30 days, unless the Company chooses to appeal the CRB's decision, in which case a formal appeal must be submitted to NAID Headquarters no later than 45 days after the date of notification of the fine/sanction. The Company understands that the NAID Complaint Resolution Council (CRC) will review appeals of CRB fines/sanctions, and the Company will be granted the opportunity to provide spoken testimony within 30 days of the formal submission of the appeal. The NAID Board of Directors will review the CRC's recommendation and make the final decision on all appeals. The Company will accept the ruling of the NAID Board of Directors as final and seek no further remedy, legal or otherwise.
21. If the Company is applying for NAID Certification of Onsite Sanitization or Degaussing Operations, copies of all Quality Control Logs and Client documentation are stored at the Headquarters Office, for review during scheduled and unannounced audits.
22. 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.
23. At any time during the application and/or audit process or after NAID Certification, the Company acknowledges that NAID, its agents and/or the NAID Certification Auditor may investigate or require additional information or documentation from the Company in order to verify information on this Application or the NAID Certification criteria.

24. 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.
25. The Company understands and agrees that if the Company has a change in address, ownership, or the operations/services it offers to Clients any time during a pending NAID Certification application or audit, or while the Company is NAID Certified, the Company must notify NAID in writing within 15 business days of this status change. Failure to do so may result in fines, sanctions and/or revocation of NAID Certification.
26. The Company understands and agrees that should it undergo a change in controlling interest in ownership, it will notify the controlling interest that written verification must be provided to NAID within 30 calendar days of the date the acquisition is final. The written notice must also state that the controlling interest will continue to operate within NAID Certification standards under the new ownership, and that it will submit to an audit within six months of the date the acquisition is final. Failure to apply for, or to successfully pass, an audit under the new ownership may result in removal of certification.
27. If the Company is certified for plant-based operations, the Company understands and agrees that should it relocate to a new location it will provide to NAID written verification within fifteen days of the date of the move that the Company will continue to operate within NAID Certification standards at the new location, and that it will submit to an audit within six months of the date of the move. Failure to apply for, or to successfully pass an audit at the new location, may result in removal of certification.
28. The Company agrees that if any location for which it is seeking NAID Certification becomes NAID Certified, then if at any time during the audit process or NAID Certification the Company elects to discontinue any or all NAID Certification operations or endorsements for such location, the Company must notify NAID in writing within 30 days of this status change and has an ethical responsibility to inform clients (aware of the Company's NAID Certification status) of the change.
29. The Company understands that ALL NAID certifiable services/operations being offered to the Company's Clients must be NAID Certified in order to gain and maintain NAID Certified status. If the Company adds a certifiable operation after NAID Certification has been approved, it has 6 months in which to apply for NAID Certification of the new operation. Failure to apply for and/or successfully pass an audit of all certifiable operations may result in the removal of all NAID Certifications.
30. The Company understands that the NAID Auditor does NOT approve or deny NAID Certification. The Auditor's findings will be submitted to the NAID Certification Review Board for approval, determination of remedial or corrective actions and/or additional fees necessary to approve a NAID Certification, or denial of application.
31. The Company has 14 business days (as determined by the date on the notice sent to the Company regarding the results of an audit) to submit to the NAID Certification Review Board in writing any protest of the results of an audit. The Company understands that the protest should clearly state the perceived reason of the failure to achieve NAID Certification and why the finding is incorrect. The Company understands that the NAID Certification Review Board will rule on the dispute within one month from receiving it. The Company will accept the ruling of the NAID Certification Review Board as final and seek no further remedy, legal or otherwise, except to reapply for NAID Certification at the Company's discretion.
32. This Application is truthful and accurately represents the daily operating procedures of the Company's Sanitization, Degaussing and/or Physical Destruction operations. If any of the Company's representatives willfully deceive NAID or a NAID Certification Auditor, the Company could be immediately removed from NAID, or the NAID Certification may be revoked.
33. Indications of the signatory's initials above and the signature below acknowledge that they are an owner, corporate officer or official representative of the Company submitting this Application. The undersigned has full authority to request this audit, with full knowledge of the Company's operations to accurately complete the application, and the authority to execute this agreement.

This information provided in this application is truthful and accurate. I have permission and legal authority to bind the organization to the above agreements in this application. By signing below, I agree to adhere to the above agreements.

Signed: _____ Date: _____

Print _____ Title: _____

	Initial	Criteria	Audit Methodology
		EMPLOYEE REQUIREMENTS	
1.1	Applicant Claims _____ NAID USE ONLY Verified by _____	***All Access Employees and Non-Access Employees*** must have the following on file: • **Confidentiality Agreement** • **I-9 Form** U.S. employees hired after November 7, 1986 or proper work registration for non-citizens *(See Employment Information Disclaimer.)*	The Auditor will request evidence of the appropriate documentation in the employee files as follows: • 7 or fewer Access and/or Non-Access Employees: Auditor will view employee files for all Access and Non-Access Employees. OR • More than 7 Access and/or Non-Access Employees: Auditor will view employee files as a random sample , totaling 25% of the entire Access and Non-Access Employees List, with a minimum of 7 employees and a maximum of 15 employees.
1.2	Applicant Claims _____ Auditor Verifies _____ NAID USE ONLY Verified by _____	***Access Employees*** must have the below employment screening requirements: • **7 Year Criminal Record Search:** o Social Security Header Search listing all associated addresses of the employee. (Must be conducted prior to the criminal background investigation to ensure all counties, states, and federal district courts of residence and employment have been included and verified in the investigation) o County records search for all counties on Social Security Header Search o Statewide records search for all states on Social Security Header Search o Federal Records Search for all Federal Districts in all states on Social Security Header Search • **Pre-hire or Initial Drug Screening** • **7 Year Employment History Verification** which must include the following for each place of employment: o Name, City and State of the previous employer o Dates of employment, as reported by the employee o Date of verification (or attempted verification if the previous employer cannot be reached) o Indication of if the previous employer was able to verify the dates employment. The criminal record search must be conducted by a third-party. County and state checks must be pulled directly from the county and state repositories. Federal checks must be pulled from the federal district courts or via PACER. The use of a secondary database, often referred to as a SuperSearch, InstaSearch and/or National/Nationwide Search is not allowed. If federal, statewide and/or county searches are not available in a particular state, the applicant must complete the ones available and provide documentation to support the unavailability of the other. Canadian searches must be done on a province/territory and National basis and obtained through a third-party background search service or Canadian Police Information Centre (CPIC). When searches are being conducted in places outside of the U.S. every effort should be made to have the searches done at a level comparable to the county and state searches done in the U.S. If a location has restrictive employee agreements in place that prevents drug screening and/or criminal record searches for certain employees, a letter must be submitted stating who and what employee screening restrictions are in place.	Auditor must inspect applicable documentation for all Non-Citizen Employees and Access Employees who are owners, partners or senior managers (of destruction division) of the Company. The following Access Employees are exempt from the Employment Verification, Drug Screening and I-9: 1) officers, directors, owners and/or partners of the Company not engaged in the day-to-day operations; 2) others who have access to or can grant 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. Any Access Employees representing the Headquarters of the Company's information destruction division, minimally the President/Vice President of area &/or Audit Coordinator, whether at the location listed on this application or at another location, must have criminal background searches conducted. Auditor will review the results of the Social Security Header Search and criminal background checks of the selected employees. Criminal background checks must include a list and the results of the jurisdictions searched. No person subject to a felony conviction in the last 7 years for any crime involving theft (of tangible or intangible property), fraud, burglary or larceny, and no person currently incarcerated for any crime may be employed in a capacity where they may come in contact with Confidential Customer Media. This applies to all Access Employees. The employment screening is applicable to all Access Employees (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 Employees whose employment predates the implementation of NAID Certification, must state that they have been employed with the company for the past 7 years.

	Initial	Criteria	Audit Methodology
1.3	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***APPLIES TO ONSITE CERTIFICATION ONLY*** Only those individuals who are verified to be on the Company's payroll, and who are direct employees of the Company (NOT contract or temporary) must perform Onsite Sanitization services.	The Auditor will review the Company's payroll records to verify that all field technicians /employees listed on the employee list (provided with this application) are directly employed by the Company, and not contracted or temporary.
1.4	Applicant Claims _____ NAID USE ONLY Verified by _____	Access Employees are monitored for drugs/substance abuse by one of the following methods (check one): ☐ Option #1: On a random basis, 50% of access employees are drug screened annually. **OR** ☐ Option #2: Management has been trained in a "Substance Abuse Recognition Awareness Program" pre-approved by NAID.	Auditor will verify evidence of the method indicated: Option #1: Invoices/results from drug testing lab for random sampling drug screening of 50% of employees **OR** 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.
1.5	Applicant Claims _____ NAID USE ONLY Verified by _____	Ongoing criminal record searches on Access Employees by one of the following methods (check one): ☐ Option #1: One-third of Access Employees have been randomly selected and criminal record searches conducted annually. ☐ Option #2: One-third of all Access Employees 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. ☐ Option #3: All Access Employees have criminal record searches conducted every three years. Year of most recent search: _____	Auditor will review the results of the criminal record search of the employees based upon the method indicated.
1.6	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	Drivers meet all licensing requirements of the governmental jurisdiction.	The applicable law or regulation for commercial driver licenses will be made available and examined by the Auditor. Auditor will request any items required by law for all drivers listed on the Access and Non-Access Employees List.
		OPERATIONAL SECURITY	
2.1a	Applicant Claims _____ NAID USE ONLY Verified by _____	The firm has written policies and procedures for drivers and destruction processing employees.	Auditor to inspect copy of policies and procedures manuals

	Initial	Criteria	Audit Methodology
2.1b	Applicant Claims _____ NAID USE ONLY Verified by _____	Prior to gaining access to confidential material, all drivers and destruction processing employees must sign an acknowledgement indicating that they have received, read and understand the Company's current written policies and procedures. A new acknowledgment must be signed by employees on an annual basis.	Auditor to inspect employee files for a signed acknowledgement of the Company's current written policies and procedures. This form must reference the version of the written policies and procedures that it applies to. A new acknowledgment must be signed by employees on an annual basis.
2.1c	Applicant Claims _____ NAID USE ONLY Verified by _____	The Company has a written policy in place, stating that the Company will notify any Customer of a potential release of, or unauthorized access to, that Customer's Confidential Customer Media that poses a threat to the security or confidentiality of that information within 60 days of the date of discovery of the data security breach incident.	Auditor will check procedures manual to ensure there is a written policy stating the Company will notify any Customer of a potential release of, or unauthorized access to, that Customer's Confidential Customer Media that poses a threat to the security or confidentiality of that information within 60 days of the date of discovery of the data security breach incident.
2.1d	Applicant Claims _____ NAID USE ONLY Verified by _____	The Company has a written policy in place instructing and requiring employees to notify management of a potential release of, or unauthorized access to, Confidential Customer Media that poses a threat to the security or confidentiality of the information.	Auditor will check procedures manual to ensure that there is a written policy instructing and requiring employees to notify management of a potential release of, or unauthorized access to, Confidential Customer Media that poses a threat to the security or confidentiality of the information.
2.1e	Applicant Claims _____ NAID USE ONLY Verified by _____	The Company has a written Incident Response Plan for responding to suspected or known security incidents. The Incident Response Plan must include a post-incident business impact analysis and a process for documenting all incidents and their outcomes.	Auditor will review the Company's written Incident Response Plan to ensure there is a policy addressing post-incident business impact analysis and documentation of all incidents and their outcomes.
2.1f	Applicant Claims _____ NAID USE ONLY Verified by _____	The Company has a written policy that addresses the procedures for employees to follow during an unannounced audit. This policy must name at least one person or position of contact with physical access to the information the auditor may ask to review, which is to be contacted in the event of an unannounced audit at the destruction plant or the office. Should circumstances prevent the designated point of contact from being available at the time of the unannounced audit, the Certification Review Board may request additional information to be provided at a later date.	Auditor will review the Company's written policies and procedures for their written policy instructing employees in the procedures to follow during an unannounced audit..

	Initial	Criteria	Audit Methodology
2.1g	Applicant Claims _____ NAID USE ONLY Verified by _____	All Access Employees must be trained annually to comply with the NAID AAA Certification requirements: ☐ Option #1: All Access Employees have taken and passed the NAID Access Employee Training Program (AETP). (Submit AETP Licensing Form with application.) ☐ Option #2: All Access Employees have taken and passed a third-party training course which has been pre-approved by NAID. (Submit AETP approval form and outline of training with application.) ☐ Option #3: All Access Employees have taken and passed an in-house training. If NAID has not already approved the training course for this purpose, an approval form and outline of the program is included with this application. (Submit AETP approval form and outline of training with application.)	Auditor will review evidence of annual training to ensure all Access Employees have passed a training program which complies with the NAID AAA Certification requirements.
2.2	Applicant Claims _____ NAID USE ONLY Verified by _____	Access Employees must display a Company-issued photo I.D. badge at all times while on duty. Badges must minimally include a photo, employee name and Company name.	Auditor will inspect the Company policies and procedures manual to ensure there is a written policy for Access Employees to display a Company-issued photo I.D. badge at all times while on duty. Auditor will also inspect employees present to verify that they are wearing photo I.D. badges.
2.3	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	While at the Customer's location, drivers and other employees of contractor must wear a specific uniform (minimum of Company shirt) to improve recognition by Customers..	Auditor will inspect the Company policies and procedures manual to ensure there is a written policy for drivers and other employees of contractor must wear a specific uniform while at the Customer's location. Auditor will also inspect drivers present to verify they are wearing uniforms.
2.4	Applicant Claims _____ NAID USE ONLY Verified by _____	At the time that media is transferred from the Customer's custody to the custody of the Company's employees, the Customer must be provided with a receipt or certificate of sanitization/degaussing/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 services rendered by the Company are not NAID Certified, but such services could be NAID Certified 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. For Plant-based Operations and Transfer Processing Stations only: If a Subcontractor is used for transport prior to sanitization/degaussing/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 _____ NAID USE ONLY Verified by _____	All media for sanitization/degaussing/destruction must always be attended by an access employee or physically secured from unauthorized access while in the custody of the contractor before it is sanitized/degaussed/destroyed.	The Auditor will verify that containers used in the field to transport media for sanitization/degaussing/destruction from the Customer's facility to the provider's vehicle have operable locks. Auditor will inspect the Company policies and procedures manual to assure that custody of the media for destruction is addressed. For Plant-based operations and Transfer Processing Stations: Auditor will determine that there is a secured area designated for holding media when unattended until that media can be destroyed.

	Initial	Criteria	Audit Methodology
2.6	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	All media is 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 in the field to verify 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.
2.7	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	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 that does not require an inspection of commercial vehicles, Auditor will require a copy of the government statement saying so. Three vehicle records will be checked.
2.8	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	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 Employee.	Auditor will inspect trucks 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. **Note:** If there are 3 trucks or less in either category (Onsite Destruction and Collection Only) all trucks in each category must be made available for inspection. If there are 4 or more trucks in either category, 75% of the vehicles in either 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 _____ ☐ Not Applicable NAID USE ONLY Verified by _____	All drivers of vehicles must have readily accessible two-way communication device.	Auditor to verify each driver has an operable two-way communication device with them or in the vehicle.
2.10	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***APPLIES TO PLANT-BASED SANITIZATION/DEGAUSSING/DESTRUCTION ONLY*** Unauthorized access to Confidential Customer Media in the designated secure destruction area, storage area and/or staging area is effectively prevented.	Auditor to inspect all entrances to verify that unauthorized access to secured area is effectively prevented when media is not attended. Auditor will verify that the Company policies and procedures manual covers access control and unauthorized access interdiction measures.

	Initial	Criteria	Audit Methodology
2.11	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***APPLIES TO PLANT-BASED SANITIZATION/DEGAUSSING/DESTRUCTION ONLY*** All visitors entering the secure destruction building or Transfer Processing Station must sign a log with their name, time in, affiliation, and time out. Visitors must be issued a Visitor Badge and be escorted or under the supervision of an Access Employee at all times while in the building. The log must be maintained for one year.	Auditor will examine visitor logs and verify the logs are maintained for one year.
2.12	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***APPLIES TO PLANT-BASED SANITIZATION/DEGAUSSING/DESTRUCTION ONLY*** There is a secure area within the building devoted specifically for sanitization/degaussing and a separate area for physical destruction of media. No media or equipment ready for resale or simple disposal may be within these areas.	Auditor to inspect building to determine that separate secured areas exist for sanitization/degaussing and physical media destruction. Staging for each process must have separate secure areas if not contained within the sanitization/degaussing or destruction area. The secured areas within the building must meet the following specifications: 1. The wall or fence securing this area must be a minimum of six feet tall and have a lockable gate or door. 2. If the wall or fence does not go all the way to the ceiling, then it must have a ceiling mounted sensor alarm inside and over the perimeter of the secure destruction area (or similar, suitable device) to detect if and when individuals have climbed over or come through a section of the secured area fence/wall.
2.13	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***APPLIES TO PLANT-BASED SANITIZATION/DEGAUSSING/DESTRUCTION ONLY*** There is a third-party monitored alarm system in place and utilized when the secure destruction building is unoccupied.	Auditor is to inspect alarm system to make sure it is operational and examine alarm test reports &/or invoices from alarm monitoring service.
2.14	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***APPLIES TO PLANT-BASED SANITIZATION/DEGAUSSING/DESTRUCTION ONLY*** There is a closed-circuit camera system monitoring all access points into the secure building/areas where media is stored, processed or destroyed. All activities are monitored with sufficient clarity to identify people. There must be enough lighting during non-business hours to ensure that all images have sufficient clarity. NAID must be notified within 48 hours of the discovery of problems with the CCTV system which result in a loss of data. Recordings must be retained for 90 consecutive days in an organized, retrievable manner. Number of days of recordings (as of the date of application): _____	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 all activities in the secure destruction building from point of entry through final destruction, including any unauthorized access to the confidential information. Auditor will also inspect the policies and procedures manual to ensure there is a written policy for notifying NAID within 48 hours of the discovery of problems with the CCTV system which result in a loss of data. 90 days of CCTV playback must be available at the time of the scheduled audit. Auditor to inspect recording library system and to review four 4-minute samples: • Two random samples during operational hours • One random sample during non-operational hours • One sample from the 90th day back from the current date Recording of operations may be suspended for playback recordings.

	Initial	Criteria	Audit Methodology
2.15	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***APPLIES TO PLANT-BASED SANITIZATION/DEGAUSSING/DESTRUCTION ONLY*** The following Operational Security systems are checked and maintained on a monthly basis: • Alarm System • Lighting • Door Locks • Visitor Logs The CCTV system must be checked on a weekly basis, including a minimum of five minutes of playback to ensure that all cameras and recording systems are working correctly. Monthly and Weekly Logs must be kept for one year.	Auditor will exam the Monthly and Weekly Operational Security Maintenance Logs and verify the are maintained for one year.
SANITIZATION, DEGAUSSING & PHYSICAL DESTRUCTION PROCESS			
3.1	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***PHYSICAL DESTRUCTION OF HARD DRIVES & ELECTRONIC MEDIA*** ***(NOTE: NOT NECESSARY WHEN APPLYING EXCLUSIVELY FOR DEGAUSSING OPERATIONS.)*** The Company has a written and verifiable process for the physical destruction of Conventional Computer Hard Drives. The Company also has written and verifiable processes for the following: • Prior to destruction the Company must provide the client with a written description of the process for physical destruction of Hard Drives/Electronic Media. • Hard drives must be damaged to the point where the platters will not spin. • Serial numbers/Unique Identifier of all Devices being destroyed for each client are recorded, unless the client has signed an agreement opting out of this requirement. The opt-out agreement must state that the Company is obligated, under NAID Certification standards, to have the client sign the agreement if they choose to not have their unique identifiers recorded. • The log of recorded serial numbers/unique identifiers of Hard Drives/Electronic Media is returned to the client upon the completion of the service, unless an opt-out agreement has been signed. • That a log of recorded unique identifiers, a log of clients that have opted out of serial number/unique identifier recordation and copies of the opt-out agreements are retained for a specified length of time, as documented in the Company's written policies, or in accordance with Client Agreements or contractual stipulations. Method of Physical Destruction: _____ _____ SSDs must be physically destroyed if the applicant is NOT also seeking certification for SSD overwriting. If SSDs are sanitized without obtaining NAID Certification, the customer must be notified in writing that they are receiving a non-NAID Certified service. (If the Company sub-contracts physical destruction to another vendor, the Company must meet all requirements for Transfer of Custody, as described in Section 3.17 herein.)	Auditor will review the Sanitization Process Questionnaire and the Company's written policies and procedures for their standard physical destruction (not wiping or overwriting) of Hard Drives/Electronic Media. Auditor will also review the Company's written policies and procedures for the following provisions: • A policy that all clients must be provided with a written description of the process for the physical destruction of Hard Drives/Electronic Media prior to destruction. • A policy that all unique identifiers of destroyed Hard Drives/Electronic Media are logged and returned to the client after the completion of the service, unless the client signs the opt-out agreement. • A policy that if the client has opted out of having their unique identifiers recorded they must sign an opt-out agreement that clearly states that the recordation of unique identifiers is a NAID Certification requirement. • That a log of recorded unique identifiers, a log of Clients that have opted out of unique identifier recordation, and copies of opt-out agreements are retained for a specified length of time, as documented in the Company's written policies, or in accordance with Client Agreements or contractual stipulations.

	Initial	Criteria	Audit Methodology
3.2	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***PHYSICAL DESTRUCTION OF NON-PAPER MEDIA*** Small Flash, Optical and/or Magnetic Media, as indicated below, are physically destroyed in accordance with the Company's standard method of destruction. Any method that deviates from this standard method of destruction must be communicated to the Customer in writing. Types of Non-Paper Media physically destroyed: ☐ Optical Media: _____ ☐ Magnetic Media: _____ ☐ Flash/SSD Media: _____ ☐ Other: _____ Method of Physical Destruction: _____	Auditor will review the Company's written policies and procedures for their standard physical destruction of Flash, Optical and/or Magnetic Media (not to include conventional computer hard drives or solid state computer drives). Auditor will review the OEM specifications for the equipment listed and will witness the destruction of at least one item listed for each category. Auditor will also review written policies and copies of documentation provided to the Customer for methods of destruction that deviate from the standard method.
3.3	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***APPLIES TO ONSITE SANITIZATION OF HARD DRIVES AND/OR SOLID-STATE MEMORY DEVICES:*** The Company has a written and verifiable process for the sanitization of Computer Hard Drives and/or Solid-State Memory Circuits (Devices) specifying the following: • Acceptance, identification & recording of serial numbers/unique identifiers and tagging of device(s). (See Item 3.1) • Wiping Software Product used • Recovery or verification Software used • The Sanitization process has a method of quality control in place to ensure all information has been removed from the sanitized media. (See Item 3.6) • The recordkeeping audit trail for the CPU throughout entire sanitization process • Confirmation receipt or Certificate of Destruction reflecting unique identifiers is provided to client indicating device(s) have been physically sanitized. • Documentation left with Client to indicate if any drives failed the wiping process. This document must include the unique identifiers of those drives, regardless of any unique identifier recordation opt-out agreement that may be in place. If any non-sanitized drives are left with the Client, this document must also state that custody of the device(s) is being transferred back to the Client. SOLID STATE DEVICE OVERWRITING: If the applicant is seeking certification for Solid State Memory Device overwriting, please list types of devices currently being erased: 1) _____ 2) _____ 3) _____ 4) _____ 5) _____ ***NOTE: List will be used to determine the type of Control Devices needed for the member to overwrite during the audit.*** (Additional components of the Sanitization Process are defined in the Sanitization Process Questionnaire.)	Auditor will review Questionnaire responses and the company's written policies and procedures detailing their standard Hard Drives sanitization process. A) HARD DRIVE SANITIZATION: Applicant will demonstrate its ability to successfully sanitize Hard Drives by: Completing sanitization on four (4) control devices provided to Applicant during the audit. These devices will have been preformatted with a known amount of control data which must be sanitized and returned to the Auditor prior to departure. These will be sent to a data recovery service to verify that the data is not conventionally retrievable. If any drives are found to be containing data, the applicant will NOT be NAID Certified. Auditor will observe the sanitization process for at least one hard drive. B) SSD OVERWRITING: Auditor will review Questionnaire responses and the Company's written policies and procedures detailing their standard Solid-State Device Overwriting process. Applicant will demonstrate the ability to successfully sanitize SSDs by: Completing sanitization on four (4) control devices with consistent storage structure provided to Applicant during the audit. These devices will have been preformatted with a known amount of control data which must be sanitized and returned to the auditor prior to departure. These will be sent to a data recovery service to verify that the data is not conventionally retrievable. If any devices are found to be containing data, Applicant will NOT be NAID Certified. Auditor will observe the sanitization process for at least one device.

	Initial	Criteria	Audit Methodology
3.4	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***APPLIES TO PLANT-BASED SANITIZATION OF HARD DRIVES AND/OR SOLID-STATE MEMORY DEVICES*** The Company has a written and verifiable process for the sanitization of Computer Hard Drives and/or Solid-State Memory Circuits (Devices), specifying the following: • Acceptance, identification & recording of serial numbers/unique identifiers and tagging of devices. (See Item 3.1 regarding the recordation of serial number/unique identifier requirements.) • Wiping Software Product used • Recovery or verification Software used • Method of tagging/identification and separation/isolation of sanitized Device(s) after processing (See Item 3.9) • The Sanitization process has a method of quality control in place to ensure all information has been removed from the sanitized media. (See Item 3.6) • The recordkeeping audit trail for the device(s) throughout entire sanitization process • Confirmation receipt or Certificate of Destruction reflecting unique identifiers is provided to client indicating device(s) have been physically sanitized. • Documentation left with Client to indicate if any drives failed the wiping process. This document must include the unique identifiers of those drives, regardless of any unique identifier recordation opt-out agreement that may be in place. If any non-sanitized drives are left with the Client, this document must also state that custody of the device(s) is being transferred back to the Client. (Additional components of the Sanitization Process are defined in the Sanitization Process Questionnaire.) SOLID STATE DEVICE OVERWRITING: If the applicant is seeking certification for Solid State Memory Device overwriting, please list types of devices currently being erased: 1) _____ 2) _____ 3) _____ 4) _____ 5) _____ ***NOTE: List will be used to determine the type of Control Devices needed for the member to overwrite during the audit.*** (Additional components of the Sanitization Process are defined in the Sanitization Process Questionnaire.)	NOTE: If the applicant seeks both Hard Drive and SSD Sanitization Endorsements, both A and B below are performed separately, and a Supplemental Forensic Fee will apply. A) HARD DRIVE SANITIZATION: Auditor will review Questionnaire responses and the Company's written policies and procedures detailing their standard Hard Drives sanitization process. Applicant will demonstrate its ability to successfully sanitize Hard Drives by: Completing sanitization on two (2) control devices provided to Applicant during the audit. These devices will have been preformatted with a known amount of control data which must be sanitized and returned to the auditor prior to departure. These will be sent to a data recovery service to verify that the data is not conventionally retrievable. If any devices are found to be containing data, Applicant will NOT be NAID Certified. Random selection of two (2) devices from the Applicant's processed inventory. The Auditor will randomly select the two (2) sanitized devices which will be sent to the data recovery service to verify that the data is not conventionally retrievable. These will be returned to Applicant after testing is completed. If any devices are found to be containing data, Applicant will NOT be NAID Certified. Auditor will observe the sanitization process for at least one drive. B) SSD OVERWRITING: Auditor will review Questionnaire responses and the Company's written policies and procedures detailing their standard Solid-State Device Overwriting process. Applicant will demonstrate its ability to successfully sanitize SSDs by: Completing sanitization on two (2) control devices with consistent storage structure provided to Applicant during the audit. These devices will have been preformatted with a known amount of control data which must be sanitized and returned to the auditor prior to departure. These will be sent to a data recovery service to verify that the data is not conventionally retrievable. If any devices are found to be containing data, Applicant will NOT be NAID Certified. Random selection of two (2) devices from the Applicant's processed inventory. The Auditor will randomly select the two (2) devices which will be sent to the data recovery service to verify that the data is not conventionally retrievable. These will be returned to Applicant after testing is completed. If any devices are found to be containing data, Applicant will NOT be NAID Certified. Auditor will observe the sanitization process for at least one device.

	Initial	Criteria	Audit Methodology
3.5	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***APPLIES TO PLANT-BASED AND ONSITE DEGAUSSING*** The Company has a written and verifiable process for the degaussing of Magnetic Media, to include the following: • Acceptance, identification & recording of serial numbers and tagging of Hard Drives. (See Item 3.1) • Degaussing equipment is listed on the National Security Agency's Evaluated Products List – Degausser (NSA EPL-D). (See Item 3.11) • Procedure for routinely verifying and calibrating degaussing equipment according to OEM specifications. (See Item 3.12) • Procedure for media evaluation by a trained technician to determine the type of media, whether the media is included on the list of approved media for the degaussing equipment used, and whether any data is stored on solid state components. (Any media with solid state components used to store data must be physically destroyed, whether or not the media is first degaussed. See Item 3.14) • Degaussing process has a method of quality control in place to ensure media is physically destroyed or degaussed within the standards stated herein. (See Item 3.7) • Tagging/identification and separation/isolation of degaussed media after processing (See Item 3.9) • The recordkeeping audit trail for the Magnetic Media throughout entire degaussing process • Confirmation receipt or Certificate of Destruction reflecting serial numbers is provided to client indicating that the Magnetic Media has been degaussed. (Additional components of the Degaussing Process are defined in the Degaussing Process Questionnaire.)	Auditor will review the Degaussing Process Questionnaire responses and the Company's written policies and procedures detailing their standard magnetic media degaussing process. Applicant will demonstrate its ability to successfully degauss Magnetic Media by: • Degaussing two (2) control devices provided to Applicant at audit appointment. These devices will have been preformatted with a known amount of control data which must be degaussed and returned to the Auditor prior to departure. These will be sent to a data recovery service to verify that the data is not conventionally retrievable. The size and type of media will be determined according to the information provided in the Degaussing Process Questionnaire, and must represent the OEM's specifications and the list of approved media for the degaussing equipment used. • Random selection of two (2) devices from the Applicant's processed inventory, the size and type of media to be determined according to the information provided herein. Auditor will randomly select the two devices which will be sent to the data recovery service to verify that the data is not conventionally retrievable. These will be returned to Applicant after testing is completed. If any devices are found to be containing data, Applicant will NOT be NAID Certified. Auditor will observe the entire degaussing process.
3.6	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***APPLIES TO PLANT-BASED AND ONSITE SANITIZATION (QUALITY CONTROL)*** The quality control software manufacturer is different than the sanitization software manufacturer, and that the Company employee performing the quality control is different than the person that performed sanitization on the device. For Onsite Sanitization, if the same Company employee performs both sanitization and quality control, the Auditor will determine whether the quality control procedures in place are effective. A specific number or percentage of sanitized devices, as determined by the Company, is selected for quality control assessment on a routine basis. For Onsite Sanitization, the Quality Control assessment is performed at each Client's site, and deemed successful, prior to leaving the site. If the quality control assessment reveals recoverable data from a sanitized drive, all devices processed since the last successful quality control assessment will be reprocessed. Instructions that a log must be kept of all quality control assessments to include: • The date of the check • The quantity of devices checked • The outcome (fail/pass) • A description of corrective actions taken as the result of any failed quality control checks. • Serial numbers/Unique Identifiers of all devices that fail the sanitization process must be recorded in the Quality Control log, regardless of any unique identifier recordation opt-out agreement that may be in place.	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. Auditor will also check logs to ensure the quality control checks are being performed within the timeframes established by the written policy.

	Initial	Criteria	Audit Methodology
3.7	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***APPLIES TO PLANT-BASED AND ONSITE DEGAUSSING (QUALITY CONTROL)*** Degaussing and destruction processes have a method of quality control in place to ensure media is degaussed within the standards stated herein. • A designated individual must perform quality control in regard to the frequency set by the Company (daily, weekly, etc.) • A log is maintained to record quality control checks to include: o Date of the check o Name/initials of individual performing the check o Results of the check o Description of any corrective action o Items checked, which minimally includes the following: ▪ Degaussing is performed within the equipment OEM specifications. ▪ Degaussing equipment is verified for proper calibration and operation using specialized equipment designed for this purpose, and in accordance with the degaussing equipment's OEM specs. An equipment verification and calibration log is maintained to record all instances of equipment verification. (See Item 3.12) ▪ Sample media has been sent to a data recovery service at the rate of frequency recommended by the degaussing equipment OEM specs. (See Item 3.15) ▪ If data was recovered by the recovery service action must be taken. (See Item 3.15) ▪ Serial numbers/Unique Identifiers must be recorded for all media degaussed. (Item 3.8) ▪ Opt-out agreements are maintained for every customer for whom serial numbers/unique identifiers are not being recorded. (See Item 3.8) ▪ The devices degaussed must match the number of devices that were brought into the facility. ▪ Degaussing is completed within 30 days, unless there is a written agreement with the client stating otherwise. (See Item 3.10)	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. Auditor will also check logs to ensure the quality control checks are being performed within the timeframes established by the written policy.
3.8	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***APPLIES TO SANITIZATION & DEGAUSSING (UNIQUE IDENTIFIER RECORDATION)*** The Company has written and verifiable processes for the following: • Manufacturer serial numbers or unique identifier of all media being degaussed for each client are recorded, unless the client has signed an agreement opting out of this requirement. Any opt out agreement must state that the Company is obligated, under NAID Certification standards, to have the client sign the agreement if they choose to not have their serial numbers or unique identifier recorded. • The log of recorded unique identifiers of degaussed media is returned to the client upon the completion of the service, unless the client has opted out of this requirement. • A log of recorded unique identifiers, a log of clients that have opted out of unique identifier recordation, copies of opt-out agreements and copies of calibration equipment verification logs are retained for a specified length of time, as documented in the Company's written policies, or in accordance with client agreements or contractual stipulations.	As part of their methodology, the Company must record the serial numbers/unique identifiers of all media being degaussed for each client and return such list to the client, unless an opt-out agreement has been signed. Auditor will also review the Company's written policies and procedures for the following: • An instruction that all unique identifiers of degaussed media are logged and returned to the client after the completion of the service, unless the client opts out by signing an opt-out agreement. • An instruction that if the client has opted out of having unique identifiers recorded, they must sign an opt-out agreement that clearly states that the recordation of unique identifiers is a NAID Certification requirement. • An instruction that a log of recorded unique identifiers, a log of clients that have opted out of unique identifier recordation, copies of opt-out agreements and copies of equipment verification and calibration logs are retained for a specified length of time, as documented in the Company's written policies, or in accordance with client agreements or contractual stipulations. Auditor will also review unique identifier logs and opt out agreement logs.

	Initial	Criteria	Audit Methodology
3.9	Applicant Claims _____ NAID USE ONLY Verified by _____	All media is tagged, or otherwise marked, to identify and distinguish the sanitized or degaussed media from those that have not yet been sanitized degaussed.	Auditor will review the Company's written policy and process of tagging, or otherwise marking the media to identify and distinguish sanitized or degaussed media from those that have not yet been sanitized or degaussed.
3.10	Applicant Claims _____ NAID USE ONLY Verified by _____	***APPLIES TO PLANT-BASED SANITIZATION AND/OR DEGAUSSING CERTIFICATION ONLY*** Standard operating procedures states that the physical destruction, Hard Drive sanitization, or Magnetic Media degaussing is completed within 30 days, or the policies and procedures, the terms and conditions, and contracts used by the applicant must specify and reflect the actual time frame in which destruction is performed.	Auditor will check procedures manual to assure that there is a procedure stating that all media are destroyed, sanitized, or degaussed within requisite timeframe and verify the timeframe indicated by the applicant. Exceptions include acts of God, breakdowns or client instruction (or permission) to retain media for a longer period
3.11	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***APPLIES TO PLANT-BASED AND ONSITE DEGAUSSING ONLY*** The equipment used by the Company for Degaussing (not wiping or overwriting) Magnetic Media is listed on the National Security Agency's Evaluated Products List – Degausser (NSA EPL-D), and therefore is approved for degaussing Magnetic Media (i.e. computer hard drives or tapes) with the recommended Oersted level for the specific media being degaussed by the Company. Degaussing is performed for media within the range of Oersted listed on the NSA EPL-D list for the specific type of equipment used, and according to the OEM specifications for the specific media being degaussed. These specifications must be listed by media type. When degaussing a media with coercivity that is not within the degaussing equipment's approved range of Oersted, the Company will notify the customer in writing of the receipt of a non-NAID Certified service. Equipment manufacturer: _____ Model No.: _____ Serial No: _____ Is this equipment listed on the NSA EPL-D? ☐ Yes ☐ No If Yes, what is the NSA recommended level of Oersted? _____ List all types of media degaussed with this equipment: _____ _____ _____	The Auditor will verify that the Company's degaussing equipment is included on the National Security Agency's Evaluated Products List – Degausser (NSA EPL-D), and that the media degaussed fall within the range of Oersted listed on the NSA EPL-D list. The auditor will also verify that the Company's degaussing process is in accordance with the equipment's OEM specifications for the specific media being degaussed. The auditor will verify that the Company's written policies and procedures includes a requirement to notify customers in writing of the receipt of a non-NAID Certified service when evaluation of media reveals that the media's coercivity is not within the degaussing equipment's approved range of Oersted.

	Initial	Criteria	Audit Methodology
3.12	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***APPLIES TO PLANT-BASED & ONSITE DEGAUSSING ONLY*** Degaussing equipment is verified for proper calibration and operation using specialized equipment designed for this purpose, and in accordance with the degaussing equipment's OEM specifications. Equipment that utilizes OEM built-in verification for proper calibration and operation satisfies this requirement. An equipment verification and calibration log is maintained to record all instances of equipment verification.	Auditor will review the Company's written policies and procedures to ensure that there is a written policy for verifying degaussing equipment for proper calibration and operation and that a log recording all instances of equipment verification is maintained. The Auditor will conduct a field test with NAID-issued equipment to ensure the degaussing equipment is properly calibrated and operating effectively, in accordance with OEM specifications.
3.13	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***APPLIES TO PLANT-BASED & ONSITE DEGAUSSING ONLY*** All technicians operating degaussing equipment and evaluating media to be degaussed have been trained on the proper use of the equipment, the types of media the equipment can effectively degauss, and how to evaluate media to determine their compatibility with the degausser. This training must be completed and documented prior to granting the technician access to the degaussing equipment or media, and then on an annual basis.	Auditor will review the Company's written policies and procedures to ensure there is a written policy for all technicians evaluating media and operating degaussing equipment to be trained on the proper use of the equipment, the types of media the equipment can effectively degauss, and how to evaluate media to determine their compatibility with the degausser, prior to being granted access to degaussing equipment or media, and then on an annual basis. Auditor will also review documentation to confirm that any employee operating degaussing equipment or evaluating media has been trained.
3.14	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***APPLIES TO PLANT-BASED DEGAUSSING ONLY*** All media are evaluated prior to degaussing by a trained technician to determine the type of media, whether the media is included on the list of approved media for the degaussing equipment used, and whether any data is stored on solid state components. *Any media with solid state components used to store data must be physically destroyed, whether or not the media is first degaussed*.* A log is maintained to track evaluated media, to include date, manufacturer, manufacturer serial number (or unique identifier), type of media, whether the media is included on the list of approved media for the degaussing equipment used, indication of any solid-state components or lack thereof, and final disposition (i.e. physical destroyed or degaussed). *Media manufactured in 2011 and later may contain a green board with solid state memory components.	Auditor will review the Company's written policies and procedures to ensure that there is a written policy for evaluating media prior to degaussing and that a log of all instances of media evaluation is maintained. Auditor will also verify that the Company has a written policy indicating that the final disposition of any media with solid state data storage components is physical destruction of the media.

	Initial	Criteria	Audit Methodology
3.15	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	***APPLIES TO PLANT-BASED & ONSITE DEGAUSSING ONLY*** Sample media are routinely tested by a third-party data recovery service at the rate of frequency recommended by the OEM specifications, and no less than once per year. Such tests must indicate that no recoverable data exists on the tested media. The Company routinely submits sample media to a data recovery service to verify that no usable data can be conventionally recovered from media degaussed with the equipment listed herein, at the rate of frequency recommended by the equipment's OEM specifications and no less than once per year. If no recommendation for testing is made by the manufacturer, ongoing testing of media is not required, other than annual testing performed by NAID. The Company has a written policy for addressing reports from the data recovery service which indicate data was recovered from one or more media. This policy must minimally include the following: • Evaluation of the recovered data to determine the nature and cause of the failure. Evaluation should include additional testing, either in-house or by the use of a third party, as deemed necessary. • Recalibration or reconfiguration of equipment. • Degaussing equipment will be verified for proper calibration and operation using specialized equipment designed for this purpose, and in accordance with the degaussing equipment's OEM specifications, once the issue(s) have been addressed and corrected. • Third party testing of additional sample media once the issue(s) have been addressed and corrected. Clients must be notified in writing of the receipt of non-certified services until the issue has been corrected and a report from the third party lab indicates no usable, recoverable data on tested media.	Auditor will review written policies and procedures and equipment OEM specification to ensure there is a written policy to submit sample media to a data recovery service, at the rate of frequency recommended by the equipment's OEM specifications, to verify that no usable data can be recovered from media degaussed with the equipment listed herein. Auditor will also verify a written policy for addressing reports from the data recovery service which indicate data was recovered. Auditor will review test reports from all tests performed by a data recovery service within the last 12 months. If any tests were returned with a report of usable data, the auditor will also review documentation verifying that the Company's response to such report(s) was in compliance with the requirements specified herein.
3.16	Applicant Claims _____ NAID USE ONLY Verified by _____	Destroyed remnants of hard drives and circuit boards must be disposed (sold, gifted, or discarded) in a responsible manner, which includes a requirement that the recipient of the destroyed electronic media is registered by International Organization for Standardization (ISO) as being compliant with the 14001 standard. Applicant must attach a list of all current recipients of destroyed paper/printed media, micro media and hard drives, indicating the final disposition of materials by the recipients. Requests for a hardship exemption must be submitted in writing to the Certification Review Board.	Auditor will review list of recipients and manner in which computer hard drives are disposed. Auditor will verify that the Company has written agreements in place to support stated responsible disposal. Auditor to check waste receptacles and area directly outside of the information destruction building/area to see that no computer hard drives whether destroyed or intact has been deposited in waste receptacles.

	Initial	Criteria	Audit Methodology
3.17	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified by _____	TRANSFER OF CUSTODY (IF APPLICABLE) Transfer of custody is used for each as indicated (Check all that apply): ☐ Temporary Staffing ☐ Transportation (of media prior to destruction) ☐ Other: _____ If media destruction is subcontracted, all Customers must be notified in writing of the following information: o name of the subcontractor company o the method of the destruction All Access Employees of the companies in the chain of custody must acknowledge in writing that they understand that all media with which they come in contact is confidential, and they accept fiduciary responsibility. All Access Employees of the companies must submit to the same background screening requirements as NAID Certification. All companies accepting custody of media must meet the NAID Certification criteria. If Company does not meet the NAID Certification criteria, then the Customer must be notified in writing that such service is not NAID Certified.	Auditor will check documentation to verify that the customer was notified if transfer of custody occurs. If a site visit is required for verification, the Applicant assumes responsibility for any additional fees of the Auditor.
3.18	Applicant Claims _____ NAID USE ONLY Verified by _____	At the time of a bid or proposal, the Company must notify the potential customer in writing of the following: • If the information destruction service being proposed to the Customer is not NAID Certified at the time of the bid; and/or • If the service involves a subcontractor for either a portion of the destruction process or for the actual destruction of the media. If the services involve a subcontractor notification must also indicate if the subcontractor is not NAID Certified.	The auditor will review the Company's policies and procedures to ensure that there is a written policy stating that all bids or proposals will notify potential customers if the proposed destruction service is not NAID Certified and/or if subcontractors will be used for all or part of the destruction service.
		COMPANY ASSURANCES	
4.1	Applicant Claims _____ NAID USE ONLY Verified by _____	Company is a legally registered business in the state of residence.	Auditor to examine business license.
	Initial	Criteria	Audit Methodology
4.2	Applicant Claims _____ NAID USE ONLY Verified by _____	General liability insurance (aggregate or umbrella) of $2,000,000 or more.	Auditor to examine valid insurance documents, which could be a certificate of insurance or a letter from broker verifying coverage limits. Letter must be dated no earlier than one month prior to audit.

	Initial	Criteria	Audit Methodology
4.3	Applicant Claims _____ NAID USE ONLY Verified by _____	Company is current with all local, state, and federal permits/licenses required for the recycling of computer equipment.	Auditor to examine permits/license required for the recycling of computer or electronic equipment, if applicable.

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

FAX: (480)658-2088
EMAIL: certification@naidonline.org
QUESTIONS: (602)788-6243

SANITIZATION PROCESS QUESTIONNAIRE

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

1. Do you provide your Clients with any written information diagramming or describing the stages of your sanitization process?

2. Briefly describe the receipt/acceptance of media, identification and recording of serial numbers/unique identifiers for Electronic Media and labeling of media for either sanitization or physical destruction.

3. How are Electronic Media for sanitization, media for degaussing (if applicable), Electronic Media for physical destruction and Electronic Media that require no destruction services identified and segregated?

4. Do you stage/hold Electronic Media identified for sanitization in an area other than where they will be sanitized? If so, describe when and how these are moved to the sanitization area.

5. Do you stage/hold Electronic Media identified for physical destruction in an area other than where they will be destroyed? If so, describe security and when and how these are moved to the physical destruction area.

6. How are Electronic Media to be sanitized and those to be physically destroyed secured from unauthorized access and isolated from commingling with other equipment or media for disposal, resale or some other purpose?

7. Identify the sanitization software used for Hard Drive Sanitization and describe the method utilized (i.e. 1's and 0's, random characters, Secure Erase, etc.).
- Manufacturer:
- Model/Version Number:
- Serial Number/Unique Identifier:
- Method:

8. Identify the sanitization software used for SSD Overwrite (if applicable) and describe the method utilized (i.e. 1's and 0's, random characters, Secure Erase, etc.).
- Manufacturer:
- Model/Version Number:
- Serial Number/Unique Identifier:
- Method:

9. How do you determine when wiping/sanitization is no longer acceptable, i.e. damaged sectors, and that physical destruction is now required?

10. Identify the Recovery/Verification software used during the Quality Control check to confirm that no information is recoverable from the sanitized Hard Drives (or define, in detail, the method used). The Quality Control software manufacturer must be different than the Sanitization software manufacturer.
- Manufacturer:
- Version/Model Number:
- Serial Number/Unique Identifier:

11. Identify the Recovery/Verification software used during the Quality Control check to confirm that no information is recoverable from the sanitized SSDs (or define, in detail, the method used). The Quality Control software manufacturer must be different than the Sanitization software manufacturer.

- Manufacturer:
- Version/Model Number:
- Serial Number/Unique Identifier:

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

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

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

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

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

DEGAUSSING PROCESS QUESTIONNAIRE

Please fully respond to each of the questions below, as well as indicating where (page or section) it is addressed within your company's policies and procedures. Please attach a separate sheet with your responses.

1. Do you provide your Clients with any written information diagramming or describing the stages of your degaussing process?

2. Briefly describe the receipt/acceptance of media, identification and recording of serial numbers/unique identifier for Magnetic Media, and labeling of media for either degaussing or physical destruction.

3. How are media for degaussing, media for sanitization (if applicable), media for physical destruction and media that require no destruction services identified and segregated?

4. Do you stage/hold media identified for degaussing in an area other than where they will be degaussed? If so, describe when and how these are moved to the degaussing area.

5. Do you stage/hold Electronic Media identified for physical destruction in an area other than where they will be destroyed? If so, describe security and when and how these are moved to the physical destruction area.

6. How are media to be degaussed and those to be physically destroyed secured from unauthorized access and isolated from commingling with other equipment or media for disposal, resale or some other purpose?

7. Identify the degaussing equipment used and describe the specific media degaussed with that equipment.
   - Manufacturer:
   - Model/Version Number:
   - Serial Number/Unique Identifier:
   - Range of Oersted listed on NSA EPL-D:

8. Describe the process for evaluating media to determine the type of media, whether the media is included on the list of approved media for the degaussing equipment used, and whether any data is stored on solid state components.

9. Describe the process for routinely verifying and calibrating degaussing equipment. What is the equipment OEM's recommendation for verifying ongoing equipment effectiveness?

10. Describe the process for testing sample media by a third-party data recovery service; including method of recovery and the frequency that testing is conducting. What is the process for addressing reports of recoverable data, including corrective actions? What method and frequency of testing does the equipment OEM recommend?

11. Briefly describe your firm's Quality Control Process.

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

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

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

- Original receipt date of media
- Serial numbers (or Unique Identifiers) of media
- Completion date for degaussing and/or physical destruction

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

NAID® CERTIFICATION PROGRAM
ADDITIONAL REQUIRED MATERIALS FOR APPLICATION

Company Name: _____ City, State/Province: _____

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

Employee Name	Date of Hire	Access Y/N	Title/Position	Citizen Y/N	NAID Auditor use only											
					All Employees		Access Employees Only									File Checked
					Conf Agr	I-9	Drug	SS Trace	Crim State	Crim Cnty	Crim Fed	Empl Ver	2.1b	2.1g	Driver Req	
1.																
2.																
3.																
4.																
5.																
6.																
7.																
8.																
9.																
10.																
11.																
12.																
13.																
14.																
15.																
16.																

ADDITIONAL REQUIRED MATERIALS FOR APPLICATION
-continued-

Company Name:_____ City, State/Province: _____

List of Destruction and Collection Vehicles

Destruction/ Collection	Vehicle Identification Number (VIN #)	Vehicle Make & Model	License Plate Number	State/Province of License	Overnight Storage Address (Addr, City, State)	Available for Audit? Y/N*	NAID Auditor use only			
							Reg. & Ins.	Road-worthy	Locks	Truck Checked
1.										
2.										
3.										
4.										
5.										
6.										
7.										
8.										
9.										
10.										

*See Section 2.8 for the requirements for fleet availability during NAID Certification Audits

List of Additional Destruction Equipment (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.						

*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.	

NAID® Custodial Membership/Certification Addendum

(For companies applying for NAID AAA Certification of destruction services, which also take intermediary or temporary custody of confidential material prior to destruction)

COMPANY INFORMATION

Company Name: _____

Audit Contact: _____ City/State: _____

Email: _____ Phone: _____

COMPANY PROFILE:

Type of Custodial Operations (Check all that apply.):

- ☐ Records Storage
- ☐ Document Scanning/Imaging
- ☐ Aggregator/Transportation
- ☐ Other (describe): _____
- ☐ Data Recovery/Forensic Breach Investigation
- ☐ Online Backup
- ☐ Backup Tape Rotation

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

_____ 1. The custodial services indicated are provided from the same corporation or legal entity and under the same name and from the same or immediately adjacent facilities.

_____ 2. Discarded information resulting from providing the indicated services are destroyed by our NAID certified destruction service when destruction is required.

_____ 3. The background screening of all employees engaged in providing the indicated custodial services is equal to or exceeds NAID certification requirements prior to unsupervised access to client information.

_____ 4. Access control measures related to providing the indicated custodial services meets or exceeds NAID Certification Plant-based Operation requirements.

_____ 5. Custodial services are provided under documented with written security policies and procedures.

_____ 6. Employees engaged in providing indicated custodial services have acknowledged the fiduciary nature of their obligation to protect client information from unauthorized access and to report to management any situation that could or has allowed unauthorized access (see NAID Confidentiality Agreement).

_____ 7. During future scheduled and unannounced NAID Certification audits, the NAID auditor will be allowed to verify any of the stipulations herein.

_____ 8. NAID will be immediately informed (5 business days) of any change in the above stipulations or any in the nature or type of the custodial services offered.

Upon receipt of this agreement, NAID would then add the indicated services to the member's certification profile, resulting in said services being reflected/searchable on the new NAID membership directory.

Signed: _____ Date: _____

Print Name: _____ Title: _____

NAID Use Only		
Audit #:	Received:	Complete:
DBU:	Cert Expires:	Processed by:

NAID Access Employee Training Program Order Form and Licensing Agreement

Please Note : The NAID Access Employee Training Program is only available to NAID Members

Company Name: _____ Individual: _____

Street Address: _____

City: _____ State: _____ Postal Code: _____ Country: _____

Phone: _____ Fax: _____ Email: _____

Will the NAID Access Employee Training Program be utilized at multiple locations? ☐ *No* ☐ *Yes*

If yes, please provide the city and state of the other locations that will be utilizing this program (must be the same company):

1. **Company: _____ City: _____ State/Prov.:_____ Country: _____**
2. **Company: _____ City: _____ State/Prov.:_____ Country: _____**
3. **Company: _____ City: _____ State/Prov.:_____ Country: _____**

NAID Access Employee Training Program

☐ $79.95

This one-time fee grants the NAID Member company (Licensee) rights to use the NAID Access Employee Training Program (Program), including training video, test, test key, and forms to document successful completion of training by Access Employees to fulfil the requirements for access employee training according to Section 2.1g of the NAID Certification Application. Upon processing of payment, a web link to download the training materials will be sent to the email address provided above.

By initialing the following statements it is agreed and understood the following stipulations are a legally binding condition of NAID Access Employee Training Program and Video (Program) use:

_____ The NAID Access Employee Training Program and Video (Program) continues to be the intellectual property of NAID in perpetuity, incorporating all rights and privileges afforded such ownership.

_____ The Member licensing the use of the Program may not reproduce or copy it, in whole or part, in any manner, including written transcripts or excerpts. Licensees are permitted to electronically copy the Program to a computer hard drive with the understanding that the Licensee has the capability and legal responsibility to prevent unauthorized access at all times.

_____ The Member may not post the video, in whole or part, to a publicly accessible website or intranet.

_____ The Member may not allow access to, or allow use by, any other company, entity, agency or individual.

_____ The Member understands the violation of any provisions herein, or a violation of NAID's copyright, and or any effort to circumvent, mitigate, eliminate or prevent NAID's ability to control the distribution of the Video or images from the Video, as determined by NAID, may mean revocation of license, sanctions by NAID including loss of membership or certification, and civil or criminal remedies as NAID may determine appropriate.

_____ Only Members with a copy of this license agreement, which will be stored at NAID Headquarters, may use the Program to fulfil the requirements for Access Employee training according to Section 2.1g of the NAID Certification application.

_____ NAID Certification allows for the use of third party or in-house resources for Access Employee training, subject to NAID approval, and the use of the Program to fulfil the NAID Certification requirement for access employee training according to Section 2.1g of the NAID Certification application is the sole discretion of the Member.

_____ Updated versions of the Program are not necessarily included in this licensing agreement fee and may need to be licensed separately as they become available.

Signed: _____ Date: _____

Print Name: _____ Title: _____

NAID Use Only			
Member#:	Received:	Shipped:	Completed by:

NAID Access Employee Training Program
Payment Form

Company Name: _____Individual: _____

Street Address *(required)*: _____

City: _____ State: _____ Postal Code: _____

TOTAL REMITTANCE: USD $ _____

Payment is by:

☐ Enclosed Check (Payable to "NAID or i-SIGMA")
Check No.: _____

☐ AmEx ☐ Discover ☐ MasterCard ☐ Visa # _____-_____-_____-_____

Expires
(mo/yr): _____ / _____ **CVV code:** _____

Name on Card: _____ Signature: _____

NAID® CERTIFICATION PROGRAM
ACCESS EMPLOYEE TRAINING PROGRAM
APPROVAL SUBMISSION FORM

Please complete this form and submit to NAID for approval of your Access Employee Training Program (AETP). Upon approval of your program a confirmation email will be sent. Please remember that all access employees must go through the program annually.

Company: _____ Contact Name: _____

Contact Email: _____

Physical Address: _____

City: _____ State/Prov: _____ Postal Code: _____

Total # Access Employees Trained: _____(all access employees must be trained, per Section 2.1g of the NAID AAA Certification Application)

Is the application for multiple locations? ☐ *No* ☐ *Yes (*If yes, please provide the Company name, city and state of the other location(s) 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: _____

Title of Program: _____

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

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

☐ Outline of Program & Handouts/materials used during training

Company Signature: _____ Date: _____

Print Name: _____ Title: _____

NAID Use Only

Signed: _____ Date: _____

Print Name: _____ Title: _____

Please submit the form via:
FAX: (480)658-2088
EMAIL: certification@naidonline.org
QUESTIONS: (602)788-6243

NAID® CERTIFICATION PROGRAM
SUBSTANCE ABUSE RECOGNITION TRAINING PROGRAM
APPROVAL SUBMISSION FORM

Please complete this form and submit to NAID for approval of your Substance Abuse Program Training (SARP). Upon approval of your program a confirmation email will be sent. Please remember that manager(s) and/or supervisors must go through the program annually.

Company: _____ Contact Name: _____

Contact Email: _____

Physical Address: _____

City: _____ State/Prov: _____ 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, 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): _____

I am providing the following program information:

☐ Certificate ☐ Graded test

☐ Signed attendance roster ☐ Other, explain _____

AND

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

Company Signature: _____ Date: _____

Print Name: _____ Title: _____

NAID Use Only

Signed: _____ Date: _____

Print Name: _____ Title: _____

Please submit the form via:
FAX: (480)658-2088
EMAIL: certification@naidonline.org
QUESTIONS: (602)788-6243

NAID® CERTIFICATION PROGRAM
SANITIZATION AUDIT PREPARATION CHECKLIST

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

EMPLOYEE REQUIREMENTS

- ☐ All employee must have Confidentiality Agreements and an I-9 form **(Item 1.1)**
- ☐ All Access Employee must have an Employment History Verification, Criminal Record Search and Drug Screening Results **(Item 1.2)**
- ☐ Employees on the company's payroll must perform Onsite Sanitization. **(Item 1.3)**
- ☐ Ongoing annual Access Employee Drug/Substance Screenings: **(Item 1.4)**
  - ☐ Option 1 - Drug/Substance Screening on annual random basis must include a file containing documentation supporting the 50% annual random Access Employee drug testing should be available.

  OR
  - ☐ Option 2 – Substance Abuse Recognition Program Form must be on file containing proof of completed yearly management training.
- ☐ Ongoing Access Employee Criminal Record Searches. **(Item 1.5)**
- ☐ Drivers must have a copy of a valid driver license and/or commercial driver license and any additional items required by governmental jurisdiction for drivers. **(Item 1.6)**

OPERATIONAL SECURITY

- ☐ Policies and Procedures manual must include: **(Item 2.1a)**
  - ☐ Policy for notifying customers of a potential release of, or unauthorized access to confidential material **(Item 2.1c)**
  - ☐ Policy for notifying management of a potential release of, or unauthorized access to confidential material **(Item 2.1d)**
  - ☐ Incident Response Plan for responding to suspected or known security incidents **(Item 2.1e)**
  - ☐ Unannounced Audit procedure and process **(Item 2.1f)**
  - ☐ All Access employees must wear a photo I.D. badge while on duty **(Item 2.2)**
  - ☐ A Company Uniform must be worn by employees **(Item 2.3)**
  - ☐ 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) **(Item 2.4)**
  - ☐ Media is secured from unauthorized access before destroyed **(Item 2.5)**
  - ☐ Containers used to transport confidential materials have operable locks **(Item 2.8)**
  - ☐ Access controls and unauthorized access to the secure destruction area **(Item 2.10)**
  - ☐ Method of physical computer hard drive destruction (if applicable) **(Item 3.3)**
  - ☐ Method of non-paper media destruction for each type of non-paper media destroyed (if applicable) **(Item 3.4)**
  - ☐ Quality control procedures **(Items 3.6 & 3.7)**
  - ☐ Media is tagged/separated between sanitized and degaussing operations **(Item 3.9)**
  - ☐ Sanitization/Degaussing/Physical Destruction timeframe of media **(Item 3.10)**
  - ☐ Employees operating degaussing equipment have been trained on how to properly use the equipment **(Item 3.13)**
  - ☐ Media is evaluated and recorded prior to degaussing **(Item 3.14)**
  - ☐ Sample degaussed media is routinely tested by a third-party **(Item 3.15)**
  - ☐ If the information destruction service being proposed to the Customer is not NAID Certified or if the service will involve subcontractors, the customer must be notified in writing at the time of the bid. **(Item 3.17)**
- ☐ All drivers and destruction processing employee files must contain an annual Acknowledgement of the company's written policies and procedures. **(Item 2.1b)**
- ☐ All access employees have been trained to comply with NAID AAA Certification requirements (AETP) **(Item 2.1g)**
- ☐ Customers are provided with a receipt at the time of Media pickup, which includes the following: **(Item 2.4)**
  - ☐ Type of Media (Paper, Micro Media or Computer Hard Drives)
  - ☐ Quantity of Media
  - ☐ Acknowledgement of the services rendered
- ☐ Customers are notified in writing when provided with 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. **(Item 2.4)**
- ☐ Material must be protected from loss due to wind, tipping/spillage or other atmospheric conditions **(Item 2.6)**
- ☐ Most recent inspections of all commercial vehicles. **(Item 2.7)**

AUDIT PREPARATION CHECKLIST

- ☐ The required number of vehicles to be inspected will be available on the day of audit. (Requirements are: If three or less mobile and/or collection vehicles, all must be available. If four or more mobile and/or collection vehicles, 75% must be available.) **(Item 2.8)**
- ☐ Readily accessible**,** operable two-way communication devices for all drivers. **(Item 2.9)**
- ☐ All visitors must sign visitor log, be issued a visitors badge and be escorted by an Access Employee at all times. Visitor logs must be retained for one year. **(Item 2.11)**
- ☐ A secured area designated is available for holding confidential materials when unattended until destroyed. **(Item 2.12)**
- ☐ A secured area devoted only to hard drive sanitization and another secured area devoted to physical hard drive destruction only. The secured areas within building must meet the following requirements: **(Item 2.12)**
  - ☐ 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 when secure destruction building is unoccupied. **(Item 2.13)**
- ☐ Closed circuit camera system (CCTV) monitoring all access points into secure destruction building/area. **(Item 2.14)**
  - ☐ The CCTV must provide sufficient clarity to identify individuals and their activities. There must be enough lighting at night or during other non-business hours to ensure that all images have sufficient clarity.
  - ☐ 90 days of CCTV recordings must be available from date of audit.
  - ☐ Alarm, Lighting, Door Locks and Visitor Logs are checked on a monthly basis and the CCTV system is checked on a weekly basis and documented via the Operational Security Maintenance Logs. Logs must be retained for one year. **(Item 2.15)**

PHYSICAL DESTRUCTION PROCESS, SANITIZATION & DEGAUSSING\

- ☐ *PHYSICAL HARD DRIVE DESTRUCTION ENDORSEMENT:* **(Item 3.1)**
  Must have the following information:
  - ☐ Recorded serial numbers of all hard drives or CPUs destroyed for each customer
  - ☐ Log of customers that have opted out of serial number recordation (if applicable)
  - ☐ Signed Opt-Out Agreements (if applicable)
  - ☐ Copies of written standards/agreements for computer hard drive destruction for these customers
- ☐ *NON-PAPER MEDIA DESTRUCTION ENDORSEMENT:* **(Item 3.2)**
  - ☐ A Standard method of destruction must be used. If any methods used deviate from the standard, the customer must be notified in writing describing the destruction process.
- ☐ *SANITIZATION OF HARD DRIVES OPERATION:* **(Item 3.3-3.4)**
  - ☐ Recorded serial numbers/unique identifiers of all hard drives or CPUs sanitized for each customer
  - ☐ Log of customers that have opted out of serial number/unique identifiers recordation (if applicable)
  - ☐ Signed Opt-Out Agreements (if applicable)
  - ☐ Wiping Software Product Used/Verified
  - ☐ Sanitization Process Questionnaire
- ☐ *DEGAUSSING OF HARD DRIVES OPERATION:* **(Item 3.5)**
  - ☐ Recorded serial numbers/unique definers of all hard drives or CPUs degaussed for each customer
  - ☐ Log of customers that have opted out of serial number/unique identifiers recordation (if applicable)
  - ☐ Signed Opt-Out Agreements (if applicable)
  - ☐ NSA Evaluated Product List (NSA EP-D) **(Item 3.11)**
  - ☐ Calibration Verification to OEM specs **(Item 3.12)**
  - ☐ Degaussing Process Questionnaire
- ☐ *OVERWRITING OF SSDS OPERATION:* **(Item 3.3-3.4)**
  - ☐ Recorded serial numbers/unique identifiers of all SSDs sanitized for each customer
  - ☐ Log of customers that have opted out of serial number/unique identifiers recordation (if applicable)
  - ☐ Signed Opt-Out Agreements (if applicable)
  - ☐ Overwrite Software Product Used/Verified
  - ☐ Sanitization Process Questionnaire
- ☐ Transfer of custody documentation including subcontractor list, subcontractor agreements, client agreements and proof of meeting certification requirements. (if applicable) **(Item 3.8)**

COMPANY ASSURANCES

- ☐ Business license **(Item 4.1)**
- ☐ Proof of General Liability Insurance (aggregate or umbrella) of $2,000,000.00 or more. **(Item 4.2)**
- ☐ Recycling permits/license **(Item 4.3)**

AUDIT PREPARATION CHECKLIST

☐: Indicates sample forms available online at www.naidonline.org.